

# Квантовая оптика<sup>1</sup>

Петрунькин В. Ю., Мурашко И. В.

5 июня 2019 г.

<sup>1</sup>Санкт Петербургский Государственный Политехнический Университет



# Оглавление

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Квантовая электродинамика</b>   | <b>13</b> |
| <b>1</b> | <b>Квантование электромагнитного поля</b>  | <b>15</b> |
| 1.1      | Разложение электромагнитного поля по модам (типам колебаний)   | 15        |
| 1.2      | Гамильтонова форма уравнений свободного электромагнитного поля . . . . .                                     | 18        |
| 1.3      | Квантование свободного электромагнитного поля . . . . .  | 19        |
| 1.4      | Разложение поля по плоским волнам в свободном пространстве   | 22        |
| 1.5      | Плотность состояний . . . . .  | 24        |
| 1.6      | Гамильтонова форма уравнений поля при разложении по плоским волнам . . . . .                                 | 26        |
| 1.7      | Квантование электромагнитного поля при разложении его по плоским волнам . . . . .                            | 28        |
| 1.8      | Свойства операторов $\hat{a}$ и $\hat{a}^\dagger$ (операторов уничтожения и рождения) . . . . .              | 30        |
| 1.9      | Квантовое состояние электромагнитного поля с определенной энергией (с определенным числом фотонов) . . . . . | 31        |
| 1.10     | Многомодовые состояния . . . . .   | 36        |
| 1.11     | Когерентные состояния . . . . .  | 38        |
| 1.12     | Смешанные состояния электромагнитного поля . . . . .   | 42        |
| 1.13     | Представление оператора плотности через когерентные состояния  | 45        |
| 1.14     | Упражнения . . . . .   | 50        |
| <b>2</b> | <b>Взаимодействие света с атомом</b>   | <b>51</b> |
| 2.1      | Излучение и поглощение атомом света . . . . .  | 51        |
| 2.2      | Гамильтониан системы атом-поле . . . . .   | 52        |
| 2.3      | Взаимодействие атома с модой электромагнитного поля . . . . .  | 56        |
| 2.4      | Интерферометр Рамси. Квантовые неразрушающие измерения .   | 62        |
| 2.5      | Взаимодействие атома с многомодовым полем. Вынужденные и спонтанные переходы . . . . .                       | 64        |
| 2.5.1    | Вынужденные переходы . . . . .   | 65        |
| 2.5.2    | Спонтанные переходы . . . . .  | 69        |

|      |   |     |
|------|---|-----|
| 2.6  | Спонтанное излучение.<br>Приближение Вайскопфа-Вигнера. . . . .   | 70  |
| 2.7  | Релаксация динамической системы. Метод матрицы плотности .  | 74  |
| 2.8  | Взаимодействие электромагнитного поля резонатора с резерву-<br>аром атомов, находящихся при температуре $T$ . . . . . | 76  |
| 2.9  | Уравнение для матрицы плотности поля в представлении чисел<br>заполнения . . . . .                                    | 79  |
| 2.10 | Уравнение движения статистического оператора поля моды в<br>представлении когерентных состояний . . . . .             | 83  |
| 2.11 | Общая теория взаимодействия динамической системы с термо-<br>статом . . . . .   | 87  |
| 2.12 | Релаксация атома в случае простейшего резервуара, состоящего<br>из гармонических осцилляторов . . . . .               | 91  |
| 2.13 | Затухание моды резонатора. Уравнение Гейзенберга - Ланжевена. . . . .   | 93  |
|      | 2.13.1 Постановка задачи. . . . .   | 93  |
|      | 2.13.2 Уравнения движения Гейзенберга для операторов. . . . .   | 94  |
|      | 2.13.3 Флуктационно-диссипационная формула . . . . .  | 100 |
| 2.14 | Упражнения . . . . .  | 100 |

## **2 Квантовая оптика 103**

### **3 Квантовая теория лазера 105**

|     |  |     |
|-----|--|-----|
| 3.1 | Модель лазера . . . . .                                      | 105 |
| 3.2 | Теория лазерной генерации . . . . .                          | 109 |
| 3.3 | Статистика лазерных фотонов . . . . .                        | 110 |
| 3.4 | Теория лазера. Представление когерентных состояний . . . . . | 112 |
| 3.5 | Упражнения . . . . .   | 120 |

### **4 Квантовая теория лазера в представлении Гейзенберга 121**

|     |  |     |
|-----|--|-----|
| 4.1 | Модель лазера . . . . .                                    | 121 |
| 4.2 | Уравнение Гейзенберга для лазерной системы . . . . .       | 122 |
|     | 4.2.1 Уравнение движения атомной подсистемы . . . . .      | 125 |
|     | 4.2.2 Уравнения движения для макро-величин . . . . .       | 131 |
|     | 4.2.3 Уравнения движения электромагнитного поля . . . . .  | 134 |
| 4.3 | Система уравнений Гейзенберга-Ланжевена, описывающая лазер | 136 |
| 4.4 | Естественная ширина линии излучения . . . . .              | 138 |
| 4.5 | Упражнения . . . . .                                       | 142 |

### **5 Оптика фотонов (квантовые явления в оптике) 143**

|     |                      |     |
|-----|----------------------|-----|
| 5.1 | Фотоэффект . . . . . | 143 |
|-----|----------------------|-----|

|          |   |            |
|----------|---|------------|
| 5.2      | Когерентные свойства света . . . . .  | 146        |
| 5.3      | Когерентность второго порядка . . . . .   | 153        |
| 5.4      | Когерентность высших порядков . . . . .   | 162        |
| 5.5      | Счет и статистика фотонов . . . . .   | 163        |
| 5.6      | Связь статистики фотонов со статистикой фотоотсчетов . . . . .  | 164        |
| 5.7      | Распределение фотоотсчетов для когерентного и хаотического<br>света . . . . .                           | 166        |
| 5.8      | Определение статистики фотонов через распределение фотоот-<br>счетов . . . . .                          | 167        |
| 5.9      | Квантовое выражение для распределения фотоотсчетов . . . . .  | 169        |
| 5.10     | Эксперименты по счету фотонов. Применение техники счета<br>фотонов для спектральных измерений . . . . . | 174        |
| 5.11     | Упражнения . . . . .  | 175        |
| <b>6</b> | <b>Квантовое описание оптических интерференционных экспе-<br/>риментов</b>                              | <b>177</b> |
| 6.1      | Общие соображения . . . . .   | 177        |
| 6.2      | Операторные соотношения . . . . .   | 181        |
| 6.3      | Интерферометр Маха-Цендера. Погрешность фазовых изме-<br>рений. . . . .                                 | 183        |
| 6.3.1    | Уравнение интерферометра . . . . .  | 183        |
| 6.3.2    | Точность измерения интерферометром . . . . .  | 186        |
| 6.4      | Упражнения . . . . .  | 187        |
| <b>7</b> | <b>Квантовое описание поляризационных свойств света</b>   | <b>189</b> |
| 7.1      | Классическое описание поляризационных свойств света . . . . .   | 189        |
| 7.2      | Квантовое описание поляризационных свойств света . . . . .  | 192        |
| 7.3      | Упражнения . . . . .  | 195        |
| <b>3</b> | <b>Неклассический свет</b>  | <b>197</b> |
| <b>8</b> | <b>Неклассический свет</b>  | <b>199</b> |
| <b>9</b> | <b>Сжатые состояния</b>   | <b>205</b> |
| 9.1      | Соотношение неопределенности Гайзенберга . . . . .  | 205        |
| 9.2      | Операторы квадратурных составляющих электромагнитного по-<br>ля . . . . .                               | 206        |
| 9.3      | Сжатие квадратурного состояния . . . . .  | 208        |
| 9.4      | Генерация квадратурно сжатых состояний . . . . .  | 215        |
| 9.5      | Наблюдение сжатого состояния. Измерение степени сжатия . . . . .  | 219        |

|           |  |            |
|-----------|--|------------|
| 9.5.1     | Балансная схема гомодинного детектора . . . . .              | 222        |
| 9.6       | Интерференционные измерения с применение сжатого света . .   | 224        |
| 9.7       | Сжатый свет в нелинейных явлениях . . . . .                  | 227        |
| 9.8       | Неклассичность сжатого состояния . . . . .                   | 228        |
| 9.9       | Когерентность второго порядка для сжатого вакуума . . . . .  | 229        |
| 9.10      | Упражнения . . . . .   | 230        |
| <b>10</b> | <b>Перепутанные состояния</b>                                | <b>231</b> |
| 10.1      | Парадокс ЭПР для параметров Стокса и перепутанные состояния  | 232        |
| 10.2      | Неравенство Белла для параметров Стокса . . . . .            | 236        |
| 10.3      | Базисные состояния Белла . . . . .                           | 240        |
| 10.4      | Получение Белловских состояний . . . . .                     | 241        |
| 10.5      | Регистрация Белловских состояний . . . . .                   | 242        |
| 10.6      | Теорема о запрете клонирования и квантовая телепортация. . . | 247        |
| 10.7      | Квантовые псевдотелепатические игры . . . . .                | 249        |
| 10.7.1    | Описание игры . . . . .                                      | 249        |
| 10.7.2    | Классическая стратегия . . . . .                             | 250        |
| 10.7.3    | Квантовая стратегия . . . . .                                | 250        |
| 10.8      | Упражнения . . . . .   | 251        |
| <b>4</b>  | <b>Квантовая теория информации</b>                           | <b>253</b> |
| <b>11</b> | <b>Введение в квантовую теорию информации</b>                | <b>255</b> |
| 11.1      | Информация и энтропия . . . . .                              | 255        |
| 11.1.1    | Энтропия в классической теории информации . . . . .          | 255        |
| 11.1.2    | Энтропия в квантовых системах . . . . .                      | 258        |
| 11.2      | Передача информации. Канал связи. . . . .                    | 259        |
| 11.2.1    | Классический канал связи . . . . .                           | 260        |
| 11.2.2    | Квантовый канал связи . . . . .                              | 260        |
| 11.2.3    | Квантовая плотная кодировка . . . . .                        | 261        |
| 11.3      | Кодирование информации . . . . .                             | 262        |
| 11.3.1    | Теорема кодирования Шенона . . . . .                         | 262        |
| 11.3.2    | Квантовая теорема кодирования . . . . .                      | 263        |
| 11.4      | Упражнения . . . . .   | 264        |
| <b>12</b> | <b>Криптография</b>  | <b>265</b> |
| 12.1      | Одноразовый блокнот . . . . .                                | 266        |
| 12.2      | Проблемы классической криптографии . . . . .                 | 268        |
| 12.3      | Квантовая криптография . . . . .                             | 269        |

|   |                |
|---|----------------|
| <b>13 Квантовые вычисления</b>  | <b>271</b>     |
| 13.1 Основные принципы квантовых вычислений . . . . .   | 272            |
| 13.1.1 Представление информации. Классические и квантовые состояния . . . . .                                   | 272            |
| 13.1.2 Обратимые вычисления . . . . .   | 273            |
| 13.2 Квантовые логические элементы . . . . .  | 274            |
| 13.2.1 Универсальный набор квантовых вентилях . . . . .   | 274            |
| 13.2.2 Управляющие элементы . . . . .   | 276            |
| 13.3 Алгоритм Шора . . . . .  | 276            |
| 13.3.1 Факторизация чисел и нахождение периода функций . . . . .  | 277            |
| 13.4 Квантовое преобразование Фурье . . . . .   | 280            |
| 13.4.1 Схема квантового преобразования Фурье . . . . .  | 280            |
| 13.4.2 Нахождение периода функций с помощью квантового преобразования Фурье . . . . .                           | 288            |
| 13.5 Квантовое преобразование Фурье и дискретное логарифмирование . . . . .                                     | 291            |
| 13.5.1 Двумерное преобразование Фурье и период функции $f(x_1, x_2)$ . . . . .                                  | 293            |
| 13.5.2 Двумерное квантовое преобразование Фурье . . . . .   | 298            |
| 13.6 Алгоритм Шора и дискретный логарифм на эллиптических кривых . . . . .                                      | 300            |
| 13.7 Алгоритм Гровера . . . . .   | 303            |
| 13.7.1 Описание алгоритма . . . . .   | 304            |
| 13.7.2 Анализ алгоритма Гровера . . . . .   | 307            |
| 13.7.3 Реализация базовых элементов алгоритма Гровера . . . . .   | 309            |
| 13.8 Адиабатические квантовые компьютеры . . . . .  | 312            |
| 13.9 Теория сложности алгоритмов и квантовые вычисления . . . . .   | 312            |
| 13.9.1 Классы сложности алгоритмов $P$ , $NP$ , $BQP$ . . . . .   | 312            |
| <br><b>5 Приложения</b>   | <br><b>313</b> |
| <b>14 Основные положения квантовой механики</b>   | <b>315</b>     |
| 14.1 Дираковская формулировка квантовой механики . . . . .  | 316            |
| 14.1.1 Кет-вектор . . . . .   | 316            |
| 14.1.2 Бра-векторы . . . . .  | 316            |
| 14.1.3 Операторы . . . . .  | 317            |
| 14.1.4 Собственные значения и собственные векторы операторов . . . . .  | 318            |
| 14.1.5 Наблюдаемые величины. Разложение по собственным векторам. Полнота системы собственных векторов . . . . . | 319            |
| 14.1.6 Оператор проектирования . . . . .  | 320            |
| 14.1.7 След оператора . . . . .   | 320            |

|           |   |            |
|-----------|---|------------|
| 14.1.8    | Средние значения операторов . . . . .   | 321        |
| 14.1.9    | Представление операторов через внешние произведения<br>собственных векторов . . . . . | 322        |
| 14.1.10   | Волновые функции в координатном и импульсном пред-<br>ставлениях . . . . .            | 323        |
| 14.2      | Динамика изменения волновой функции . . . . .   | 323        |
| 14.2.1    | Уравнение Шрёдингера . . . . .  | 323        |
| 14.2.2    | Различия между чистыми и смешанными состояниями.<br>Декогеренция . . . . .            | 326        |
| 14.2.3    | Редукция волновой функции. Измерение в квантовой ме-<br>ханике . . . . .              | 329        |
| 14.3      | Измеримость физических величин . . . . .  | 332        |
| 14.3.1    | Принцип неопределенности Гейзенберга . . . . .  | 332        |
| 14.3.2    | Соотношение неопределенности энергия-время . . . . .                                  | 334        |
| 14.3.3    | Одновременная измеримость физических величин . . . . .                                | 334        |
| 14.4      | Процедура квантования . . . . .   | 335        |
| 14.4.1    | Обобщенные координаты и импульсы . . . . .  | 336        |
| 14.4.2    | Квантование углового момента . . . . .  | 337        |
| 14.5      | Составные системы . . . . .   | 340        |
| 14.6      | Координатное представление когерентного состояния . . . . .                           | 341        |
| 14.7      | Адиабатическая теорема . . . . .  | 343        |
| 14.8      | Бозоны и фермионы . . . . .   | 344        |
| 14.9      | Золотое правило Ферми . . . . .   | 346        |
| <b>15</b> | <b>Теория вероятностей</b>  | <b>351</b> |
| 15.1      | Алгебра множеств и базовые понятия теории вероятностей . . . . .                      | 351        |
| 15.2      | Классическая Колмогоровская теория вероятностей . . . . .                             | 352        |
| 15.2.1    | Базовые понятия и аксиомы теории вероятности . . . . .                                | 352        |
| 15.2.2    | Случайная величина. Функции распределения . . . . .                                   | 354        |
| 15.2.3    | Распределение Пуассона . . . . .  | 355        |
| 15.2.4    | Случайные процессы . . . . .  | 356        |
| 15.3      | Квантовая теория вероятностей . . . . .   | 358        |
| <b>16</b> | <b>Абстрактная алгебра</b>  | <b>361</b> |
| 16.1      | Введение в теорию групп . . . . .   | 361        |
| 16.2      | Поля . . . . .  | 363        |
| <b>17</b> | <b>Линейная алгебра</b>   | <b>365</b> |
| 17.1      | Линейное пространство . . . . .   | 365        |
| 17.1.1    | Прямая сумма линейных пространств и тензорное про-<br>изведение . . . . .             | 365        |



|           |   |            |
|-----------|---|------------|
| 17.1.2    | Теорема об операторном разложении . . . . .             | 365        |
| 17.2      | Гильбертово пространство . . . . .                      | 367        |
| 17.2.1    | Теорема Стоуна . . . . .                                | 367        |
| <b>18</b> | <b>Преобразование Фурье</b>                             | <b>369</b> |
| 18.1      | Преобразование Фурье . . . . .                          | 369        |
| 18.2      | Дискретное преобразование Фурье . . . . .               | 370        |
| 18.2.1    | Определение . . . . .                                   | 370        |
| 18.2.2    | Свойства дискретного преобразования Фурье . . . . .     | 372        |
| 18.2.3    | Быстрое преобразование Фурье . . . . .                  | 375        |
| 18.3      | Двумерное преобразование Фурье . . . . .                | 376        |
| 18.3.1    | Определение . . . . .                                   | 376        |
| <b>19</b> | <b>Дискретная математика</b>                            | <b>377</b> |
| 19.1      | Наибольший общий делитель. Алгоритм Евклида . . . . .   | 377        |
| 19.1.1    | Соотношение Безу . . . . .                              | 379        |
| 19.2      | Сравнение по модулю . . . . .                           | 380        |
| 19.2.1    | Арифметические операции . . . . .                       | 381        |
| 19.2.2    | Решение уравнений . . . . .                             | 381        |
| 19.2.3    | Поле $\mathbb{F}_p$ . . . . .                           | 382        |
| 19.3      | Функция Эйлера . . . . .                                | 382        |
| 19.3.1    | Определение . . . . .                                   | 382        |
| 19.3.2    | Свойства . . . . .                                      | 382        |
| 19.4      | Малая теорема Ферма . . . . .                           | 383        |
| 19.4.1    | Псевдопростые числа . . . . .                           | 384        |
| 19.5      | Китайская теорема об остатках . . . . .                 | 384        |
| 19.6      | Алгоритм RSA . . . . .                                  | 384        |
| 19.6.1    | Генерация ключей . . . . .                              | 384        |
| 19.6.2    | Шифрование . . . . .                                    | 385        |
| 19.6.3    | Де-шифрование . . . . .                                 | 386        |
| 19.6.4    | Доказательство . . . . .                                | 386        |
| 19.7      | Дискретный логарифм . . . . .                           | 387        |
| 19.8      | Протокол Диффи-Хеллмана (Diffie-Hellman, DH) . . . . .  | 388        |
| 19.9      | Схема Эль-Гамала (Elgamal) . . . . .                    | 389        |
| 19.9.1    | Генерация ключей . . . . .                              | 389        |
| 19.9.2    | Шифрование . . . . .                                    | 390        |
| 19.9.3    | Дешифрование . . . . .                                  | 390        |
| 19.10     | Эллиптическая криптография . . . . .                    | 391        |
| 19.10.1   | Эллиптические кривые над полем $\mathbb{R}$ . . . . .   | 391        |
| 19.10.2   | Эллиптические кривые над полем $\mathbb{F}_p$ . . . . . | 396        |
| 19.10.3   | Скалярное умножение и дискретный логарифм . . . . .     | 398        |

|           |  |            |
|-----------|--|------------|
| 19.11     | Алгоритм ECDH . . . . .                                | 400        |
| <b>20</b> | <b>Теория алгоритмов</b>                               | <b>401</b> |
| 20.1      | Основная теорема о рекуррентных соотношениях . . . . . | 401        |
| 20.2      | Разделяй и властвуй . . . . .                          | 401        |
| 20.3      | Булева логика. Булевы формулы КНФ . . . . .            | 401        |
| 20.4      | Машина Тьюринга . . . . .                              | 403        |
| 20.5      | Теория вычислимости . . . . .                          | 405        |
| 20.6      | Классы сложности $P$ , $NP$ . . . . .                  | 411        |
| 20.6.1    | Иерархия классов сложности . . . . .                   | 413        |
| 20.6.2    | Теорема Кука-Левина . . . . .                          | 414        |
| <b>6</b>  | <b>Ответы на вопросы</b>                               | <b>417</b> |
| <b>21</b> | <b>Квантовая электродинамика</b>                       | <b>419</b> |
| 21.1      | Квантование электромагнитного поля . . . . .           | 419        |
| 21.1.1    | 5: Число мод . . . . .                                 | 419        |
| 21.2      | Взаимодействие света с атомом . . . . .                | 419        |
| 21.2.1    | 13: Определение частоты перехода атома лития . . . . . | 419        |
| <b>22</b> | <b>Квантовая оптика</b>                                | <b>423</b> |
| 22.1      | Квантовая теория лазера . . . . .                      | 423        |
| 22.1.1    | 6: Естественная ширина линии . . . . .                 | 423        |

# Введение

Квантовая оптика изучает оптические явления, в которых проявляется квантовая сущность света. Можно сказать, что квантовая оптика рассматривает оптические явления, при которых свет и взаимодействующую с ним систему необходимо описывать квантовыми уравнениями.

В квантовой оптике рассматривается область частот примерно от  $f_1 \simeq 10^{13}$  Гц до  $f_2 \simeq 10^{18}$  Гц, т. е. от инфракрасного диапазона до рентгеновского. Нижний предел определяется условием превышения энергией кванта энергии теплового движения:  $\omega_1 \hbar > kT$ . Верхний предел устанавливается исходя из того, что в квантовой оптике рассматриваются, как правило, нерелятивистские энергии электронов и, следовательно, энергия кванта должна быть заметно меньше, чем энергия покоя электрона:  $\omega_2 \hbar \ll mc^2$ .

В настоящее время существует мало учебных материалов посвященных квантовой оптике. Из отечественных стоит отметить [51]. Предлагаемый материал отражает ряд вопросов квантовой теории света, излагаемых в курсе “Квантовая оптика”. Пособие состоит из трех частей.

В первой части пособия дается введение в квантовую электродинамику. Рассматриваются простейшие задачи, связанные с взаимодействием светового поля и вещества. На простейшей модели строится квантовая теория лазера. Рассматривается квантовое описание когерентности света и ее связь с классическим описанием. В главе 1 дается краткое введение в квантовую электродинамику в объеме, необходимом для изложения курса квантовой оптики. Рассматриваются различные квантовые состояния светового поля, применяемые в квантовой оптике. Особое внимание уделяется когерентным состояниям, позволяющим максимально приблизить квантовое описание оптических явлений к классическому. В главе 2 рассматриваются простейшие задачи для светового поля, связанного как с отдельными атомами, так и с большим числом атомов, находящихся в тепловом равновесии. Особое внимание уделяется связи поля с термостатом, приводящей к релаксационным процессам, играющим важную роль в квантовой оптике и квантовой электронике.

Во второй части пособия рассмотрены некоторые прикладные вопросы квантовой оптики. В 3 главе на простой модели рассматривается квантовая теория лазера. Получено выражение для статистики лазерных фотонов и

формула, оценивающая “естественную” ширину линии генерации лазера. В 4 главе рассматривается квантовая теория лазера в представлении Гейзенберга.

5 глава посвящена оптике фотонов. Излагается квантовое описание когерентности света и его связь с классическим описанием, функции когерентности различных порядков, проблема статистики фотонов и ее связь со статистикой фото-отсчетов (формула Манделя). Приводятся многочисленные примеры. Далее рассматривается связь статистики фотонов со спектральными свойствами световых пучков и ее применение для спектральных измерений.

В 6 главе дается квантовое описание интерферометрических экспериментов. Рассматривается интерферометр Маха-Цендера и погрешность интерференционных измерений. В дальнейшем в главе 9 будет показано как повысить точность измерений с помощью сжатых состояний.

Глава 7 посвящена квантовому описанию поляризационных свойств света. В дальнейшем этот материал используется при описании перепутанных состояний в главе 10.

В третьей части пособия обсуждаются неклассические состояния света. Дано определение неклассического состояния (см. гл. 8). Описаны сжатые (гл. 9) и перепутанные (см. гл. 10) неклассические состояния света. Для каждого типа неклассического состояния дается определение, способы получения, применение и доказываемая неклассичность.

В четвертой части пособия рассмотрена квантовая теория информации. В частности в главе 11 дано введение в квантовую теорию информации. Определено понятие количества информации в классическом и квантовом случае. Рассмотрена классическая теорема кодирования Шенона и ее квантовый аналог. Глава 12 посвящена теории защиты информации (криптографии): описана классическая теория криптографии и ее основные недостатки. Приведено описание квантовой криптографии. Глава 13 описывает основные квантовые алгоритмы: алгоритм Шора для факторизации целых чисел и алгоритм Гровера для поиска в неструктурированном массиве данных.

В приложениях собран материал который дополняет основной курс и носит в основном справочный характер, позволяющий не прибегать к специальной литературе.

Пособие предназначено для студентов старших курсов, специализирующихся в области квантовой электроники.

## Часть 1

# Квантовая электродинамика



# Глава 1

## Квантование электромагнитного поля

Квантовая электродинамика служит основой квантовой оптики. Ниже излагаются положения квантовой теории электромагнитного поля, необходимые для изучения и понимания квантовой оптики.

### 1.1 Разложение электромагнитного поля по модам (типам колебаний)

Электромагнитное поле удовлетворяет системе уравнений Максвелла:

$$\operatorname{rot} \vec{H} = \frac{\partial \vec{D}}{\partial t} + \vec{j}, \quad \operatorname{rot} \vec{E} = -\frac{\partial \vec{B}}{\partial t}, \quad \operatorname{div} \vec{D} = \rho, \quad \operatorname{div} \vec{B} = 0. \quad (1.1)$$

В свободном пространстве ( $\vec{j} = 0$ ,  $\rho = 0$ ) имеем более простую систему:

$$\begin{aligned} \operatorname{rot} \vec{H} &= \varepsilon_0 \frac{\partial \vec{E}}{\partial t}, & \operatorname{rot} \vec{E} &= -\mu_0 \frac{\partial \vec{H}}{\partial t}, \\ \operatorname{div} \vec{H} &= 0, & \operatorname{div} \vec{E} &= 0, \\ \vec{B} &= \mu_0 \vec{H}, & \vec{D} &= \varepsilon_0 \vec{E}, & \mu_0 \varepsilon_0 &= \frac{1}{c^2}. \end{aligned} \quad (1.2)$$

Исключив из (1.2) величину  $\vec{H}$ , получим уравнение:

$$\operatorname{rot} \operatorname{rot} \vec{E} = -\mu_0 \frac{\partial}{\partial t} \operatorname{rot} \vec{H} = -\varepsilon_0 \mu_0 \frac{\partial^2 \vec{E}}{\partial t^2} = -\frac{1}{c^2} \frac{\partial^2 \vec{E}}{\partial t^2}.$$

С учетом  $\operatorname{rot} \operatorname{rot} \vec{E} = \operatorname{grad} \operatorname{div} \vec{E} - \Delta \vec{E} = -\Delta \vec{E}$ <sup>1</sup> получим следующую систему

---

<sup>1</sup>при условии  $\operatorname{div} \vec{E} = 0$

$$\begin{aligned}
\Delta \vec{E} - \frac{1}{c^2} \frac{\partial^2 \vec{E}}{\partial t^2} &= 0; \\
\operatorname{div} \vec{E} &= 0, \quad \frac{\partial H}{\partial t} = -\frac{1}{\mu_0} \operatorname{rot} \vec{E} \\
\vec{B} &= \mu_0 \vec{H}, \quad \vec{D} = \varepsilon_0 \vec{E}, \quad \mu_0 \varepsilon_0 = \frac{1}{c^2}.
\end{aligned} \tag{1.3}$$

которая полностью эквивалентна исходной системе уравнений.

Для квантования электромагнитного поля его уравнения удобно представить в так называемом гамильтоновом виде. Суть метода, хорошо известная радиофизикам, заключается в том, что поле разлагается по модам, и решение уравнений сводится к решению системы обыкновенных дифференциальных уравнений для коэффициентов разложения, зависящих от времени. Для этой цели вводится система ортогональных векторных функций, являющихся распределением полей, соответствующих собственным колебаниям электромагнитного поля в некотором объеме  $V$ , ограниченном идеально проводящей поверхностью  $S$ . Поля должны удовлетворять системе уравнений (1.3). На поверхности  $S$  должны выполняться некоторые граничные условия, например:

$$\left[ \vec{n} \vec{E} \right] \Big|_S = 0 \text{ или } \left( \vec{n} \vec{H} \right) \Big|_S = 0, \tag{1.4}$$

соответствующие идеально проводящей поверхности.

Произвольное в объеме  $V$  электромагнитное поле представляется разложениями:

$$\vec{E}(r, t) = \sum_{(n)} Q_n(t) \vec{E}_n(r), \quad \vec{H}(r, t) = \sum_{(n)} P_n(t) \vec{H}_n(r), \tag{1.5}$$

где  $Q_n(t) \vec{E}_n(r)$  и  $P_n(t) \vec{H}_n(r)$  - частные решения уравнений, удовлетворяющие граничным условиям (1.4);  $\vec{E}_n(r)$  и  $\vec{H}_n(r)$  соответствуют  $n$ -ому типу колебаний в объеме  $V$  (моды). Из уравнений (1.3) имеем:

$$Q_n(t) \Delta \vec{E}_n(r) = \frac{1}{c^2} \frac{d^2 Q_n}{dt^2} \vec{E}_n(r). \tag{1.6}$$

Разделяя переменные, получаем:

$$\frac{d^2 Q_n}{dt^2} + \omega_n^2 Q_n = 0, \quad \Delta \vec{E}_n(r) = -\frac{\omega_n^2}{c^2} \vec{E}_n(r) \tag{1.7}$$

где  $\omega_n$  постоянная разделения, являющаяся частотой собственных колебаний.



Второе из уравнений (1.7) имеет следующий вид:

$$\Delta \vec{E}_n(r) + k_n^2 \vec{E}_n(r) = 0, \quad k_n^2 = \frac{\omega_n^2}{c^2}, \quad (1.8)$$

с граничными условиями  $\left[ \vec{n} \vec{E}_n \right] \Big|_S = 0$ . Эта задача имеет решение только при определенных значениях  $k_n(\omega_n)$ .

Для определения  $\vec{H}_n(r)$  воспользуемся уравнениями (1.3):

$$Q_n(t) \operatorname{rot} \vec{E}_n(r) = -\mu_0 \frac{dP_n}{dt} \vec{H}_n(r). \quad (1.9)$$

Прежде всего сделаем следующую подстановку:

$$Q_n(t) = \frac{\omega_n}{\sqrt{\varepsilon_0}} q_n(t), \quad P_n(t) = \frac{1}{\sqrt{\mu_0}} p_n(t). \quad (1.10)$$

Для новой переменной  $q_n$  очевидно имеем из (1.7)

$$\frac{d^2 q_n}{dt^2} + \omega_n^2 q_n = 0.$$

Разложение (1.5) в новых переменных имеет вид:

$$\vec{E}(r, t) = \sum_{(n)} \frac{q_n(t) \omega_n}{\sqrt{\varepsilon_0}} \vec{E}_n(r), \quad \vec{H}(r, t) = \sum_{(n)} \frac{p_n(t)}{\sqrt{\mu_0}} \vec{H}_n(r), \quad (1.11)$$

С учетом подстановки (1.10) и выражения для скорости света  $c = \frac{1}{\sqrt{\varepsilon_0 \mu_0}}$  (1.2) мы можем переписать (1.9) в следующем виде

$$q_n(t) \operatorname{rot} \vec{E}_n(r) = -\frac{1}{c \omega_n} \frac{dp_n(t)}{dt} \vec{H}_n(r) \quad (1.12)$$

Уравнения (1.12) будут удовлетворены, если

$$p_n = \frac{dq_n}{dt}, \quad \frac{dp_n}{dt} = \frac{d^2 q_n}{dt^2} = -\omega_n^2 q_n,$$

тогда

$$\begin{aligned} \operatorname{rot} \vec{E}_n(r) &= k_n \vec{H}_n(r), \\ \vec{H}_n(r) &= \frac{1}{k_n} \operatorname{rot} \vec{E}_n(r) \end{aligned} \quad (1.13)$$

Из курса “Электромагнитные колебания” известно, что система функций  $\vec{E}_n(r)$ ,  $\vec{H}_n(r)$  ортогональна и может быть нормирована:

$$\int_{\nu} (\vec{E}_n \vec{E}_m) d\nu = \delta_{nm}, \quad \int_{\nu} (\vec{H}_n \vec{H}_m) d\nu = \delta_{nm}, \quad \int_{\nu} (\vec{H}_n \vec{E}_m) d\nu = 0. \quad (1.14)$$

Решение исходной электродинамической задачи сводится к нахождению коэффициентов  $q_n(t)$ ,  $p_n(t)$  в разложениях (1.11).

## 1.2 Гамильтонова форма уравнений свободного электромагнитного поля

Представим поле в объеме  $V$  в виде разложений (1.11):

$$\vec{E}(r, t) = \sum_{(n)} \frac{q_n(t) \omega_n}{\sqrt{\varepsilon_0}} \vec{E}_n(r), \quad \vec{H}(r, t) = \sum_{(n)} \frac{p_n(t)}{\sqrt{\mu_0}} \vec{H}_n(r), \quad (1.15)$$

причем  $p_n = \frac{dq_n}{dt}$ , а  $q_n$  удовлетворяет уравнению

$$\frac{d^2 q_n}{dt^2} + \omega_n^2 q_n = 0.$$

Это уравнение гармонического осциллятора. Его решение:

$$q_n(t) = q_n(0) \cos \omega_n t + \frac{\dot{q}_n(0)}{\omega_n} \sin \omega_n t \quad (1.16)$$

$q_n(0)$  и  $\dot{q}_n(0)$  определяются из разложения начального поля по  $\vec{E}_n$ ,  $\vec{H}_n$ .

Запишем теперь уравнения электродинамики в гамильтоновой форме. Функция Гамильтона для электромагнитного поля (энергия поля)

$$\mathcal{H} = \frac{1}{2} \int_{\nu} \left( \varepsilon_0 (\vec{E})^2 + \mu_0 (\vec{H})^2 \right) d\nu \quad (1.17)$$

Подставляя в (1.17) разложения (1.15) и используя ортогональность собственных функций, получим

$$\begin{aligned} \mathcal{H} &= \frac{1}{2} \int_{\nu} \left( \sum_{(n)} \sum_{(m)} \varepsilon_0 \frac{q_n q_m \omega_n \omega_m}{\varepsilon_0} (\vec{E}_n \vec{E}_m) \right) d\nu + \\ &\quad + \frac{1}{2} \int_{\nu} \left( \sum_{(n)} \sum_{(m)} \mu_0 \frac{p_n p_m}{\mu_0} (\vec{H}_n \vec{H}_m) \right) d\nu = \\ &= \frac{1}{2} \sum_{(n)} (\omega_n^2 q_n^2 + p_n^2). \end{aligned} \quad (1.18)$$

Это выражение соответствует функции Гамильтона для совокупности независимых гармонических осцилляторов.

Для одной моды функция Гамильтона

$$\mathcal{H}_n = \frac{1}{2} (\omega_n^2 q_n^2 + p_n^2). \quad (1.19)$$

тогда

$$\mathcal{H} = \sum_{(n)} \mathcal{H}_n \quad (1.20)$$

Уравнения движения получим из функции Гамильтона известным путем (1.4.49):

$$\dot{q}_n = \frac{\partial \mathcal{H}_n}{\partial p_n} = p_n, \quad \dot{p}_n = -\frac{\partial \mathcal{H}_n}{\partial q_n} = -\omega_n^2 q_n = \ddot{q}_n. \quad (1.21)$$

Полученные уравнения совпадают с уравнениями (1.7). Функция Гамильтона механического осциллятора

$$\mathcal{H} = \frac{1}{2} \left( M \Omega^2 x^2 + \frac{p^2}{M} \right)$$

Следовательно, (1.19) формально соответствует осциллятору с единичной массой и собственной частотой  $\omega_n$ . Гамильтонова запись уравнений электромагнитного поля удобна для процедуры квантования поля. Этот подход во многих случаях пригоден и для решения различных классических задач. Подробнее с этим можно познакомиться в книге [38].

### 1.3 Квантование свободного электромагнитного поля

Используя отмеченную ранее аналогию, можно проквантовать электромагнитное поле подобно тому, как квантуется простой механический гармонический осциллятор.

При квантовании  $q_n$  и  $p_n$  становятся операторами  $\hat{q}_n$ ,  $\hat{p}_n$ , удовлетворяющими тем же коммутационным соотношениям, что координата и импульс:

$$[\hat{q}_n, \hat{p}_n] = \hat{q}_n \hat{p}_n - \hat{p}_n \hat{q}_n = i\hbar \quad (1.22)$$

где  $\hat{q}_n$  и  $\hat{p}_n$  - эрмитовы (самосопряженные) операторы. В представлении Шредингера они не зависят от времени, в представлении Гейзенберга - зависят.

Удобно через эти операторы ввести новые, не являющиеся самосопряженными, но сопряженные друг другу операторы:

$$\hat{a}_n = \frac{1}{\sqrt{2\hbar\omega_n}} (\omega_n \hat{q}_n + i\hat{p}_n), \quad \hat{a}_n^\dagger = \frac{1}{\sqrt{2\hbar\omega_n}} (\omega_n \hat{q}_n - i\hat{p}_n), \quad (1.23)$$

Обратная зависимость дает

$$\hat{q}_n = \sqrt{\frac{\hbar}{2\omega_n}} (\hat{a}_n + \hat{a}_n^\dagger), \quad \hat{p}_n = i\sqrt{\frac{\hbar\omega_n}{2}} (\hat{a}_n^\dagger - \hat{a}_n), \quad (1.24)$$

При помощи выражений (1.22), (1.23), (1.24) можно получить коммутационные соотношения для операторов  $\hat{a}_n$  и  $\hat{a}_n^\dagger$ :

$$\begin{aligned} [\hat{a}_n, \hat{a}_n^\dagger] &= \frac{1}{2\hbar\omega_n} (\omega_n \hat{q}_n + i\hat{p}_n) (\omega_n \hat{q}_n - i\hat{p}_n) - \\ &\quad - \frac{1}{2\hbar\omega_n} (\omega_n \hat{q}_n - i\hat{p}_n) (\omega_n \hat{q}_n + i\hat{p}_n) = \\ &= \frac{1}{2\hbar\omega_n} (-2i\omega_n (\hat{q}_n \hat{p}_n - \hat{p}_n \hat{q}_n)) = 1. \end{aligned} \quad (1.25)$$

Таким образом,

$$[\hat{a}_n, \hat{a}_n^\dagger] = 1. \quad (1.26)$$

Кроме того очевидно, что

$$[\hat{a}_n, \hat{a}_n] = 0, \quad [\hat{a}_n^\dagger, \hat{a}_n^\dagger] = 0. \quad (1.27)$$

Гамильтониан, выраженный через новые операторы, принимает вид

$$\begin{aligned} \hat{\mathcal{H}}_n &= \frac{1}{2} (\omega_n^2 \hat{q}_n^2 + \hat{p}_n^2) = \\ &= \frac{1}{2} \frac{\omega_n \hbar}{2} ((\hat{a}_n + \hat{a}_n^\dagger) (\hat{a}_n + \hat{a}_n^\dagger) - (\hat{a}_n^\dagger - \hat{a}_n) (\hat{a}_n^\dagger - \hat{a}_n)) = \\ &= \frac{\omega_n \hbar}{2} (\hat{a}_n \hat{a}_n^\dagger + \hat{a}_n^\dagger \hat{a}_n) = \frac{\omega_n \hbar}{2} (1 + \hat{a}_n^\dagger \hat{a}_n + \hat{a}_n^\dagger \hat{a}_n) = \\ &= \omega_n \hbar \left( \hat{a}_n^\dagger \hat{a}_n + \frac{1}{2} \right) \end{aligned} \quad (1.28)$$

Здесь использованы связь  $\hat{q}_n, \hat{p}_n$  с  $\hat{a}_n^\dagger, \hat{a}_n$  (1.23), а также коммутационное соотношение (1.26).

Энергия  $\frac{1}{2}\omega_n \hbar$  соответствует нулевым колебаниям. Полная энергия нулевых колебаний

$$\frac{1}{2} \sum_{(n)} \omega_n \hbar \rightarrow \infty,$$



Рис. 1.1: Электромагнитное поле в резонаторе образованном двумя зеркалами. Длина резонатора  $L$ . Волновой вектор электромагнитного поля направлен по оси  $z$ , электрическое поле по оси  $x$ , а магнитное поле по оси  $y$ .

так как число мод бесконечно. Это не приводит к заметным трудностям, так как нас интересуют только разности энергий и постоянную часть можно отбросить. Тогда гамильтониан приобретает вид

$$\hat{\mathcal{H}} = \sum_{(n)} \hat{\mathcal{H}}_n = \sum_{(n)} \hbar \omega_n \hat{a}_n^\dagger \hat{a}_n \quad (1.29)$$

Операторы электрического и магнитного поля можно представить в виде

$$\begin{aligned} \hat{\vec{E}} &= \sum_{(n)} \frac{\hat{q}_n \omega_n}{\sqrt{\varepsilon_0}} \vec{E}_n(r) = \sum_{(n)} \sqrt{\frac{\hbar \omega_n}{2\varepsilon_0}} (\hat{a}_n^\dagger + \hat{a}_n) \vec{E}_n(r), \\ \hat{\vec{H}} &= \sum_{(n)} \frac{\hat{p}_n}{\sqrt{\mu_0}} \vec{H}_n(r) = i \sum_{(n)} \sqrt{\frac{\hbar \omega_n}{2\mu_0}} (\hat{a}_n^\dagger - \hat{a}_n) \vec{H}_n(r). \end{aligned} \quad (1.30)$$

Приведем простой пример. В теории лазера рассматривают резонатор, образованный двумя параллельными зеркалами. При этом часто используют приближенное представление поля, считая, что поле зависит только от продольной координаты (рис. 1.1). В этом приближении нормированную собственную функцию (моду) можно представить следующим образом:

$$E_{nx} = \sqrt{\frac{2}{V}} \sin k_n z, \quad H_{ny} = \sqrt{\frac{2}{V}} \cos k_n z, \quad k_n = \frac{\pi n}{L}, \quad \omega_n = \frac{c\pi n}{L}, \quad (1.31)$$

где  $V = SL$ ,  $L$  - длина резонатора,  $S$  - сечение светового пучка.

Оператор электрического поля моды при этом будет иметь вид:

$$\begin{aligned}\hat{E}_{nx} &= \sqrt{\frac{\hbar\omega_n}{2\varepsilon_0}} (\hat{a}_n^\dagger + \hat{a}_n) \sqrt{\frac{2}{V}} \sin k_n z = E_1 (\hat{a}_n^\dagger + \hat{a}_n) \sin k_n z, \\ \hat{H}_{ny} &= iE_1 \sqrt{\frac{\varepsilon_0}{\mu_0}} (\hat{a}_n^\dagger - \hat{a}_n) \cos k_n z,\end{aligned}\quad (1.32)$$

где  $E_1 = \sqrt{\frac{\hbar\omega}{\varepsilon_0 V}}$  - электрическое поле, соответствующее одному фотону (кванту) в моде.

## 1.4 Разложение поля по плоским волнам в свободном пространстве

До сих пор мы рассматривали электромагнитное поле в физически выделенном объеме - в резонаторе. Если мы имеем дело со свободным пространством, можно искусственно выделить достаточно большой объем, содержащий интересующую нас область пространства, определить для него моды (типы колебаний) при подходящих граничных условиях, а дальше действовать уже рассмотренным способом. При необходимости объем в конечном результате можно устремить в бесконечность. Обычно используют достаточно большой кубический объем со стороной  $L$  (рис. 1.2). В этом случае принято использовать периодические граничные условия:

$$\begin{aligned}\vec{E}(0, y, z) &= \vec{E}(L, y, z), \\ \vec{E}(x, 0, z) &= \vec{E}(x, L, z), \\ \vec{E}(x, y, 0) &= \vec{E}(x, y, L).\end{aligned}\quad (1.33)$$

Удобно вести разложение по плоским волнам. Как известно из курса электромагнитных колебаний, решение, соответствующее плоской волне, имеет вид

$$\vec{E}_k(r, t) = A_k(t) \vec{e}_k e^{i(\vec{k}\vec{r})} + (\text{к. с.}), \quad (1.34)$$

где  $\vec{e}_k$  - единичный вектор поляризации волны;  $k$  - волновое число;  $\vec{k}$  - волновой вектор;  $A_k(t) = A_k(0) e^{-i\omega_k t}$ .

Магнитное поле связано с электрическим полем соотношением

$$\vec{H}_k(r, t) = \sqrt{\frac{\varepsilon_0}{\mu_0}} \frac{1}{k} [\vec{k} \vec{e}_k] A_k(t) e^{i(\vec{k}\vec{r})} + (\text{к. с.}). \quad (1.35)$$



Рис. 1.2: Разложение электромагнитного поля по плоским волнам в свободном пространстве. Область пространства в которой производится разложение выбрана в виде куба со стороной  $L$ . На границе куба используются периодические граничные условия.

Справедливы следующие равенства:

$$\left(\vec{k}\vec{E}_k\right) = \left(\vec{k}\vec{H}_k\right) = \left(\vec{E}_k\vec{H}_k\right) = 0, \quad k^2 = \left(\vec{k}\vec{k}\right) = \frac{\omega_k^2}{c^2} \quad (1.36)$$

указывающие, что  $\vec{E}_k$  и  $\vec{H}_k$  перпендикулярны направлению распространения волны и друг к другу (волна поперечная).

Условие периодичности (1.33) будет удовлетворено, если

$$\vec{k} = \frac{2\pi}{L} (n_x \vec{x}_0 + n_y \vec{y}_0 + n_z \vec{z}_0), \quad n_x, n_y, n_z = 0, \pm 1, \pm 2, \dots \quad (1.37)$$

Тогда получим

$$\begin{aligned} \left(\vec{k}\vec{r}\right) &= \frac{2\pi}{L} (n_x x + n_y y + n_z z), \\ \left(\vec{k}\vec{r}\right)\Big|_{x=L} &= 2\pi n_x + \frac{2\pi}{L} (n_y y + n_z z) = 2\pi n_x + \left(\vec{k}\vec{r}\right)\Big|_{x=0}. \end{aligned} \quad (1.38)$$

Следовательно,  $e^{i(\vec{k}\vec{r})}$  периодически по  $x$ . Таким же образом показывается периодичность по  $y$  и  $z$ .

В дальнейшем вместо вещественных функций (1.34), (1.35) будем пользоваться комплексными собственными функциями

$$\vec{E}_k(r) = \vec{e}_k e^{i(\vec{k}\vec{r})}, \quad \vec{H}_k(r) = \sqrt{\frac{\varepsilon_0}{\mu_0}} \frac{1}{k} \left[ \vec{k} \vec{E}_k(r) \right]. \quad (1.39)$$

Справедливы соотношения

$$\left(\vec{k}\vec{E}_k\right) = \left(\vec{k}\vec{H}_k\right) = \left(\vec{E}_k\vec{H}_k\right) = 0, \quad k^2 = \left(\vec{k}\vec{k}\right) = \frac{\omega_k^2}{c^2}.$$

Собственные частоты  $\omega_k$  определяются уравнением (1.37). Действительно из (1.37) с учетом  $k^2 = \frac{\omega_k^2}{c^2}$  имеем

$$\omega_k = c\sqrt{k_x^2 + k_y^2 + k_z^2} = \frac{2\pi c}{L}\sqrt{n_x^2 + n_y^2 + n_z^2}. \quad (1.40)$$

При линейной поляризации векторы поляризации  $\vec{e}_k$  равны:

$$\vec{e}_{k_1} = \vec{\xi}_0, \quad \vec{e}_{k_2} = \vec{\eta}_0,$$

где  $\vec{\xi}_0, \vec{\eta}_0$ , - орты направлений, составляющих с вектором  $\vec{k}$  прямоугольную систему направлений, следовательно,

$$\left(\vec{\xi}_0\vec{k}\right) = \left(\vec{\eta}_0\vec{k}\right) = (\vec{e}_{k_1}\vec{e}_{k_2}) = 0.$$

Для круговой поляризации

$$\vec{e}_{k_1} = \frac{\vec{\xi}_0 + i\vec{\eta}_0}{\sqrt{2}}, \quad \vec{e}_{k_2} = \frac{\vec{\xi}_0 - i\vec{\eta}_0}{\sqrt{2}}.$$

В этом случае выполняются условие ортогональности:  $(\vec{e}_{k_1}\vec{e}_{k_2}^*)$  и условия нормировки:  $(\vec{e}_{k_1}\vec{e}_{k_1}^*) = (\vec{e}_{k_2}\vec{e}_{k_2}^*) = 1$ .

Произвольное электромагнитное поле при помощи комплексных функций (1.39) можно представить разложениями

$$\begin{aligned} \vec{E}(r, t) &= \sum_{(k)} A_k(t) \vec{E}_k(r) + (\text{к. с.}), \\ \vec{H}(r, t) &= \sum_{(k)} A_k(t) \vec{H}_k(r) + (\text{к. с.}) \end{aligned} \quad (1.41)$$

## 1.5 Плотность состояний

Если объем квантования  $L^3$  велик, плотность состояний (число мод, входящих на единичный интервал частот) будет весьма большой. Волновой вектор моды определяется соотношением (1.37)

$$\vec{k}_{n_x, n_y, n_z} = \frac{2\pi}{L} (n_x \vec{x}_0 + n_y \vec{y}_0 + n_z \vec{z}_0) \quad (1.42)$$





Рис. 1.3: Разрешенные моды электромагнитного поля (обозначены точками) для ограниченной области пространства в виде куба со стороной  $L$ . Прямоугольная система координат.

Каждому набору целых чисел соответствуют две волны, отличающиеся поляризацией. Моды можно представить наглядно точками в декартовой системе координат, по осям которой отложены  $n_x, n_y, n_z$  (рис. 1.3). Число колебаний в объеме  $\Delta n_x \Delta n_y \Delta n_z$ , очевидно, составит  $\Delta N = 2\Delta n_x \Delta n_y \Delta n_z$ , или, с учетом связи между  $k$  и  $n$  (1.37),

$$\Delta N = 2 \left( \frac{L}{2\pi} \right)^3 \Delta k_x \Delta k_y \Delta k_z. \quad (1.43)$$

Двойка в формуле (1.43) появляется из-за того, что одному значению  $k$  соответствуют две моды с различными поляризациями. При большом  $L$  ( $L \rightarrow \infty$ ) распределение квазинепрерывно и суммирование по модам, которое почти всегда требуется при решении задач квантовой оптики, можно заменить интегрированием по  $k$ :

$$2 \sum_{(n)} (\dots) = 2 \left( \frac{L}{2\pi} \right)^3 \iiint_{-\infty}^{+\infty} (\dots) dk_x dk_y dk_z. \quad (1.44)$$

Переход от прямоугольных координат  $k_x, k_y, k_z$  к сферическим координатам  $k, \theta, \varphi$  (рис. 1.4), дает

$$\begin{aligned} k_x &= k \sin \theta \cos \varphi, & k_y &= k \sin \theta \sin \varphi, & k_z &= k \cos \theta, \\ dk_x dk_y dk_z &= k^2 \sin \theta dk d\theta d\varphi = k^2 dk d\Omega, \end{aligned} \quad (1.45)$$

где  $d\Omega = \sin \theta d\theta d\varphi$  элемент телесного угла в направлении  $\vec{k}$ . Таким образом,



Рис. 1.4: Разрешенные моды электромагнитного поля (обозначены точками) для ограниченной области пространства в виде куба со стороной  $L$ . Сферическая система координат.

получим

$$dN = 2 \left( \frac{L}{2\pi} \right)^3 k^2 dk d\Omega \quad (1.46)$$

или, учитывая, что  $k^2 c^2 = \omega^2$  т. е.  $k^2 dk = \frac{\omega^2 d\omega}{c^3}$ :

$$dN = 2 \left( \frac{L}{2\pi c} \right)^3 \omega^2 d\omega d\Omega \quad (1.47)$$

т.е. число состояний, приходящихся на единицу объема, единицу частоты и единицу телесного угла

$$g(\omega) = \frac{2\omega^2}{(2\pi c)^3} \quad (1.48)$$

(спектральная плотность собственных состояний).

## 1.6 Гамильтонова форма уравнений поля при разложении по плоским волнам

Собственные функции (1.39) ортогональны, т.е.

$$\begin{aligned} \int_{\nu} \left( \vec{E}_k \vec{E}_{k'}^* \right) d\nu &= C \int_{\nu} e^{i(\vec{k}\vec{r})} e^{-i(\vec{k}'\vec{r})} d\nu = \\ &= C \int_0^L dx \int_0^L dy \int_0^L dz \left[ e^{i((k_x - k'_x)x + (k_y - k'_y)y + (k_z - k'_z)z)} \right] = 0, \end{aligned} \quad (1.49)$$

если справедливо хотя бы одно из неравенств  $k_x \neq k'_x$ ,  $k_y \neq k'_y$ ,  $k_z \neq k'_z$ , (или  $\vec{k} - \vec{k}' \neq 0$ ). Это следует из периодичности подинтегральных функций.

Аналогично получим:

$$\int_{\nu} \left( \vec{E}_k \vec{E}_{k'} \right) d\nu = 0, \quad \vec{k} \neq -\vec{k}'. \quad (1.50)$$

Собственные функции  $\vec{E}_k$  можно нормировать, положив

$$\int_{\nu} \left( \vec{E}_k \vec{E}_k^* \right) d\nu = 1. \quad (1.51)$$

Тогда собственные функции будут иметь вид

$$\vec{E}_k(r) = \frac{1}{\sqrt{\nu}} \vec{e}_k e^{i(\vec{k}\vec{r})}, \quad \vec{H}_k(r) = \frac{1}{k} \left[ \vec{k} \vec{e}_k(r) \right] \sqrt{\frac{\varepsilon_0}{\nu \mu_0}} e^{i(\vec{k}\vec{r})}.$$

Заметим, что под индексом  $k$  мы подразумеваем  $k_j$ , где  $j = 1, 2$  соответствуют двум различным поляризациям. Функции  $\vec{E}_k$  и  $\vec{H}_k$ , записанные в таком виде, удовлетворяют следующим условиям ортогональности и нормировки:

$$\begin{aligned} \int_{\nu} \left( \vec{E}_k \vec{E}_{k'}^* \right) d\nu &= 0 \quad \text{при } \vec{k} \neq \vec{k}', \\ \int_{\nu} \left( \vec{E}_k \vec{E}_{k'} \right) d\nu &= 0 \quad \text{при } \vec{k} \neq -\vec{k}', \\ \int_{\nu} \left( \vec{E}_k \vec{E}_k^* \right) d\nu &= 1, \quad \int_{\nu} \left( \vec{E}_k \vec{E}_{-k} \right) d\nu = 1, \\ \int_{\nu} \left( \vec{H}_k \vec{H}_{k'}^* \right) d\nu &= 0 \quad \text{при } \vec{k} \neq \vec{k}', \\ \int_{\nu} \left( \vec{H}_k \vec{H}_{k'} \right) d\nu &= 0 \quad \text{при } \vec{k} \neq -\vec{k}', \\ \int_{\nu} \left( \vec{H}_k \vec{H}_k^* \right) d\nu &= \frac{\varepsilon_0}{\mu_0}, \quad \int_{\nu} \left( \vec{H}_k \vec{H}_{-k} \right) d\nu = -\frac{\varepsilon_0}{\mu_0}. \end{aligned} \quad (1.52)$$

Ортогональность мод с одинаковым значением  $k$ , но разными поляризациями следует из равенств:

$$(\vec{e}_{k_1} \vec{e}_{k_2}^*) = 0, \quad (\vec{e}_{k_1} \vec{e}_{-k_2}) = 0.$$

Электрическое и магнитное поля выражаются через эти функции при помощи разложения:

$$\begin{aligned} \vec{E}(r, t) &= \sum_{(k)} A_k(t) \vec{E}_k(r) + \text{к. с.}, \\ \vec{H}(r, t) &= \sum_{(k)} A_k(t) \vec{H}_k(r) + \text{к. с.} \end{aligned} \quad (1.53)$$

Суммирование по  $k = k_j$  подразумевает суммирование по всем значениям  $k$  и двум поляризациям ( $j = 1, 2$ ):  $\sum_{(k)} \equiv \sum_{j=1,2} \sum_{(k_j)}$ .

Функция Гамильтона электромагнитного поля имеет вид:

$$\mathcal{H} = \frac{1}{2} \int_{\nu} \left( \varepsilon_0 \left( \vec{E}(r, t) \right)^2 + \mu_0 \left( \vec{H}(r, t) \right)^2 \right) d\nu \quad (1.54)$$

Подставляя в (1.54) ряды (1.53), перемножая их и учитывая условия ортогональности и нормировки, получим

$$\begin{aligned} \mathcal{H} = & \frac{1}{2} \varepsilon_0 \int_{(\nu)} \left\{ \sum_{(k)} \sum_{(k')} \left( A_k \vec{E}_k + A_k^* \vec{E}_k^* \right) \left( A_{k'} \vec{E}_{k'} + A_{k'}^* \vec{E}_{k'}^* \right) \right\} d\nu + \\ & + \frac{1}{2} \mu_0 \int_{(\nu)} \left\{ \sum_{(k)} \sum_{(k')} \left( A_k \vec{H}_k + A_k^* \vec{H}_k^* \right) \left( A_{k'} \vec{H}_{k'} + A_{k'}^* \vec{H}_{k'}^* \right) \right\} d\nu = \\ & \frac{\varepsilon_0}{2} \sum_{(k)} \left( A_k A_k^* + A_k A_{-k} + A_k^* A_{-k}^* + A_k^* A_k + \right. \\ & \left. + A_k A_k^* - A_k A_{-k} - A_k^* A_{-k}^* + A_k^* A_k \right) = \varepsilon_0 \sum_{(k)} \left( A_k A_k^* + A_k^* A_k \right). \quad (1.55) \end{aligned}$$

## 1.7 Квантование электромагнитного поля при разложении его по плоским волнам

Для квантования электромагнитного поля в этом случае обратим внимание на аналогию (1.55) и (1.28):

$$\hat{\mathcal{H}}_n = \frac{\omega_n \hbar}{2} \left( \hat{a}_n \hat{a}_n^\dagger + \hat{a}_n^\dagger \hat{a}_n \right) = \omega_n \hbar \left( \hat{a}_n^\dagger \hat{a}_n + \frac{1}{2} \right)$$

и

$$\mathcal{H} = \varepsilon_0 \sum_{(k)} \left( A_k A_k^* + A_k^* A_k \right).$$

Из этой аналогии следует, что можно использовать следующую процедуру квантования:

$$\sqrt{\varepsilon_0} A_k \rightarrow \sqrt{\frac{\omega_k \hbar}{2}} \hat{a}_k, \quad \sqrt{\varepsilon_0} A_k^* \rightarrow \sqrt{\frac{\omega_k \hbar}{2}} \hat{a}_k^\dagger.$$

Такая замена приводит к следующему выражению для гамильтониана:

$$\hat{\mathcal{H}}_k = \frac{\omega_k \hbar}{2} \left( \hat{a}_k \hat{a}_k^\dagger + \hat{a}_k^\dagger \hat{a}_k \right).$$

Воспользовавшись коммутационными соотношениями

$$[\hat{a}, \hat{a}^\dagger] = 1, \quad \hat{a}\hat{a}^\dagger - \hat{a}^\dagger\hat{a} = 1, \quad \hat{a}\hat{a}^\dagger = \hat{a}^\dagger\hat{a} + 1,$$

имеем  $\hat{\mathcal{H}}_k = \omega_k \hbar \left( \hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right)$  - выражение, полностью совпадающее с (1.28). Полный гамильтониан получим суммированием по всем модам:

$$\hat{\mathcal{H}} = \sum_{(k)} \hat{\mathcal{H}}_k = \sum_{(k)} \omega_k \hbar \left( \hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right). \quad (1.56)$$

В гамильтоновом виде можно представить и импульс электромагнитного поля. Классический импульс электромагнитного поля, находящегося в объеме  $V$ , определяется формулой

$$\vec{G} = \frac{1}{c^2} \int_{(\nu)} [\vec{E} \vec{H}] d\nu. \quad (1.57)$$

Используя разложение поля по плоским волнам, учитывая соотношения ортогональности, получим

$$\begin{aligned} \vec{G} &= \frac{1}{c^2} \int_{(\nu)} [\vec{E} \vec{H}] d\nu = \\ &= \frac{1}{c^2} \int_{(\nu)} \left[ \left( \sum_{(k)} A_k \vec{E}_k + \sum_{(k)} A_k^* \vec{E}_k^* \right) \left( \sum_{(k')} A_{k'} \vec{H}_{k'} + \sum_{(k')} A_{k'}^* \vec{H}_{k'}^* \right) \right] d\nu = \\ &= \sum_{(k)} \frac{1}{c^2} \int_{(\nu)} \left( A_k A_k^* [\vec{E}_k \vec{H}_k^*] + A_k^* A_k [\vec{E}_k^* \vec{H}_k] \right) d\nu = \\ &= \frac{1}{c^2} \sum_{(k)} \frac{\vec{k}}{k} \sqrt{\frac{\varepsilon_0}{\mu_0}} (A_k A_k^* + A_k^* A_k). \end{aligned}$$

Переходя к операторам имеем

$$\begin{aligned} \hat{\vec{G}} &= \frac{1}{c^2} \sum_{(k)} \frac{\vec{k}}{k} \sqrt{\frac{\varepsilon_0}{\mu_0}} \frac{\hbar \omega_k}{2\varepsilon_0} \left( \hat{a}_k^\dagger \hat{a}_k + \hat{a}_k \hat{a}_k^\dagger \right) = \\ &= \sum_{(k)} \hbar \vec{k} \frac{\omega_k}{ck} \frac{1}{c\sqrt{\varepsilon_0\mu_0}} \frac{\hat{a}_k^\dagger \hat{a}_k + \hat{a}_k \hat{a}_k^\dagger}{2} = \sum_{(k)} \vec{k} \hbar \left( \hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right). \end{aligned}$$

Из симметрии следует, что  $\sum_{(k)} \vec{k} \hbar = 0$  и, следовательно,

$$\hat{\vec{G}} = \sum_{(k)} \vec{k} \hbar \hat{a}_k^\dagger \hat{a}_k. \quad (1.58)$$

Оператор электрического поля выражается теперь следующим образом:

$$\hat{\vec{E}} = \sum_{(k)} \hat{a}_k \sqrt{\frac{\hbar\omega_k}{2\nu\epsilon_0}} \vec{e}_k e^{i(\vec{k}\vec{r})} + \sum_{(k)} \hat{a}_k^\dagger \sqrt{\frac{\hbar\omega_k}{2\nu\epsilon_0}} \vec{e}_k^* e^{-i(\vec{k}\vec{r})}. \quad (1.59)$$

В дальнейшем будем пользоваться дираковской формулировкой уравнений квантовой механики, поэтому в [разд. 14.1](#) дано краткое изложение дираковского формализма: введено понятие вектора состояния и изложены способы оперирования с ним.

## 1.8 Свойства операторов $\hat{a}$ и $\hat{a}^\dagger$ (операторов уничтожения и рождения)

Прежде всего, рассмотрим свойства операторов  $\hat{a}$  и  $\hat{a}^\dagger$ . Покажем, что

$$[\hat{\mathcal{H}}, \hat{a}] = -\hbar\omega\hat{a}, \quad [\hat{\mathcal{H}}, \hat{a}^\dagger] = \hbar\omega\hat{a}^\dagger. \quad (1.60)$$

Поскольку

$$\hat{\mathcal{H}} = \hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right)$$

то, используя коммутационные соотношения

$$[\hat{a}, \hat{a}^\dagger] = 1,$$

получим

$$\begin{aligned} [\hat{\mathcal{H}}, \hat{a}] &= \hbar\omega \left( \hat{a}^\dagger \hat{a} \hat{a} + \frac{1}{2} \hat{a} - \hat{a} \hat{a}^\dagger \hat{a} - \frac{1}{2} \hat{a} \right) = \\ &= \hbar\omega \left( \hat{a}^\dagger \hat{a} \hat{a} - (1 + \hat{a}^\dagger \hat{a}) \hat{a} \right) = -\hbar\omega \hat{a}, \end{aligned}$$

Второе равенство (1.60) доказывается аналогично.

В представлении Шредингера операторы от времени не зависят, а в представлении Гейзенберга - зависят и подчиняются уравнениям движения:

$$\dot{\hat{a}}(t) = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{a}] = -i\omega\hat{a}(t), \quad \dot{\hat{a}}^\dagger(t) = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{a}^\dagger] = i\omega\hat{a}^\dagger(t). \quad (1.61)$$

Здесь использованы равенства (1.60). Решение этих уравнений:

$$\hat{a}(t) = \hat{a}(0) e^{-i\omega t}, \quad \hat{a}^\dagger(t) = \hat{a}^\dagger(0) e^{i\omega t}, \quad (1.62)$$

где  $\hat{a}(0)$ ,  $\hat{a}^\dagger(0)$  - операторы в представлении Шредингера.

## 1.9 Квантовое состояние электромагнитного поля с определенной энергией (с определенным числом фотонов)

Сначала рассмотрим одну моду электромагнитного поля (простой гармонический осциллятор). Вектор состояния с определенной энергией  $|E_n\rangle$  удовлетворяет следующему уравнению

$$\hat{\mathcal{H}}|E_n\rangle = E_n|E_n\rangle \quad (1.63)$$

Здесь и далее будем пользоваться формализмом Дирака (см. [разд. 14.1](#)). Используя соотношение (1.60), получим

$$\hat{\mathcal{H}}\hat{a}|E_n\rangle = (\hat{a}\hat{\mathcal{H}} - \hbar\omega\hat{a})|E_n\rangle = (E_n - \hbar\omega)\hat{a}|E_n\rangle \quad (1.64)$$

т. е.  $\hat{a}|E_n\rangle$  также является вектором состояния с энергией  $E_n - \hbar\omega$ . Отсюда следует, что

$$\hat{a}|E_n\rangle = |E_n - \hbar\omega\rangle$$

Следовательно, оператор  $\hat{a}$  понижает энергию состояния на  $\hbar\omega$ , где  $\omega$  - частота моды (осциллятора). Часто  $\hat{a}$  называют понижающим оператором, или оператором уничтожения. Наименьшая энергия должна быть положительной, и понижение энергии не может продолжаться неограниченно. Для произвольного вектора состояния ожидаемое значение энергии

$$\langle\Phi|\hbar\omega\left(a^\dagger a + \frac{1}{2}\right)|\Phi\rangle = \hbar\omega\langle\Phi'|\Phi'\rangle + \frac{1}{2}\hbar\omega, \quad (1.65)$$

где  $\hat{a}|\Phi\rangle = |\Phi'\rangle$ ,  $\langle\Phi|\hat{a}^\dagger = \langle\Phi'|$ . Поскольку норма вектора состояния должна быть положительной, наименьшее значение энергии будет при  $\langle\Phi'|\Phi'\rangle = 0$ . Это означает, что  $\hat{a}|0\rangle = 0$ , где  $|\Phi\rangle = |0\rangle$  - вектор состояния с наименьшей энергией. Наименьшая энергия

$$E_0 = \frac{\hbar\omega}{2} \quad (1.66)$$

называется энергией нулевых колебаний. Для проверки этого утверждения можно написать

$$\begin{aligned} \hat{\mathcal{H}}|0\rangle &= \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|0\rangle = \\ &= \hbar\omega\hat{a}^\dagger\hat{a}|0\rangle + \frac{\hbar\omega}{2}|0\rangle = \\ &= \frac{\hbar\omega}{2}|0\rangle = E_0|0\rangle. \end{aligned} \quad (1.67)$$

С помощью (1.60) можно получить

$$\begin{aligned}\hat{\mathcal{H}}\hat{a}^\dagger|0\rangle &= \hat{\mathcal{H}}|1\rangle = \left(\hat{a}^\dagger\hat{\mathcal{H}} + \hbar\omega\hat{a}^\dagger\right)|0\rangle = \\ &= \hbar\omega\left(1 + \frac{1}{2}\right)\hat{a}^\dagger|0\rangle = \hbar\omega\left(1 + \frac{1}{2}\right)|1\rangle\end{aligned}\quad (1.68)$$

где через  $|1\rangle = \hat{a}^\dagger|0\rangle$  обозначено состояние с энергией  $\hbar\omega\left(1 + \frac{1}{2}\right)$ .

По индукции имеем

$$\hat{\mathcal{H}}(\hat{a}^\dagger)^n|0\rangle = \hat{\mathcal{H}}|n\rangle = \hbar\omega\left(n + \frac{1}{2}\right)(\hat{a}^\dagger)^n|0\rangle = \hbar\omega\left(n + \frac{1}{2}\right)|n\rangle \quad (1.69)$$

где  $|n\rangle = (\hat{a}^\dagger)^n|0\rangle$  без нормировки, которую проведем далее - состояние с энергией  $\hbar\omega\left(n + \frac{1}{2}\right)$ ,  $n$  - целое положительное число.

Видим, что оператор  $\hat{a}^\dagger$  повышает энергию состояния на  $\hbar\omega$ . Его можно рассматривать как оператор рождения частицы - фотона с энергией  $\hbar\omega$ . О фотоне как о частице лучше говорить в случае разложения поля по плоским волнам. Тогда это будет частица с энергией  $\hbar\omega$  и импульсом  $\hbar\vec{k}$ , как это следует из (1.58).

Соотношения  $\hat{a}|n\rangle = |n-1\rangle$  и  $\hat{a}^\dagger|n\rangle = |n+1\rangle$  определяют ненормированные векторы состояния. Определим нормирующий множитель. Предположим, что  $\hat{a}|n\rangle = S_n|n-1\rangle$ , где  $|n\rangle$  и  $|n-1\rangle$  нормированы к 1, а  $S_n$  является нормирующим множителем. Отсюда получим

$$S_n^2\langle n-1|n-1\rangle = \langle n|\hat{a}^\dagger\hat{a}|n\rangle = n\langle n|n\rangle$$

т.к. оператор  $\hat{a}^\dagger\hat{a} = \hat{n}$  является оператором числа фотонов, собственным числом которого является число фотонов. Это видно из формулы (1.69). Действительно, из равенства

$$\hat{\mathcal{H}}|n\rangle = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle = \hbar\omega\left(n + \frac{1}{2}\right)|n\rangle,$$

получаем:

$$\hat{n}|n\rangle = \hat{a}^\dagger\hat{a}|n\rangle = n|n\rangle.$$

Из условия нормировки следует:  $\langle n|n\rangle = 1$  и  $S_n^2 = n$ , откуда  $S_n = \sqrt{n}$  и, следовательно, имеем:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \quad (1.70)$$

По аналогии, с помощью коммутационных соотношений (1.26), а также 14.7 и 14.8 из разд. 14.1, получаем

$$\begin{aligned}\hat{a}^\dagger|n\rangle &= S_{n+1}|n+1\rangle, \quad \langle n|\hat{a} = S_{n+1}\langle n+1|, \\ \langle n|\hat{a}\hat{a}^\dagger|n\rangle &= S_{n+1}^2\langle n+1|n+1\rangle = \langle n|\hat{a}^\dagger\hat{a} + 1|n\rangle = (n+1)\langle n|n\rangle, \\ S_{n+1}^2 &= n+1.\end{aligned}\quad (1.71)$$



Следовательно, имеем равенство

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle, \quad (1.72)$$

Собственные состояния оператора числа фотонов  $\hat{n}$  являются ортонормированными. Действительно из того факта что оператор  $\hat{n}$  является эрмитовым:

$$\hat{n}^\dagger = (\hat{a}^\dagger \hat{a})^\dagger = \hat{a}^\dagger (\hat{a}^\dagger)^\dagger = \hat{a}^\dagger \hat{a} = \hat{n}$$

следует (см. [разд. 14.1](#)), что собственные функции этого оператора, соответствующие разным собственным числам, ортогональны, т. е.

$$\langle n|n'\rangle = 0, \text{ если } n \neq n'. \quad (1.73)$$

Дадим сводку соотношений, в которые входят операторы  $\hat{a}$  и  $\hat{a}^\dagger$ :

$$\begin{aligned} \hat{\mathcal{H}} &= \hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right), \quad \hat{a} |0\rangle = 0, \quad \hat{a}^\dagger \hat{a} |n\rangle = \hat{n} |n\rangle, \\ [\hat{a}, \hat{a}^\dagger] &= \hat{a} \hat{a}^\dagger - \hat{a}^\dagger \hat{a} = 1, \quad \hat{a} |n\rangle = \sqrt{n} |n-1\rangle \\ \hat{\mathcal{H}} |n\rangle &= \hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) |n\rangle, \\ \hat{a}^\dagger |n\rangle &= \sqrt{n+1} |n+1\rangle, \quad |n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle \end{aligned} \quad (1.74)$$

и сопряженные равенства

$$\begin{aligned} \langle 0| \hat{a}^\dagger &= 0, \quad \langle n| \hat{a} = \sqrt{n+1} \langle n+1| \\ \langle n| \hat{a}^\dagger &= \sqrt{n} \langle n-1|, \quad \langle n| = \frac{1}{\sqrt{n!}} \langle 0| (\hat{a}^\dagger)^n. \end{aligned} \quad (1.75)$$

Для простейшей модели резонатора имеем

$$\hat{E}(z, t) = E_1 (\hat{a} + \hat{a}^\dagger) \sin k_n z$$

где  $E_1 = \sqrt{\frac{\hbar\omega}{\varepsilon_0 V}}$  поле, соответствующее одному фотону в моде.

Рассмотрим некоторые свойства энергетических состояний, т.е. состояний с определенным числом фотонов. Покажем, что среднее значение электрического поля в этом состоянии равно нулю:

$$\begin{aligned} \langle n| \hat{E} |n\rangle &= E_1 \sin k_n z (\langle n| \hat{a} |n\rangle + \langle n| \hat{a}^\dagger |n\rangle) = \\ &= E_1 \sin k_n z (\langle n|n-1\rangle \sqrt{n} + \langle n|n+1\rangle \sqrt{n+1}) = 0 \end{aligned} \quad (1.76)$$

что следует из ортогональности состояний [\(1.73\)](#)  $\langle n|n'\rangle = 0$ .

Среднее значение оператора квадрата электрического поля отлично от нуля:

$$\begin{aligned}\langle n | \hat{E}^2 | n \rangle &= E_1^2 \sin^2 k_n z \langle n | (\hat{a}^\dagger \hat{a}^\dagger + \hat{a} \hat{a}^\dagger + \hat{a}^\dagger \hat{a} + \hat{a} \hat{a}) | n \rangle = \\ &= 2E_1^2 \sin^2 k_n z \left( n + \frac{1}{2} \right).\end{aligned}\quad (1.77)$$

Обычно рассматриваемые в квантовой оптике поля не находятся в стационарном состоянии с определенной энергией (с определенным числом фотонов). Однако произвольное состояние можно представить как суперпозицию состояний  $|n\rangle$ :

$$|\psi\rangle = \sum_{(n)} C_n |n\rangle \quad (1.78)$$

где  $|C_n|^2$  - вероятность при измерении обнаружить в моде  $n$  фотонов;  $\sum_{(n)} |C_n|^2 = 1$ . В [разд. 14.1](#) показано, что

$$C_n = \langle n | \psi \rangle, \quad |\psi\rangle = \sum_{(n)} \langle n | \psi \rangle |n\rangle = \sum_{(n)} |n\rangle \langle n | \psi \rangle, \quad \sum_{(n)} |n\rangle \langle n| = \hat{I},$$

где  $\hat{I}$  - единичный оператор.

**Комментарий 1.9.1** (О состояниях с определенной энергией в квантовой механике). *Стоит отметить, что состояния с определенной энергией не нарушают соотношение неопределенности Гейзенберга для пары энергия - время*

$$\Delta E \Delta t \geq \frac{\hbar}{2},$$

(более подробно см. [разд. 14.3.2](#)).

Вместе с тем, если посмотреть на оператор энергии гармонического осциллятора, записанный в виде

$$\hat{\mathcal{H}} = \frac{1}{2} (\hat{p}^2 + \omega^2 \hat{q}^2)$$

и воспользоваться выражениями (1.24), то можно получить, что  $\langle n | \hat{q} | n \rangle = \langle n | \hat{p} | n \rangle = 0$ . Вместе с тем

$$\begin{aligned}\langle n | \hat{q}^2 | n \rangle &= \frac{\hbar}{2\omega} \left[ \langle n | \hat{a}^2 | n \rangle + \langle n | (\hat{a}^\dagger)^2 | n \rangle + \right. \\ &\quad \left. + \langle n | \hat{a}^\dagger \hat{a} | n \rangle + \langle n | \hat{a} \hat{a}^\dagger | n \rangle \right] = \\ &= \frac{\hbar}{2\omega} [n + n + 1],\end{aligned}$$

а также

$$\begin{aligned}\langle n | \hat{p}^2 | n \rangle &= -\frac{\hbar\omega}{2} \left[ \langle n | \hat{a}^2 | n \rangle + \langle n | (\hat{a}^\dagger)^2 | n \rangle - \right. \\ &\quad \left. - \langle n | \hat{a}^\dagger \hat{a} | n \rangle - \langle n | \hat{a} \hat{a}^\dagger | n \rangle \right] = \\ &= \frac{\hbar\omega}{2} [n + n + 1].\end{aligned}$$

Т. о.

$$\Delta p = \sqrt{\langle n | \hat{p}^2 | n \rangle - \langle n | \hat{p} | n \rangle^2} = \sqrt{\frac{\hbar\omega}{2} (2n + 1)}$$

и

$$\Delta q = \sqrt{\langle n | \hat{q}^2 | n \rangle - \langle n | \hat{q} | n \rangle^2} = \sqrt{\frac{\hbar}{2\omega} (2n + 1)}$$

или

$$\Delta p \Delta q = \frac{\hbar}{2} (2n + 1) \geq \frac{\hbar}{2},$$

что находится в соответствии с соотношениями неопределенности Гейзенберга (14.47).

Таким образом состояния с определенной энергией это такие состояния, в которых несмотря на невозможность определить без погрешностей  $p$  и  $q$  имеется возможность определения величины  $\frac{1}{2} (p^2 + \omega^2 q^2)$ . Это отражает тот факт, что для квантовых систем возможны ситуации при которых существуют составные события при отсутствии элементарных (см. [разд. 15.3](#)). И, в частности, такая ситуация имеет место для фотона - состояния с определенной энергией  $|1\rangle$ .

Это может привести нас к рассуждению о том, что фотон это виртуальная частица, которая отсутствует в реальном физическом мире [15]. Вместе с тем математический аппарат связанный с понятием фотона как то, операторы рождения  $\hat{a}^\dagger$  и уничтожения  $\hat{a}$ , состояния электромагнитного поля с определенной энергией  $\{|n\rangle\}$  (которые могут быть использованы в качестве базисных состояний), представляется удобным для теоретического описания.

Стоит так же отметить, что с точки зрения формального определения неклассического состояния (8.5),  $|n\rangle$  является неклассическим состоянием света поскольку из (5.29) следует  $G^{(2)} < 1$ .

С другой стороны, если посмотреть на минимально возможную энергию моды электромагнитного поля то из соотношения (1.19)

$$\mathcal{H} = \frac{1}{2} (\omega^2 q^2 + p^2)$$

следует, что в классическом случае минимально возможная нулевая энергия достигается при  $p = 0, q = 0$ , но в силу (14.47) нулевые значения невозможны в квантовом случае, а с учетом неопределенности измерений получим

$$\begin{aligned} \frac{1}{2} (\omega^2 (\Delta q)^2 + (\Delta p)^2) &\geq \\ &\geq \omega \Delta q \Delta p \geq \frac{\hbar \omega}{2} \end{aligned}$$

то есть минимально возможная энергия (энергия вакуума) определяется неравенствами Гейзенберга для пары координата - импульс.

## 1.10 Многомодовые состояния

До сих пор мы рассматривали одномодовые поля. Результаты легко обобщаются на многомодовое состояние. Для электромагнитного поля в некотором объеме имеем разложение (1.11):

$$\vec{E}(r, t) = \sum_{(s)} \frac{q_s(t) \omega_s}{\sqrt{\varepsilon_0}} \vec{E}_s(r), \quad \vec{H}(r, t) = \sum_{(s)} \frac{p_s(t)}{\sqrt{\mu_0}} \vec{H}_s(r), \quad (1.79)$$

Функция Гамильтона равна сумме функций Гамильтона всех мод, так как моды соответствуют независимым осцилляторам:

$$\mathcal{H} = \frac{1}{2} \sum_{(s)} (\omega_s^2 q_s^2 + p_s^2) \quad (1.80)$$

Квантование сводится к замене  $q_s$  и  $p_s$  на операторы  $\hat{q}_s$  и  $\hat{p}_s$  с коммутационными соотношениями:

$$[\hat{q}_s, \hat{p}_{s'}] = i\hbar \delta_{ss'}, \quad [\hat{q}_s, \hat{q}_{s'}] = [\hat{p}_s, \hat{p}_{s'}] = 0. \quad (1.81)$$

Функция Гамильтона при этом превратится в оператор Гамильтона:

$$\hat{\mathcal{H}} = \frac{1}{2} \sum_{(s)} (\omega_s^2 \hat{q}_s^2 + \hat{p}_s^2) \quad (1.82)$$

Как в разделе 1.3, вводим операторы рождения и уничтожения для каждой моды (1.23):

$$\hat{a}_s = \frac{1}{\sqrt{2\hbar\omega_s}} (\omega_s \hat{q}_s + i\hat{p}_s), \quad \hat{a}_s^\dagger = \frac{1}{\sqrt{2\hbar\omega_s}} (\omega_s \hat{q}_s - i\hat{p}_s), \quad (1.83)$$

С их помощью гамильтониан можно представить в виде

$$\hat{\mathcal{H}}_s = \omega_n \hbar \left( \hat{a}_s^\dagger \hat{a}_s + \frac{1}{2} \right)$$

Общее состояние, когда в первой моде  $n_1$  фотонов, во второй  $n_2$  фотонов, в  $s$ -й -  $n_s$  фотонов и т.д., можно представить в виде произведения векторов состояний каждой моды (см. [разд. 14.5](#)):

$$|\{n_s\}\rangle = |n_1, n_2, \dots, n_s, \dots\rangle = |n_1\rangle \otimes |n_2\rangle \otimes \dots \otimes |n_s\rangle \otimes \dots,$$

где  $\{n_s\}$  означает совокупность чисел заполнения мод.

Действие операторов  $\hat{a}_s^\dagger$  и  $\hat{a}_s$ , относящихся к  $s$ -й моде, на вектор состояния описывается равенствами

$$\begin{aligned} \hat{a}_s |n_1, n_2, \dots, n_s, \dots\rangle &= \sqrt{n_s} |n_1, n_2, \dots, n_s - 1, \dots\rangle, \\ \hat{a}_s^\dagger |n_1, n_2, \dots, n_s, \dots\rangle &= \sqrt{n_s + 1} |n_1, n_2, \dots, n_s + 1, \dots\rangle. \end{aligned} \quad (1.84)$$

Вектор состояния в общем случае можно представить линейной суперпозицией состояний  $|\{n_s\}\rangle$ :

$$|\Psi\rangle = \sum_{n_1} \sum_{n_2} \dots \sum_{n_s} \dots C_{n_1, n_2, \dots, n_s, \dots} |n_1, n_2, \dots, n_s, \dots\rangle = \sum_{\{n_s\}} C_{\{n_s\}} |\{n_s\}\rangle \quad (1.85)$$

При разложении поля по плоским волнам оператор электрического поля имеет вид

$$\hat{\vec{E}} = \sum_{(k)} \sqrt{\frac{\hbar \omega_k}{2 \varepsilon_0 V}} \left( \hat{a}_k(t) \vec{e}_k e^{i(\vec{k}\vec{r})} + \hat{a}_k^\dagger(t) \vec{e}_k^* e^{-i(\vec{k}\vec{r})} \right) \quad (1.86)$$

Это выражение записано в представлении Гайзенберга (оператор зависит от времени). В этом представлении

$$\hat{a}_k(t) = \hat{a}_k(0) e^{-i\omega_k t}, \quad \hat{a}_k^\dagger(t) = \hat{a}_k^\dagger(0) e^{i\omega_k t},$$

где  $\hat{a}_k(0)$ ,  $\hat{a}_k^\dagger(0)$  - операторы в представлении Шредингера. В представлении Шредингера в выражении (1.86) операторы от времени не зависят. Для каждой моды имеем равенства (1.76), (1.77):

$$\langle n_k | \hat{a}_k | n_k \rangle = \langle n_k | \hat{a}_k^\dagger | n_k \rangle = 0$$

Отсюда для полного поля получим

$$\langle \{n_k\} | \hat{\vec{E}} | \{n_k\} \rangle = 0, \quad \langle \{n_k\} | \hat{\vec{E}}^2 | \{n_k\} \rangle = \sum_{(k)} \frac{\hbar \omega_k}{\varepsilon_0 V} \left( n + \frac{1}{2} \right) \quad (1.87)$$

Выражение (1.86) можно разбить на два слагаемых: частотно положительную часть, в которую входят операторы уничтожения, и частотно отрицательную часть, в которую входят операторы рождения:

$$\begin{aligned}\hat{\vec{E}} &= \hat{\vec{E}}^{(+)} + \hat{\vec{E}}^{(-)}, \\ \hat{\vec{E}}^{(+)} &= \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k(t) \vec{e}_k e^{i(\vec{k}\vec{r})}, \\ \hat{\vec{E}}^{(-)} &= \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k^\dagger(t) \vec{e}_k^* e^{-i(\vec{k}\vec{r})}\end{aligned}\quad (1.88)$$

$\hat{\vec{E}}^{(+)}$  соответствует аналитическому сигналу в классическом случае.

## 1.11 Когерентные состояния

Состояния  $|n\rangle$  не стремятся при увеличении  $n$  к классическому решению для осциллятора. Этим свойством обладают так называемые когерентные состояния. Они были введены Э.Шредингером, а затем развиты в наше время Р.Глаубером [48] и Э.Судершаном [46] применительно к задачам квантовой оптики. Когерентное состояние может быть определено различными путями. Воспользуемся определением в виде суперпозиции состояний  $|n\rangle$ :

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{(n)} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad \langle\alpha| = e^{-\frac{1}{2}|\alpha|^2} \sum_{(n)} \frac{\alpha^{*n}}{\sqrt{n!}} \langle n|, \quad (1.89)$$

где  $\alpha$  - некоторый комплексный параметр, смысл которого выяснится в дальнейшем.

Из определения (1.89) следует ряд свойств когерентных состояний. Прежде всего,

$$\langle\alpha|\alpha\rangle = e^{-|\alpha|^2} \sum_{(n)} \frac{(\alpha\alpha^*)^n}{n!} = e^{|\alpha|^2} e^{-|\alpha|^2} = 1, \quad (1.90)$$

т.е. когерентные состояния нормированы. Однако эти состояния не ортогональны:

$$\langle\alpha|\beta\rangle = e^{-\frac{1}{2}(|\alpha|^2+|\beta|^2)} \sum_{(n)} \frac{(\alpha^*\beta)^n}{n!} = e^{-\frac{1}{2}|\alpha|^2-\frac{1}{2}|\beta|^2+\alpha^*\beta} \quad (1.91)$$

Отсюда

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha|^2-|\beta|^2+\alpha^*\beta+\alpha\beta^*} = e^{-|\alpha-\beta|^2}, \quad (1.92)$$

т.е. эти состояния могут считаться приближенно ортогональными, если  $|\alpha - \beta|$  достаточно велико.

Неортогональность когерентных состояний является следствием переполненности системы ( $\alpha$  - любое комплексное число, а  $n$  - только целые числа).

Когерентные состояния являются собственными состояниями оператора уничтожения с собственным числом  $\alpha$ :

$$\hat{a} |\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{(n)} \frac{\alpha^n}{\sqrt{n!}} \sqrt{n} |n-1\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{(m=n-1)} \frac{\alpha \alpha^m}{\sqrt{m!}} |m\rangle = \alpha |\alpha\rangle \quad (1.93)$$

Сопряженное соотношение имеет вид

$$\langle \alpha | \hat{a}^\dagger = \alpha^* \langle \alpha | \quad (1.94)$$

Вероятность обнаружить (измерить) в когерентном состоянии  $n$  фотонов

$$|\langle n | \alpha \rangle|^2 = e^{-|\alpha|^2} \frac{(|\alpha|^2)^n}{n!} \quad (1.95)$$

соответствует распределению Пуассона со средним числом фотонов  $\langle n \rangle = |\alpha|^2$ . Используя известное нам соотношение

$$|n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle \quad (1.96)$$

когерентное состояние можно представить в виде

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{(n)} \frac{(\alpha \hat{a}^\dagger)^n}{n!} |0\rangle = e^{\alpha \hat{a}^\dagger - \frac{1}{2}|\alpha|^2} |0\rangle \quad (1.97)$$

Перепишем (1.97) в ином виде, для этого воспользуемся следующим соотношением

$$e^{-\alpha^* \hat{a}} |0\rangle = (1 - \alpha^* \hat{a} + \dots) |0\rangle = |0\rangle,$$

в результате получим

$$|\alpha\rangle = e^{\alpha \hat{a}^\dagger} e^{-\frac{1}{2}|\alpha|^2} e^{-\alpha^* \hat{a}} |0\rangle. \quad (1.98)$$

Далее воспользуемся операторным тождеством (формулой Бейкера-Хаусдорфа)

$$e^{\hat{c} + \hat{d}} = e^{-\frac{1}{2}[\hat{c}, \hat{d}]} e^{\hat{c}} e^{\hat{d}} \quad (1.99)$$

справедливым при условии  $[\hat{c}, [\hat{c}, \hat{d}]] = [\hat{d}, [\hat{c}, \hat{d}]] = 0$ . Если положить  $\hat{c} = \alpha \hat{a}^\dagger$ ,  $\hat{d} = -\alpha^* \hat{a}$  то из (1.98) получим

$$|\alpha\rangle = e^{\alpha \hat{a}^\dagger} e^{-\frac{1}{2}|\alpha|^2} e^{-\alpha^* \hat{a}} |0\rangle = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha \hat{a}^\dagger} e^{-\alpha^* \hat{a}} |0\rangle = e^{\alpha \hat{a}^\dagger - \alpha^* \hat{a}} |0\rangle. \quad (1.100)$$

Для того чтобы наглядно представить когерентные состояния, в разд. 14.6 дано координатное представление когерентного состояния.

Приведем еще несколько полезных соотношений, полученных из (1.97). Дифференцируя (1.97) по  $\alpha$ , имеем:

$$\frac{\partial}{\partial \alpha} |\alpha\rangle = \left( \hat{a}^\dagger - \frac{1}{2} \alpha^* \right) |\alpha\rangle,$$

или иначе

$$\hat{a}^\dagger |\alpha\rangle = \left( \frac{\partial}{\partial \alpha} + \frac{1}{2} \alpha^* \right) |\alpha\rangle.$$

сопряженное равенство имеет вид

$$\langle \alpha | \hat{a} = \left( \frac{\partial}{\partial \alpha^*} + \frac{1}{2} \alpha \right) \langle \alpha |$$

В общем случае оператор положительно частотной части электрического поля имеет вид

$$\hat{E}^{(+)} = \sum_{(k)} \sqrt{\frac{\hbar \omega_k}{2 \varepsilon_0 V}} \hat{a}_k(t) \vec{e}_k e^{-i \omega_k t + i(\vec{k} \vec{r})},$$

Положим, что поле (многомодовое) находится в состоянии

$$|\{\alpha_s\}\rangle = |\alpha_1, \alpha_2, \dots, \alpha_s, \dots\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \dots \otimes |\alpha_s\rangle \otimes \dots,$$

где  $\{\alpha_s\} = \{\alpha_{k_s}\}$  обозначает некоторую совокупность параметров  $\alpha$ . Если действовать оператором  $\hat{E}^{(+)}$  на состояние  $|\{\alpha_{k_s}\}\rangle$ , получим

$$\begin{aligned} \hat{E}^{(+)} |\{\alpha_{k_s}\}\rangle &= \left\{ \sum_{(k_s)} \sqrt{\frac{\hbar \omega_k}{2 \varepsilon_0 V}} \hat{a}_{k_s} \vec{e}_k e^{-i \omega_k t + i(\vec{k} \vec{r})} \right\} |\{\alpha_{k_s}\}\rangle = \\ &= \sum_{(k_s)} \sqrt{\frac{\hbar \omega_k}{2 \varepsilon_0 V}} \alpha_{k_s} \vec{e}_k e^{-i \omega_k t + i(\vec{k} \vec{r})} |\{\alpha_{k_s}\}\rangle, \end{aligned} \quad (1.101)$$

т.е.  $|\{\alpha_{k_s}\}\rangle$  является собственным вектором оператора положительно-частотной части электрического поля, а собственным значением является классическое



поле (аналитический сигнал), у которого комплексные амплитуды мод равны  $\sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}}\alpha_k$ . Отсюда следует, что каждому классическому полю соответствует некоторое когерентное состояние.

Среднее значение оператора электрического поля  $\hat{\vec{E}} = \hat{\vec{E}}^{(+)} + \hat{\vec{E}}^{(-)}$  в когерентном состоянии получим, рассмотрев сначала одну моду:

$$\langle \alpha_k | \hat{\vec{E}}_k | \alpha_k \rangle = 2\sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} |\alpha_k| \cos \left( \omega_k t - \left( \vec{k}\vec{r} + \theta_k \right) \right),$$

где  $\alpha_k = |\alpha_k| e^{i\theta_k}$ , что следует из соотношений

$$\langle \alpha_k | \hat{a}_k | \alpha_k \rangle = \alpha_k, \quad \langle \alpha_k | \hat{a}_k^\dagger | \alpha_k \rangle = \alpha_k^*$$

Обобщая это на многомодовый случай, получим

$$\langle \{\alpha_k\} | \hat{\vec{E}} | \{\alpha_k\} \rangle = 2 \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} |\alpha_k| \cos \left( \omega_k t - \left( \vec{k}\vec{r} \right) + \theta_k \right), \quad (1.102)$$

что соответствует классическому многомодовому полю, т.е. среднее значение  $\hat{\vec{E}}$  в когерентном состоянии является классическим полем с соответствующими амплитудами и фазами мод.

Когерентные состояния, как мы видели, не ортогональны из-за переполненности системы собственных векторов, но они удовлетворяют условию полноты:

$$\frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2\alpha = \hat{I}, \quad (1.103)$$

Здесь  $d^2\alpha = d \operatorname{Re} \alpha d \operatorname{Im} \alpha$ ,  $\hat{I}$  - единичный оператор, а интегрирование ведется по всей комплексной плоскости. Докажем это, воспользовавшись полярными координатами, изображенными на [рис. 1.5](#).

Используя разложение  $|\alpha\rangle$  по  $|n\rangle$  в полярных координатах, получим

$$\begin{aligned} & \int d^2\alpha |\alpha\rangle \langle \alpha| = \\ &= \int_0^\infty d|\alpha| \int_0^{2\pi} | \alpha | \sum_{(n)} \sum_{(m)} e^{-i(n-m)\varphi} e^{-|\alpha|^2} |m\rangle \langle n| \frac{|\alpha|^m |\alpha|^n}{\sqrt{n!m!}} d\varphi = \\ &= \pi \sum_{(n)} \frac{1}{n!} \int_0^\infty 2 |\alpha| |\alpha|^{2n} e^{-|\alpha|^2} |n\rangle \langle n| d|\alpha| = \\ &= \pi \sum_{(n)} \frac{|n\rangle \langle n|}{n!} \int_0^\infty x^n e^{-x} dx = \pi \sum_{(n)} |n\rangle \langle n| = \pi \hat{I}, \quad (1.104) \end{aligned}$$



Рис. 1.5: Комплексная плоскость на которой определены когерентные состояния. Полярные координаты.

где учтено, что

$$\int_0^{2\pi} e^{-i(n-m)\varphi} d\varphi = 2\pi\delta_{nm},$$

сделана замена переменных:

$$|\alpha|^2 = x, \quad 2|\alpha| d|\alpha| = dx,$$

использовано интегральное представление факториала:

$$n! = \int_0^\infty x^n e^{-x} dx$$

Таким образом, доказана формула (1.103). При помощи этого соотношения можно выразить одно когерентное состояние через все остальные:

$$|\alpha\rangle = \frac{1}{\pi} \int |\beta\rangle \langle\beta|\alpha\rangle d^2\beta,$$

но в (1.91) мы имели  $\langle\alpha|\beta\rangle = e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2 + \alpha^*\beta}$ , следовательно,

$$|\alpha\rangle = \frac{1}{\pi} \int |\beta\rangle e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2 + \alpha^*\beta} d^2\beta. \quad (1.105)$$

## 1.12 Смешанные состояния электромагнитного поля

До сих пор мы рассматривали только чистые состояния электромагнитного поля, описываемые векторами состояний. Одним из наиболее отличительных свойств чистых состояний является принцип суперпозиции.

Чистыми системами могут быть только изолированные системы, тогда как смешанные системы не изолированы от своего окружения. Для описания смешанных состояний используют аппарат матрицы плотности. Оператор плотности можно ввести следующим образом.

Рассмотрим смешанное состояние, для которого известны вероятности  $P_M$  нахождения поля в каждом из состояний  $|M\rangle$ . Вычислим среднее значение оператора  $\hat{O}$ , соответствующего наблюдаемой  $O$  в этом статистически смешанном состоянии. Среднее для статистической смеси состояний

$$\langle \hat{O} \rangle = \sum_{(M)} P_M \langle M | \hat{O} | M \rangle, \quad (1.106)$$

где, очевидно,

$$\sum_{(M)} P_M = 1.$$

Это выражение можно представить в другом виде. Используя некоторый полный набор состояний  $|S\rangle$  и условие его полноты

$$\sum_{(S)} |S\rangle \langle S| = \hat{I},$$

получим

$$\langle \hat{O} \rangle = \sum_{(M)} P_M \sum_{(S)} \langle M | \hat{O} | S \rangle \langle S | M \rangle = \sum_{(M)} \sum_{(S)} P_M \langle S | M \rangle \langle M | \hat{O} | S \rangle. \quad (1.107)$$

Исходя из (1.107), можно ввести статистический оператор  $\hat{\rho}$  при помощи выражения

$$\hat{\rho} = \sum_{(M)} P_M |M\rangle \langle M|. \quad (1.108)$$

Тогда равенство (1.107) можно представить в виде

$$\langle \hat{O} \rangle = \sum_{(S)} \langle S | \hat{\rho} \hat{O} | S \rangle = Sp(\hat{\rho} \hat{O}), \quad (1.109)$$

Это соотношение не зависит от выбора  $|S\rangle$ , так как след оператора не зависит от представления. Заметим, что

$$Sp(\hat{\rho}) = \sum_{(M)} \langle M | \hat{\rho} | M \rangle = \sum_{(M)} P_M = 1 \quad (1.110)$$

В качестве примера рассмотрим тепловое возбуждение фотонов в одну моду:

$$\hat{\rho} = \sum_{(n)} P_n |n\rangle \langle n|, \quad (1.111)$$

где  $P_n$  определяется распределением Больцмана

$$P_n = e^{-\beta n \hbar \omega} (1 - e^{-\beta \hbar \omega}),$$

здесь  $\beta = \frac{1}{k_b T}$ , а  $(1 - e^{-\beta \hbar \omega})$  - нормирующий множитель.

Среднее число фотонов в моде при тепловом возбуждении:

$$\begin{aligned} \bar{n} &= \langle \hat{n} \rangle = Sp(\hat{\rho} \hat{n}) = Sp(\hat{\rho} \hat{a}^\dagger \hat{a}) = \\ &= \sum_{(m)} \sum_{(n)} P_n \langle m | n \rangle \langle n | \hat{a}^\dagger \hat{a} | m \rangle = \\ &= \sum_{(n)} P_n \langle n | \hat{n} | n \rangle = \sum_{(n)} n e^{-\beta n \hbar \omega} (1 - e^{-\beta \hbar \omega}) = \frac{1}{e^{\beta \hbar \omega} - 1} \end{aligned} \quad (1.112)$$

Это известное выражение, полученное Планком. При этом мы воспользовались следующим выражением

$$\sum_{n=0}^{\infty} n r^{n-1} = \frac{d}{dr} \sum_{n=0}^{\infty} r^n = \frac{1}{(1-r)^2},$$

справедливым при  $|r| < 1$ .

Равенства (1.111), (1.112) можно записать в другом виде. Из (1.112) получим

$$e^{-\beta \hbar \omega} = \frac{\bar{n}}{1 + \bar{n}},$$

следовательно,

$$P_n = e^{-\beta \hbar \omega n} (1 - e^{-\beta \hbar \omega}) = \frac{\bar{n}^n}{(1 + \bar{n})^{n+1}}. \quad (1.113)$$

При этом матрица плотности приобретает вид:

$$\hat{\rho} = \sum_{(n)} \frac{\bar{n}^n}{(1 + \bar{n})^{n+1}} |n\rangle \langle n|.$$

Эта формула описывает матрицу плотности хаотического света через  $\bar{n}$  - среднее значение числа фотонов в моде. При этом  $\bar{n}$  не обязательно зависит от частоты в соответствии с формулой Планка (1.113). Зависимость  $\bar{n}$  от частоты

определяет форму линии хаотического света (различным частотам соответствуют различные моды). Обобщая полученный результат, можем написать выражение для статистического оператора хаотического света:

$$\hat{\rho} = \sum_{\{n_k\}} P_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| = \sum_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| \prod_{\{k\}} \frac{\bar{n}_k^{n_k}}{(1 + \bar{n}_k)^{n_k+1}}, \quad (1.114)$$

где  $\bar{n}_k$  зависят от частоты. Например, для хаотического света, имеющего лоренцовскую линию,

$$\bar{n}_k = \frac{IS}{\hbar\omega_{k_0}} \frac{\gamma}{(\omega_{k_0} - \omega_k)^2 + \gamma^2},$$

где  $\frac{IS}{\hbar\omega_{k_0}}$  - среднее число фотонов в пучке;  $I$  - интенсивность пучка (поток энергии);  $S$  - сечение пучка.

## 1.13 Представление оператора плотности через когерентные состояния

Важным для квантовой оптики является описание оптических явлений при помощи когерентных состояний. Используя дважды условие полноты для состояний с различным числом фотонов, для произвольного статистического оператора получим:

$$\hat{\rho} = \hat{I}\hat{\rho}\hat{I} = \sum_{(n)} \sum_{(m)} |n\rangle \langle n| \hat{\rho} |m\rangle \langle m| = \sum_{(n)} \sum_{(m)} \rho_{mn} |n\rangle \langle m|$$

Аналогично для когерентных состояний

$$\begin{aligned} \hat{\rho} &= \hat{I}\hat{\rho}\hat{I} = \frac{1}{\pi^2} \int d^2\alpha \int |\alpha\rangle \langle \alpha| \hat{\rho} |\beta\rangle \langle \beta| d^2\beta = \\ &= \frac{1}{\pi^2} \int d^2\alpha \int R(\alpha^*, \beta) e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2} |\alpha\rangle \langle \beta| d^2\beta, \end{aligned} \quad (1.115)$$

где

$$R(\alpha^*, \beta) = \langle \alpha| \hat{\rho} |\beta\rangle e^{\frac{1}{2}|\alpha|^2 + \frac{1}{2}|\beta|^2}$$

Если выразить  $|\alpha\rangle$  и  $|\beta\rangle$  через состояния  $|n\rangle$ , получим формулу

$$R(\alpha^*, \beta) = \sum_{(n)} \sum_{(m)} \frac{(\alpha^*)^n (\beta)^m}{\sqrt{n!m!}} \rho_{nm} \quad (1.116)$$

т. е.  $R(\alpha^*, \beta)$  легко найти, если известна матрица плотности в представлении чисел заполнения (чисел фотонов). Как пример рассмотрим тепловое возбуждение моды:

$$\begin{aligned} R(\alpha^*, \beta) &= \sum_{(n)} \sum_{(m)} \frac{(\alpha^*)^n (\beta)^m}{\sqrt{n!m!}} e^{-\beta n \hbar \omega} (1 - e^{-\beta \hbar \omega}) \delta_{nm} = \\ &= \sum_{(n)} \frac{(\alpha^* \beta)^n}{n!} e^{-\beta n \hbar \omega} (1 - e^{-\beta \hbar \omega}) = (1 - e^{-\beta \hbar \omega}) e^{\alpha^* \beta e^{-\beta \hbar \omega}}. \end{aligned} \quad (1.117)$$

Это представление зависит от двух параметров  $\alpha^*$  и  $\beta$ . Может оказаться более удобным другое представление матрицы плотности, введенное Р.Глаубером [48], называемое диагональным представлением и зависящее от одного параметра. Оно имеет вид

$$\hat{\rho} = \int P(\alpha) |\alpha\rangle \langle \alpha| d^2\alpha, \quad (1.118)$$

где  $P(\alpha)$  - действительная функция, удовлетворяющая условию

$$\int P(\alpha) d^2\alpha = 1.$$

Кроме того,  $P(\alpha)$  - вещественная функция комплексного аргумента. Это все следует из условий  $Sp(\hat{\rho}) = 1$  и  $\hat{\rho} = \hat{\rho}^\dagger$ .

Такое разложение возможно из-за переполненности системы когерентных состояний. Если  $P(\alpha)$  положительная функция, ее можно интерпретировать как распределение вероятностей. Это относится к некоторым наиболее интересным с практической точки зрения состояниям поля, например, к полностью хаотическому состоянию, но это не верно в общем случае. Иногда  $P(\alpha)$  может быть отрицательной в некоторой ограниченной области значений  $\alpha$ , тогда ее нельзя интерпретировать как распределение вероятности.  $P(\alpha)$  может быть и обобщенной функцией (примером является  $\delta$ -функция).

Строгое обоснование возможности представления (1.118) содержится в литературе [48], [46]. Обосновать возможность введения диагонального представления (1.118) можно следующим образом. Положим что статистический оператор  $\hat{\rho}$ , как и любой другой оператор, действующий на электромагнитное поле, может быть представлен в виде функции операторов рождения и уничтожения:

$$\hat{\rho} = \bar{f}(\hat{a}^\dagger, \hat{a}).$$

Тогда оператор может быть представлен в упорядоченном виде: нормальном и антинормальном. В первом случае операторы рождения располагаются справа от операторов уничтожения, а во втором случае наоборот - слева.

Например,

$$(\hat{a}^\dagger)^m (\hat{a})^n$$

нормально упорядоченный оператор. В антинормально упорядоченном операторе порядок обратный: операторы рождения стоят справа от оператора уничтожения. Например, оператор

$$(\hat{a})^n (\hat{a}^\dagger)^m$$

антинормально упорядочен. Упорядочение можно осуществить многократным применением коммутационного соотношения. Например, оператор

$$(\hat{a}^\dagger \hat{a})^2 = \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a}$$

не является ни нормальным, ни антинормальным. Используя условие  $[\hat{a}, \hat{a}^\dagger] = 1$ , приведем его к нормальному виду:

$$(\hat{a}^\dagger \hat{a})^2 = \hat{a}^\dagger (1 + \hat{a}^\dagger \hat{a}) \hat{a} = \hat{a}^\dagger \hat{a} + (\hat{a}^\dagger)^2 (\hat{a})^2$$

можно этот оператор представить в антинормальном виде:

$$\begin{aligned} (\hat{a}^\dagger \hat{a})^2 &= (\hat{a} \hat{a}^\dagger - 1) (\hat{a} \hat{a}^\dagger - 1) = \hat{a} \hat{a}^\dagger \hat{a} \hat{a}^\dagger - 2 \hat{a} \hat{a}^\dagger + 1 = \\ &= \hat{a} (\hat{a} \hat{a}^\dagger - 1) \hat{a}^\dagger - 2 \hat{a} \hat{a}^\dagger + 1 = (\hat{a})^2 (\hat{a}^\dagger)^2 - 3 \hat{a} \hat{a}^\dagger + 1. \end{aligned}$$

Существуют и другие, более эффективные методы упорядочения операторов [61].

Представим оператор плотности в антинормальном виде (рассматриваем одномодовый случай):

$$\hat{\rho}^{(a)}(\hat{a}, \hat{a}^\dagger) = \sum_{(n)} \sum_{(m)} C_{nm}^{(a)} (\hat{a})^n (\hat{a}^\dagger)^m \quad (1.119)$$

Воспользуемся теперь разложением (1.103) для единичного оператора  $\hat{I}$

$$\hat{I} = \frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2 \alpha$$

в результате получим

$$\begin{aligned} \hat{\rho}^{(a)}(\hat{a}, \hat{a}^\dagger) &= \sum_{(n)} \sum_{(m)} C_{nm}^{(a)} (\hat{a})^n \hat{I} (\hat{a}^\dagger)^m = \\ &= \frac{1}{\pi} \sum_{(n)} \sum_{(m)} C_{nm}^{(a)} \int d^2 \alpha (\hat{a})^n |\alpha\rangle \langle \alpha| (\hat{a}^\dagger)^m = \\ &= \frac{1}{\pi} \sum_{(n)} \sum_{(m)} \int d^2 \alpha C_{nm}^{(a)} \alpha^n \alpha^{*m} |\alpha\rangle \langle \alpha|. \end{aligned} \quad (1.120)$$

Обозначив теперь

$$P(\alpha, \alpha^*) = \frac{1}{\pi} \sum_{(n)} \sum_{(m)} C_{nm}^{(a)} \alpha^n \alpha^{*m}$$

получим что  $\hat{\rho}$  можно представить в виде

$$\hat{\rho} = \int d^2\alpha P(\alpha, \alpha^*) |\alpha\rangle \langle\alpha|. \quad (1.121)$$

Среднее значение оператора при использовании диагонального представления

$$\begin{aligned} \langle \hat{O} \rangle &= Sp(\hat{\rho} \hat{O}) = \\ &= \sum_{(n)} \langle n | \int d^2\alpha P(\alpha, \alpha^*) |\alpha\rangle \langle\alpha| \hat{O} |n\rangle = \\ &= \sum_{(n)} \int d^2\alpha P(\alpha, \alpha^*) \langle\alpha| \hat{O} |n\rangle \langle n | \alpha \rangle = \\ &= \int d^2\alpha P(\alpha, \alpha^*) \langle\alpha| \hat{O} |\alpha\rangle, \end{aligned} \quad (1.122)$$

т. к.  $\sum_{(n)} |n\rangle \langle n| = \hat{I}$ .

Выражение  $\langle\alpha| \hat{O} |\alpha\rangle$  легко вычисляется, если оператор  $\hat{O}$  представлен в нормальном виде:

$$\hat{O} = \hat{O}^{(n)} = \sum_{(n)} \sum_{(m)} d_{nm} (\hat{a}^\dagger)^n (\hat{a})^m, \quad (1.123)$$

тогда

$$\langle\alpha| \hat{O} |\alpha\rangle = \sum_{(n)} \sum_{(m)} d_{nm} \langle\alpha| (\hat{a}^\dagger)^n (\hat{a})^m |\alpha\rangle = \sum_{(n)} \sum_{(m)} d_{nm} \alpha^{*n} \alpha^m. \quad (1.124)$$

Отсюда следует простое правило: чтобы получить необходимый матричный элемент, нужно в операторе, представленном в нормально упорядоченном виде, произвести замену  $\hat{a} \rightarrow \alpha$ ,  $\hat{a}^\dagger \rightarrow \alpha^*$ .

В качестве примера покажем, что для теплового возбуждения моды

$$P(\alpha, \alpha^*) = \frac{1}{\pi \bar{n}} e^{-\frac{|\alpha|^2}{\bar{n}}} \quad (1.125)$$

и, следовательно

$$\hat{\rho} = \frac{1}{\pi \bar{n}} \int d^2\alpha e^{-\frac{|\alpha|^2}{\bar{n}}} |\alpha\rangle \langle\alpha|.$$



Найдем теперь матричные элементы оператора  $\hat{\rho}$  в представлении чисел заполнения (числа фотонов)

$$\begin{aligned}\langle n | \hat{\rho} | n \rangle &= \frac{1}{\pi \bar{n}} \int d^2 \alpha e^{-\frac{|\alpha|^2}{\bar{n}}} \langle n | \alpha \rangle \langle \alpha | n \rangle = \\ &= \frac{1}{\pi \bar{n}} \int d^2 \alpha e^{-\frac{|\alpha|^2}{\bar{n}}} \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2}\end{aligned}$$

Получившийся интеграл можно вычислить записав в полярной системе координат:

$$\alpha = r e^{i\varphi}, \quad d^2 \alpha = r dr d\varphi, \quad \text{т. е. } |\alpha| = r, \quad \arg \alpha = \varphi,$$

откуда

$$\begin{aligned}& \frac{1}{\pi \bar{n}} \int d^2 \alpha e^{-\frac{|\alpha|^2}{\bar{n}}} \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} = \\ &= \frac{1}{\pi \bar{n}} \int_0^{2\pi} d\varphi \int_0^\infty r dr \frac{\exp\left(-r^2 \frac{\bar{n}+1}{\bar{n}}\right)}{n!} r^{2n} = \\ &= \frac{1}{\bar{n}} \int_0^\infty 2r dr \frac{\exp\left(-r^2 \frac{\bar{n}+1}{\bar{n}}\right)}{n!} r^{2n} = \\ &= \frac{1}{\bar{n}} \int_0^\infty \frac{e^{-x}}{n!} \frac{\bar{n}^{n+1}}{(\bar{n}+1)^{n+1}} x^n dx = \\ &= \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \frac{1}{n!} \int_0^\infty e^{-x} x^n dx = \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}},\end{aligned}\tag{1.126}$$

где сделана замена  $x = r^2 \frac{\bar{n}+1}{\bar{n}}$ .

Таким образом, мы получили известный нам матричный элемент статистического оператора хаотического поля в представлении чисел заполнения. Отсюда следует, что выражение (1.125) действительно является статистическим оператором хаотического поля в представлении когерентных состояний. Следовательно для теплового возбуждения фотонов в моду имеем

$$P(\alpha) = \frac{1}{\pi \bar{n}} e^{-\frac{|\alpha|^2}{\bar{n}}}, \quad \text{где } \bar{n} = \frac{1}{e^{\hbar\omega\beta} - 1}\tag{1.127}$$

Обобщение полученных выражений на многомодовый случай очевидно:

$$\langle \hat{O} \rangle = \int \cdots \int_{\{\alpha_k\}} P^{(a)}(\{\alpha_k\}) O^{(n)}(\{\alpha_k\}) \prod_k d^2 \alpha_k,\tag{1.128}$$

$$P^{(a)}(\{\alpha_k\}) = \prod_k \frac{1}{\pi \bar{n}_k} e^{-\frac{|\alpha_k|^2}{\bar{n}_k}}.$$

## 1.14 Упражнения

1. Доказать ортогональность полей собственных колебаний (1.14).
2. Доказать для плоских волн равенства (1.52).
3. Исходя из равенства (1.57), получить выражение (1.58) для оператора импульса квантованного электромагнитного поля.
4. Доказать формулу Бейкера-Хаусдорфа (1.99)
5. Сколько мод электромагнитного поля с длиной волны  $\lambda \geq 500\text{нм}$  находятся в кубе квантования со стороной  $L = 1\text{мм}$  [12]

## Глава 2

# Взаимодействие света с атомом

Рассматриваются вопросы, связанные с взаимодействием квантованного электромагнитного поля с атомом. Используется упрощенная модель атома - двухуровневый атом. Такое упрощение оправдано при резонансном взаимодействии и широко используется в задачах квантовой электроники и квантовой оптики. Большое внимание уделено рассмотрению взаимодействия атома, моды резонатора (динамической системы) с термостатом (диссипативной системой), которое ответственно за релаксацию динамической системы.

### 2.1 Излучение и поглощение атомом света

Рассмотрим простейшую задачу о взаимодействии одномодового излучения с двухуровневым атомом. Упрощения оправданы тем, что лазерное излучение часто можно рассматривать как одномодовое, и при резонансном взаимодействии можно пренебречь всеми уровнями атома, кроме двух, частота перехода между которыми близка к частоте взаимодействующей с атомом моды. Эта простейшая ситуация изображена на [рис. 2.1](#)



Рис. 2.1: Взаимодействие моды электромагнитного поля с двухуровневым атомом.

Положим, что атом и поле первоначально находятся в состояниях

$$|\psi_A\rangle = C_a |a\rangle + C_b |b\rangle, |\psi_F\rangle = \sum_{(n)} C_n |n\rangle \quad (2.1)$$

где:  $|a\rangle, |b\rangle$  - векторы соответственно верхнего и нижнего состояний атома,  $|n\rangle$  вектор состояния моды, содержащей  $n$  фотонов.

Полный вектор состояния системы атом-поле равен

$$|\psi_{AF}\rangle = \sum_{(n)} (C_{an} |a\rangle |n\rangle + C_{bn} |b\rangle |n\rangle). \quad (2.2)$$

Здесь  $C_{an}, C_{bn}$  - соответствующие амплитуды вероятностей. Из-за взаимодействия между атомом и полем амплитуды вероятностей меняются во времени. Например, если атом первоначально находился на верхнем уровне, а поле моды содержало  $n$  фотонов, то есть  $|\psi_{AF}\rangle = |a\rangle |n\rangle$ , то в последующие моменты времени поле будет находиться в состоянии

$$|\psi_{AF}\rangle = C_{an} |a\rangle |n\rangle + C_{b,n+1} |b\rangle |n+1\rangle. \quad (2.3)$$

## 2.2 Гамильтониан системы атом-поле

Гамильтониан системы атом-поле можно представить в виде

$$\hat{\mathcal{H}} = \hat{\mathcal{H}}^{(A)} + \hat{\mathcal{H}}^{(F)} + \hat{V}$$

где  $\hat{\mathcal{H}}^{(A)}$  - гамильтониан двухуровневого атома,  $\hat{\mathcal{H}}^{(F)}$  - гамильтониан электромагнитного поля и  $\hat{V}$  - гамильтониан взаимодействия.

Для гамильтониана электромагнитного поля мы имеем выражение (1.28):

$$\hat{\mathcal{H}}^{(F)} = \hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right).$$

В случае гамильтониана двухуровневого атома воспользуемся следующими соотношениями:

$$\begin{aligned} \hat{\mathcal{H}}^{(A)} |a\rangle &= \hbar\omega_a |a\rangle, \\ \hat{\mathcal{H}}^{(A)} |b\rangle &= \hbar\omega_b |b\rangle, \\ |a\rangle \langle a| + |b\rangle \langle b| &= \hat{I}, \end{aligned}$$

откуда получим

$$\begin{aligned} \hat{\mathcal{H}}^{(A)} &= \hat{\mathcal{H}}^{(A)} \hat{I} = \hat{\mathcal{H}}^{(A)} |a\rangle \langle a| + \hat{\mathcal{H}}^{(A)} |b\rangle \langle b| = \\ &= \hbar\omega_a |a\rangle \langle a| + \hbar\omega_b |b\rangle \langle b| = \\ &= \hbar\omega_a \hat{\sigma}_a + \hbar\omega_b \hat{\sigma}_b, \end{aligned} \quad (2.4)$$

где введены следующие обозначения

$$\hat{\sigma}_a = |a\rangle \langle a|, \quad \hat{\sigma}_b = |b\rangle \langle b|.$$

Выражение (2.4) может быть переписано в матричной форме:

$$\hat{\mathcal{H}}^{(A)} = \hbar \begin{pmatrix} \omega_a & 0 \\ 0 & \omega_b \end{pmatrix}. \quad (2.5)$$

Для гамильтониана взаимодействия  $\hat{V}$  при полуклассическом подходе в дипольном приближении имеем:

$$\hat{V} = -e \left( \hat{\vec{r}} \vec{E}(t) \right). \quad (2.6)$$

Применив к (2.6) дважды условие полноты получим

$$\begin{aligned} \hat{V} &= \hat{I} \hat{V} \hat{I} = -e \left( \vec{E}(t) \hat{I} \hat{\vec{r}} \hat{I} \right) = \\ &= -e \left( \vec{E}(t) (|a\rangle \langle a| + |b\rangle \langle b|) \hat{\vec{r}} (|a\rangle \langle a| + |b\rangle \langle b|) \right) = \\ &= - \left( \vec{E}(t) \left( \vec{P}_{ab} |a\rangle \langle b| + \vec{P}_{ba} |b\rangle \langle a| \right) \right), \end{aligned} \quad (2.7)$$

где

$$\vec{P}_{ab} = \vec{P}_{ba}^* = e \langle a | \hat{\vec{r}} | b \rangle$$

матричный элемент электрического дипольного момента. Для простоты будем считать, что  $\vec{P}_{ab} = \vec{P}_{ba} = \vec{p}$  - вещественная величина. В результате выражение (2.7) может быть записано в виде

$$\begin{aligned} \hat{V} &= - \left( \vec{E}(t) \vec{p} \right) (|a\rangle \langle b| + |b\rangle \langle a|) = \\ &= - \left( \vec{E}(t) \vec{p} \right) (\hat{\sigma}^\dagger + \hat{\sigma}), \end{aligned} \quad (2.8)$$

где  $\hat{\sigma}^\dagger = |a\rangle \langle b|$  и  $\hat{\sigma} = |b\rangle \langle a|$  - операторы перехода.  $\hat{\sigma}^\dagger$  - оператор перехода из нижнего состояния в верхнее (повышающий оператор):

$$\hat{\sigma}^\dagger |b\rangle = |a\rangle \langle b|b\rangle = |a\rangle,$$

$\hat{\sigma}$  - оператор перехода из верхнего состояния в нижнее (понижающий оператор):

$$\hat{\sigma} |a\rangle = |b\rangle \langle a|a\rangle = |b\rangle.$$

Кроме этого выполняются равенства

$$\hat{\sigma}^\dagger |a\rangle = |a\rangle \langle b|a\rangle = 0$$



Рис. 2.2: Гамильтониан взаимодействия. Процесс описываемый  $\hat{a}\hat{\sigma}$  - поглощение фотона и переход атома из верхнего состояния в нижнее.

и

$$\hat{\sigma} |b\rangle = |b\rangle \langle a|b\rangle = 0.$$

Для операторов  $\hat{\sigma}$  и  $\hat{\sigma}^\dagger$  может быть записано следующее соотношение:

$$\begin{aligned} \hat{\sigma}\hat{\sigma}^\dagger + \hat{\sigma}^\dagger\hat{\sigma} &= \\ &= |b\rangle \langle a|a\rangle \langle b| + |a\rangle \langle b|b\rangle \langle a| = \\ &= |b\rangle \langle b| + |a\rangle \langle a| = \hat{I}, \end{aligned} \quad (2.9)$$

где  $\hat{I}$  - единичный оператор.

Выражение (2.8) может быть также записано в матричной форме

$$\hat{V} = - \left( \vec{p} \vec{E} \right) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.10)$$

Переход от полуклассического гамильтониана взаимодействия к полностью квантовому выражению осуществляется заменой классического электрического поля на оператор электрического поля. Таким образом, получаем

$$\hat{V} = -pE_1 \sin kz (\hat{a} + \hat{a}^\dagger) (\hat{\sigma} + \hat{\sigma}^\dagger) \quad (2.11)$$

Здесь использовано простейшее выражение для оператора электрического поля моды (1.32).

Полный гамильтониан системы атом-поле имеет вид

$$\hat{\mathcal{H}}_{AF} = \hbar\omega_a \sigma_a + \hbar\omega_b \sigma_b + \hbar\omega \left( \hat{a}^\dagger \hat{a} + \frac{1}{2} \right) + \hbar g (\hat{a} + \hat{a}^\dagger) (\hat{\sigma} + \hat{\sigma}^\dagger)$$

где  $g = -\frac{p}{\hbar} E_1 \sin kz$  - константа взаимодействия, зависящая от распределения поля моды в пространстве.

Не все члены, входящие в гамильтониан взаимодействия (2.11), равноправны. При перемножении скобок получаем члены:

1.  $\hat{a}\hat{\sigma}$  - этот член соответствует поглощению фотона и переходу атома из верхнего состояния в нижнее. Условно этот процесс изображен на рис. 2.2;



Рис. 2.3: Гамильтониан взаимодействия. Процесс описываемый  $\hat{a}\hat{\sigma}^\dagger$  - поглощение фотона и переход атома из нижнего состояния в верхнее.



Рис. 2.4: Гамильтониан взаимодействия. Процесс описываемый  $\hat{a}^\dagger\hat{\sigma}$  - излучение фотона и переход атома из верхнего состояния в нижнее.



Рис. 2.5: Гамильтониан взаимодействия. Процесс описываемый  $\hat{a}^\dagger\hat{\sigma}^\dagger$  - излучение фотона и переход атома из нижнего состояния в верхнее.

2.  $\hat{a}\hat{\sigma}^\dagger$  - этот член соответствует поглощению фотона и переходу атома из нижнего состояния в верхнее (см. [рис. 2.3](#));
3.  $\hat{a}^\dagger\hat{\sigma}$  - этот член соответствует излучению фотона и переходу атома из верхнего состояния в нижнее (см. [рис. 2.4](#));
4.  $\hat{a}^\dagger\hat{\sigma}^\dagger$  - этот член соответствует излучению фотона и переходу атома из нижнего состояния в верхнее (см. [рис. 2.5](#)).

Случаи 1 и 4 относятся к процессам (см. [рис. 2.2](#) и [2.5](#)) при которых нарушается закон сохранения энергии. Эти процессы можно отнести к так называемым виртуальным процессам. Их вероятность с ростом времени стремится к 0 и их вкладом в гамильтониан взаимодействия можно пренебречь. Остаются члены 2 и 3 (см. [рис. 2.3](#) и [2.4](#)), соответствующие процессам, идущим без нарушения закона сохранения энергии. С учетом всего сказанного гамильтониан взаимодействия принимает вид:

$$\hat{V} = g\hbar (\hat{a}\hat{\sigma}^\dagger + \hat{a}^\dagger\hat{\sigma}) \quad (2.12)$$

Удобно перейти к представлению взаимодействия (см. [разд. 14.2.1](#)), используя известную формулу ([14.31](#))

$$\hat{V}_I = e^{i\frac{\hat{\mathcal{H}}_0 t}{\hbar}} \hat{V} e^{-i\frac{\hat{\mathcal{H}}_0 t}{\hbar}} \quad (2.13)$$

где  $\hat{\mathcal{H}}_0 = \hat{\mathcal{H}}^{(A)} + \hat{\mathcal{H}}^{(F)}$  - невозмущенный гамильтониан системы атом-поле. Можно показать, что в представлении взаимодействия гамильтониан взаимодействия имеет вид

$$\hat{V}_I = g\hbar \left( \hat{a}^\dagger\hat{\sigma} e^{i(\omega - \omega_{ab})t} + \hat{\sigma}^\dagger\hat{a} e^{-i(\omega - \omega_{ab})t} \right). \quad (2.14)$$

Это проще всего сделать, вычислив матричные элементы  $\langle n+1 | \langle b | \hat{V}_I | a \rangle | n \rangle$  и  $\langle n | \langle a | \hat{V}_I | b \rangle | n+1 \rangle$  для оператора взаимодействия  $\hat{V}_I$ , представимого в виде ([2.13](#)) и ([2.14](#)), и убедиться, что они одинаковы в обоих случаях.

## 2.3 Взаимодействие атома с модой электромагнитного поля

Уравнение Шредингера в представлении взаимодействия имеет вид

$$i\hbar \frac{\partial}{\partial t} |\psi(r, t)\rangle_I = \hat{V}_I |\psi(r, t)\rangle_I, \quad (2.15)$$



где через  $|\psi(r, t)\rangle_I$  записана волновая функция в представлении взаимодействия:

$$|\psi(r, t)\rangle_I = e^{i\frac{\hat{H}_0 t}{\hbar}} |\psi(r, t)\rangle. \quad (2.16)$$

Решим это уравнение для начального состояния  $|\psi(r, 0)\rangle_I = |b, n+1\rangle_I$ , т. е. будем считать, что в начальный момент атом находится в нижнем состоянии, а поле содержит  $n+1$  фотонов. Другой случай соответствует начальному состоянию системы  $|a, n\rangle_I$ , т.е. атом находится в верхнем состоянии, а поле моды содержит  $n$  фотонов. Через некоторое время в результате взаимодействия атома и поля система будет находиться в суперпозиционном состоянии

$$|\psi(r, t)\rangle_I = C_{a,n}(t)_I |a, n\rangle_I + C_{b,n+1}(t)_I |b, n+1\rangle_I. \quad (2.17)$$

Воспользовавшись (2.16) в левой части выражения (2.17) получим

$$\begin{aligned} & C_{a,n}(t)_I |a, n\rangle_I + C_{b,n+1}(t)_I |b, n+1\rangle_I = \\ & = C_{a,n}(t)_I e^{i\frac{\hat{H}_0 t}{\hbar}} |a, n\rangle + C_{b,n+1}(t)_I e^{i\frac{\hat{H}_0 t}{\hbar}} |b, n+1\rangle = \\ & = C_{a,n}(t)_I \exp\left\{i\left(\omega_a + \omega\left(n + \frac{1}{2}\right)\right)t\right\} |a, n\rangle + \\ & + C_{b,n+1}(t)_I \exp\left\{i\left(\omega_b + \omega\left(n + 1 + \frac{1}{2}\right)\right)t\right\} |b, n+1\rangle \\ & = C_{a,n}(t) |a, n\rangle + C_{b,n+1}(t) |b, n+1\rangle, \end{aligned}$$

где через  $C_{a,n}(t)$  и  $C_{b,n+1}(t)$  обозначено

$$\begin{aligned} C_{a,n}(t) &= C_{a,n}(t)_I \exp\left\{i\left(\omega_a + \omega\left(n + \frac{1}{2}\right)\right)t\right\}, \\ C_{b,n+1}(t) &= C_{b,n+1}(t)_I \exp\left\{i\left(\omega_b + \omega\left(n + 1 + \frac{1}{2}\right)\right)t\right\}. \end{aligned}$$

Таким образом уравнение (2.15) принимает следующий вид

$$\begin{aligned} & i\left(\dot{C}_{a,n}(t) |a, n\rangle + \dot{C}_{b,n+1}(t) |b, n+1\rangle\right) = \\ & = g\left(\hat{a}\hat{\sigma}^\dagger e^{-i(\omega-\omega_{ab})t} + \hat{a}^\dagger\hat{\sigma} e^{i(\omega-\omega_{ab})t}\right)(C_{a,n} |a, n\rangle + C_{b,n+1} |b, n+1\rangle) = \\ & = g\sqrt{n+1}\left(C_{b,n+1} e^{-i(\omega-\omega_{ab})t} |a, n\rangle + C_{a,n} e^{i(\omega-\omega_{ab})t} |b, n+1\rangle\right). \quad (2.18) \end{aligned}$$

Помножим это уравнение слева соответственно на  $\langle a, n|$  и  $\langle b, n+1|$ . Учитывая свойства операторов  $\hat{a}$ ,  $\hat{a}^\dagger$ ,  $\hat{\sigma}$ ,  $\hat{\sigma}^\dagger$  и ортогональность векторов состояния, получим систему уравнений для амплитуд вероятностей

$$\begin{aligned} \dot{C}_{a,n}(t) &= -ig\sqrt{n+1}e^{-i(\omega-\omega_{ab})t}C_{b,n+1}(t), \\ \dot{C}_{b,n+1}(t) &= -ig\sqrt{n+1}e^{i(\omega-\omega_{ab})t}C_{a,n}(t). \end{aligned} \quad (2.19)$$



Рис. 2.6: Поглощение фотона двухуровневым атомом. В результате взаимодействия атом переходит с нижнего уровня в верхний, а в моде электромагнитного поля становится на один фотон меньше.



Рис. 2.7: Излучение фотона двухуровневым атомом. В результате взаимодействия атом переходит с верхнего уровня в нижний, а в моде электромагнитного поля становится на один фотон больше.

Для случая, когда атом находится в нижнем состоянии (случай поглощения фотона) имеем в начальный момент  $C_{a,n}(0) = 0$ ,  $C_{b,n+1}(0) = 1$  (рис. 2.6). Формальное интегрирование (2.19) дает

$$C_{a,n}(t) = -ig\sqrt{n+1} \int_0^t e^{-i(\omega-\omega_{ab})t'} C_{b,n+1}(t') dt' \quad (2.20)$$

В первом приближении для малых времен можно в (2.20) под интегралом положить  $C_{b,n+1}(t') = 1$ . Тогда, интегрируя, получим

$$C_{a,n}(t) = -ig\sqrt{n+1} \frac{e^{-i(\omega-\omega_{ab})t} - 1}{-i(\omega-\omega_{ab})} \quad (2.21)$$

откуда для вероятности возбуждения атома и поглощения фотона имеем

$$|C_{a,n}(t)|^2 = g^2(n+1)t^2 \frac{\sin^2((\omega-\omega_{ab})t/2)}{(\omega-\omega_{ab})^2(t/2)^2}. \quad (2.22)$$

В таком приближении можно решить и вторую задачу (рис. 2.7)  $C_{a,n}(0) = 1$ ,  $C_{b,n+1}(0) = 0$ . Получим для вероятности перехода атома в нижнее состояние и излучения фотона аналогичное (2.22) выражение

$$|C_{b,n+1}(t)|^2 = g^2(n+1)t^2 \frac{\sin^2((\omega-\omega_{ab})t/2)}{(\omega-\omega_{ab})^2(t/2)^2}. \quad (2.23)$$

В случае, когда поле не имеет ни одного фотона ( $n = 0$ ), получаем отличную от нуля вероятность  $|C_{b,1}(t)|^2 \cong g^2 t^2 \left(\frac{\sin^2 x}{x^2} \cong 1, \text{ если } x \ll 1\right)$ , откуда видно, что возбужденный атом даже при отсутствии фотонов может перейти в нижнее состояние. Такой процесс носит название спонтанного излучения или спонтанного перехода. Он связан с нулевыми колебаниями поля. Заметим, что при полуклассическом рассмотрении спонтанное излучение не следует из полуклассических уравнений и вводится из дополнительных соображений. Из квантовых уравнений спонтанное излучение следует естественным образом. Систему уравнений (2.19) можно решить точно. Для простоты будем рассматривать резонансный случай  $\omega = \omega_{ab}$ . Исключим из уравнений  $C_{b,n+1}(t)$ :

$$\ddot{C}_{a,n}(t) = -ig\sqrt{n+1}\dot{C}_{b,n+1}(t) = -g^2(n+1)C_{a,n}(t).$$

Решение полученного уравнения:

$$C_{a,n}(t) = A \sin(g\sqrt{n+1}t) + B \cos(g\sqrt{n+1}t)$$

При поглощении начальные условия ( $C_{a,n}(0) = 0, C_{b,n+1}(0) = 1$ ) дают  $A = i, B = 0$ , следовательно,

$$C_{a,n}(t) = -i \sin\left(\frac{\omega_R t}{2}\right), \quad C_{b,n+1}(t) = \cos\left(\frac{\omega_R t}{2}\right), \quad (2.24)$$

где  $\omega_R = 2g\sqrt{n+1}$  - частота Раби в квантовом случае. Для случая излучения из начальных условий ( $C_{a,n}(0) = 1, C_{b,n+1}(0) = 0$ ) имеем  $A = 0, B = 1$ , следовательно,

$$C_{a,n}(t) = \cos\left(\frac{\omega_R t}{2}\right), \quad C_{b,n+1}(t) = -i \sin\left(\frac{\omega_R t}{2}\right), \quad (2.25)$$

На рис. 2.8 изображены зависимости вероятностей  $|C_{a,n}(t)|^2$  и  $|C_{b,n+1}(t)|^2$  от времени для случая излучения фотона.

В полуклассическом выражении частота Раби  $\omega_R$  равна  $\frac{|pE|}{\hbar}$ , в квантовом -  $2g\sqrt{n+1}$ , т. е.  $E$  соответствует  $E_1\sqrt{n+1}$ , где  $E_1$  - поле, соответствующее одному фотону в моде. При больших  $n$  эти два выражения практически совпадают. Но при малых  $n$  различие может быть значительным. Из квантового выражения следует, что даже когда в моде нет фотонов, вероятности осциллируют с частотой  $g$ . На самом деле известно, что осцилляции на частоте Раби затухают. Расхождение связано с тем, что атом взаимодействует со всеми модами пространства, мы же учитывали только взаимодействие с одной модой.



Рис. 2.8: Зависимости вероятностей  $|C_{a,n}|^2$  и  $|C_{b,n+1}|^2$  от времени для случая излучения фотона.

Попробуем теперь найти общее решение системы уравнений (2.19). Рассматриваемые соотношения можно записать в следующем виде

$$\begin{aligned}\dot{C}_{a,n}(t) &= -i\frac{\omega_R}{2}e^{-i\delta t}C_{b,n+1}(t), \\ \dot{C}_{b,n+1}(t) &= -i\frac{\omega_R}{2}e^{i\delta t}C_{a,n}(t),\end{aligned}$$

где  $\delta = \omega - \omega_{ab}$  - расстройка частоты. Задачу будем решать только для случая излучения, т. е. начальные условия имеют вид

$$\begin{aligned}C_{a,n}(0) &= 1, \\ C_{b,n+1}(0) &= 0.\end{aligned}$$

При этом интересоваться нас будет прежде всего поведение вероятностей  $|C_{b,n+1}(t)|^2$ . Т. о. обозначив  $x(t) = C_{b,n+1}(t)$  получим

$$\begin{aligned}\ddot{x} &= -i\frac{\omega_R}{2}\frac{d(e^{i\delta t}C_{a,n}(t))}{dt} = \\ &= i\delta\left(-i\frac{\omega_R}{2}e^{i\delta t}C_{a,n}(t)\right) - i\frac{\omega_R}{2}e^{i\delta t}\frac{dC_{a,n}(t)}{dt} = \\ &= i\delta\dot{x} - \frac{\omega_R^2}{4}e^{-i\delta t}e^{i\delta t}x = \\ &= i\delta\dot{x} - \frac{\omega_R^2}{4}x,\end{aligned}$$

т. е.

$$\ddot{x} - i\delta\dot{x} + \frac{\omega_R^2}{4}x = 0. \quad (2.26)$$



Рис. 2.9: График 1: Осцилляции Раби с нулевой расстройкой  $\delta = 0$ . Период осцилляций  $\frac{2\pi}{\omega_R}$ ,  $\Omega_R = \omega_R$ , максимальная амплитуда вероятности  $|C_{b,n+1}|^2 = 1$ . График 2: Осцилляции Раби с ненулевой расстройкой  $\delta = \sqrt{3}\omega_R$ . Период осцилляций  $\frac{\pi}{\omega_R}$ ,  $\Omega_R = 2 \cdot \omega_R$ , максимальная амплитуда вероятности  $|C_{b,n+1}|^2 = \frac{\omega_R^2}{\Omega_R^2} = \frac{1}{4}$ .

Уравнение (2.26) должно быть решено при следующих начальных условиях:

$$\begin{aligned} x|_{t=0} &= C_{b,n+1}(0) = 0, \\ \dot{x}|_{t=0} &= -i \frac{\omega_R}{2} C_{a,n}(0) = -i \frac{\omega_R}{2}. \end{aligned}$$

Результат:

$$x(t) = -ie^{\frac{i\delta t}{2}} \frac{\omega_R}{\sqrt{\omega_R^2 + \delta^2}} \sin\left(\frac{\sqrt{\omega_R^2 + \delta^2}}{2} t\right),$$

обозначив через  $\Omega_R = \sqrt{\omega_R^2 + \delta^2}$  - обобщенную частоту Раби - для искомой вероятности  $|C_{b,n+1}|^2$  получим см. [рис. 2.9](#)

$$|C_{b,n+1}|^2 = \frac{\omega_R^2}{\Omega_R^2} \sin^2 \frac{\Omega_R}{2} t. \quad (2.27)$$

**Комментарий 2.3.1** (Переменный Штарк - эффект). *Стоит отметить, что в случае  $\delta \neq 0$  состояния, которые мы использовали в выражении 2.3 не удовлетворяют закону сохранения энергии. Действительно если система изначально находилась в состоянии  $|a\rangle |n\rangle$  с энергией  $E_a + \hbar n\omega$ , то через некоторое время она, с ненулевой вероятностью, может быть зарегистрирована в состоянии  $|b\rangle |n+1\rangle$  с энергией*

$$E_b + \hbar(n+1)\omega \neq E_a + \hbar n\omega.$$



Рис. 2.10: Интерферометр Рамси. Атом из источника  $S$  последовательно проходит 3 зоны  $R_1$ ,  $C$  и  $R_2$ , на выходе  $D$  происходит определение состояния атома после прохождения 3 зон.



Рис. 2.11: Трехуровневый атом используемый в эксперименте.

Т.е. получается нарушение закона сохранения энергии. Указанное противоречие разрешается следующим образом. В силу переменного Штарк эффекта (в англоязычной литературе этот эффект еще называют AC-Stark effect или Autler-Townes effect)[26], энергетические уровни атома смещаются, что обеспечивает выполнение закона сохранения энергии.

Например, при малых расстройках  $\delta \approx 0$ , это смещение составляет [26]

$$\Delta E \approx \pm \frac{\hbar \omega_R}{2}.$$

## 2.4 Интерферометр Рамси. Квантовые неразрушающие измерения

Наблюдение фотона обычно предполагает его разрушение, например в при использовании фотодетектора энергия фотона преобразуется в электрический сигнал при этом сам фотон исчезает.

Интересный эксперимент [19] использующий осцилляции Раби продемонстрировал возможность наблюдения фотона без его разрушения. При этом использовался интерферометр Рамси (см рис. 2.10)

Схема работы следующая. Используются атомы со структурой уровней изображенной на рис. 2.11. Частота перехода  $\omega_{ab}$  между уровнями  $a$  и  $b$  совпадает с частотой излучения в зонах  $R_1$  и  $R_2$  интерферометра (см рис. 2.10). Зона  $C$  содержит исследуемое электромагнитное поле для которого мы хотим ответить на вопрос есть в нем один фотон или нет, т. е. находится оно

в состоянии  $|1\rangle$  или в вакуумном состоянии  $|0\rangle$ . Исследуемое поле в зоне  $C$  имеет частоту совпадающую с частотой перехода  $\omega_{ac}$  между уровнями  $a$  и  $c$ .

Размер зон  $R_{1,2}$  подбирается таким образом, чтобы время взаимодействия  $t_R$  атома с электромагнитным полем в них соответствовало следующему соотношению

$$\omega_R^{(R)} t_R = \frac{\pi}{2},$$

где  $\omega_R^{(R)}$  частота Раби, соответствующая частоте перехода  $\omega_{ab}$ . Время взаимодействия  $t_C$  в зоне  $C$  определяется выражением

$$\omega_R^{(C)} t_C = 2\pi,$$

где  $\omega_R^{(C)}$  частота Раби, соответствующая частоте перехода  $\omega_{ac}$ .

Для взаимодействия в зонах  $R_{1,2}$  справедливы следующие соотношения (2.24), 2.25:

$$\begin{aligned} |a\rangle &\rightarrow \frac{1}{\sqrt{2}} (|a\rangle - i |b\rangle), \\ |b\rangle &\rightarrow \frac{1}{\sqrt{2}} (-i |a\rangle + |b\rangle). \end{aligned} \quad (2.28)$$

Выражение (2.28) может быть переписано в матричном виде  $|\psi\rangle \rightarrow R |\psi\rangle$ , где

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

Зона  $C$  никак не влияет на состояние  $|b\rangle$ , для состояния  $|a\rangle$  в случае вакуумного состояния  $|0\rangle$  (отсутствия фотона)

$$|a\rangle \rightarrow |a\rangle,$$

т.е. в случае отсутствия фотона состояние атома не меняется. Действительно если рассматривать двухуровневую систему, образованную состояниями  $|a\rangle$  и  $|c\rangle$ , то  $|a\rangle |0\rangle$  будет являться минимально возможным энергетическим состоянием, из которого система (двухуровневый атом и электромагнитное поле) не сможет перейти ни в какое другое состояние. В этом случае для  $C$  имеем

$$C_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Для случая присутствия фотона из (2.24)

$$|a\rangle \rightarrow -|a\rangle,$$

и в этом случае  $C$  имеет вид

$$C_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Таким образом если изначально атом испускаемый источником  $S$  находится в состоянии  $|a\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ , то в случае отсутствия фотона в зоне  $C$  на детекторе  $D$  мы получим атом в состоянии

$$\begin{aligned} R_2 C_0 R_1 |a\rangle &= \\ &= \frac{1}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \\ &= -i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -i |b\rangle, \end{aligned}$$

т.е. атом будет наблюдаться в невозбужденном состоянии  $|b\rangle$ .

Для случая присутствия одного фотона в зоне  $C$  имеем

$$\begin{aligned} R_2 C_1 R_1 |a\rangle &= \\ &= \frac{1}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \\ &= - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = -|a\rangle, \end{aligned}$$

т.е. атом будет наблюдаться в возбужденном состоянии  $|a\rangle$ . Т. о. можно сделать вывод о присутствии фотона в зоне  $C$  без разрушающего воздействия на него.

## 2.5 Взаимодействие атома с многомодовым полем. Вынужденные и спонтанные переходы

Выше мы установили, что вероятность перехода атома из нижнего в верхнее состояние при взаимодействии с одной модой поля, находящейся в состоянии с  $n$  фотонами, равна (2.22)

$$|C_{a,n}(t)|^2 = 4g^2(n+1) \frac{\sin^2((\omega - \omega_{ab})t/2)}{(\omega - \omega_{ab})^2}$$

Запишем эту вероятность в следующем виде

$$P_a = |C_{a,n}(t)|^2 = P_a^{\text{BH}} + P_a^{\text{СП}}, \quad (2.29)$$



где

$$\begin{aligned} P_a^{\text{BH}} &= 4g^2 n \frac{\sin^2((\omega - \omega_{ab}) t/2)}{(\omega - \omega_{ab})^2}, \\ P_a^{\text{СП}} &= 4g^2 \frac{\sin^2((\omega - \omega_{ab}) t/2)}{(\omega - \omega_{ab})^2} \end{aligned} \quad (2.30)$$

вероятности вынужденного ( $P_a^{\text{BH}}$ ) и спонтанного ( $P_a^{\text{СП}}$ ) перехода.

### 2.5.1 Вынужденные переходы

В дальнейшем сосредоточимся на вероятности вынужденного перехода  $P_a^{\text{BH}}$ . Для получения вероятности перехода, учитывая взаимодействие со всеми модами, нужно сложить вероятности (2.30), соответствующие каждой моде.

В случае атома, взаимодействующего с полем свободного пространства (разложение поля по плоским волнам), константа взаимодействия равна [61]:

$$g = -\frac{(\vec{p}\vec{e})}{\hbar} \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}} \quad (2.31)$$

где  $\vec{p}$  - матричный элемент оператора дипольного момента,  $\vec{e}$  - вектор поляризации поля.

Если в выражении (2.30) время  $t$  не очень мало (но существенно меньше, чем характерное время изменения вероятностей), зависимость  $|C_{a,n}(t)|^2$  от частоты будет иметь резкий пик при  $\omega = \omega_{ab}$ , что указывает на сохранение энергии в элементарном акте (энергия поглощенного фотона равна изменению энергии атома). Положим, что падающее в направлении  $\vec{k}$  в телесном угле  $d\Omega$  поле имеет спектр, мало меняющийся вблизи от частоты  $\omega_{ab}$ .

Число мод, приходящихся на интервал частот  $d\omega$  вблизи  $\omega_{ab}$  и телесный угол  $d\Omega$  вокруг направления  $\vec{k}$ , как известно (1.47), равно

$$dN = 2 \left( \frac{L}{2\pi c} \right)^3 \omega^2 d\omega d\Omega \quad (2.32)$$

Вероятность поглощения фотона при взаимодействии атома с одной модой дается формулой (2.30). Полная вероятность может быть получена суммированием по всем модам. Считая спектр мод квазинепрерывным (см. (1.44)), суммирование можно заменить интегрированием

$$W_{b \rightarrow a} = \int_{\Omega} 8|g|^2 n(\vec{k}) \left( \frac{L}{2\pi c} \right)^3 \omega_{ab}^2 d\Omega \int_{-\infty}^{+\infty} \frac{\sin^2((\omega - \omega_{ab}) t/2)}{(\omega - \omega_{ab})^2} d\omega. \quad (2.33)$$

Здесь учтено, что  $\frac{\sin^2 x}{x^2}$  имеет узкий пик вблизи  $x = 0$ , при этом в выражении (2.33) мы предполагаем, что  $t$  мало по сравнению с характерным временем изменения  $C$ , однако, достаточно велико, чтобы проявились фильтрующие свойства интеграла. Все медленно меняющиеся члены взяты при  $\omega = \omega_{ab}$  и вынесены из-под интеграла. Известно, что  $\int_{-\infty}^{+\infty} \frac{\sin^2 x}{x^2} dx = \pi$ . Отсюда легко получить

$$\int_{-\infty}^{+\infty} \frac{\sin^2((\omega - \omega_{ab})t/2)}{(\omega - \omega_{ab})^2} d\omega = \frac{\pi t}{2}.$$

Таким образом, имеем

$$W_{b \rightarrow a} = t \frac{\omega^2 2\pi\omega}{\hbar\epsilon_0 (2\pi c)^3} \int_{\Omega} n(\vec{k}) |(\vec{p}\vec{e})|^2 d\Omega. \quad (2.34)$$

Заметим, что в окончательное выражение объем квантования не вошел, а число фотонов  $n$  зависит от направления, т. е. телесного угла  $\Omega$ . Формула (2.34) показывает, что вероятность перехода пропорциональна времени. Это позволяет ввести понятие скорости перехода, т.е. вероятности перехода в единицу времени

$$w_{b \rightarrow a} = \frac{W_{b \rightarrow a}}{t} = \frac{2\pi\omega^3}{\hbar\epsilon_0 (2\pi c)^3} \int_{\Omega} n(\vec{k}) |(\vec{p}\vec{e})|^2 d\Omega. \quad (2.35)$$

Скорость перехода или скорость поглощения фотона можно выразить [61] через поток энергии (поток фотонов), распространяющихся в направлении  $\vec{k}$  в телесном угле  $d\Omega$ . Поток энергии определяется как энергия, перенесенная через единичную площадь  $dS$  в единицу времени  $dt$  т. е.

$$dI = \frac{dH}{dSdt}.$$

Из рис. 2.12 имеем, что через площадь  $dS$  за единицу времени  $dt$  пройдет столько фотонов, сколько их содержится в цилиндре изображенном на рис. 2.12, т. е. перенесенная энергия может быть записана как

$$dH = n\hbar\omega dN,$$

где  $dN$  - число мод, приходящихся на интервал  $d\omega d\Omega$  в рассматриваемом объеме  $c \cdot dSdt$  (1.47):

$$dN = 2 \left( \frac{1}{2\pi c} \right)^3 \omega^2 c \cdot dSdt d\omega d\Omega,$$

откуда имеем

$$dI = I(\omega, \vec{k}) d\omega d\Omega = \frac{2n\hbar\omega c}{(2\pi c)^3} \omega^2 d\omega d\Omega, \quad (2.36)$$



Рис. 2.12: К определению потока энергии (потока фотонов). Поток энергии определяется как энергия  $dH$ , перенесенная через площадь  $dS$  в единицу времени  $dt$ . Эту энергию можно определить через число фотонов в цилиндре объемом  $V$ .

где  $I(\omega, \vec{k})$  - поток энергии фотонов в направлении  $\vec{k}$ , приходящийся на единичный интервал частот и единичный телесный угол. Таким образом из (2.36) получим

$$I(\omega, \vec{k}) = \frac{2n\hbar\omega^3 c}{(2\pi c)^3}$$

Подставляя это в выражение (2.35), получим:

$$w_{ab} = \frac{\pi}{\hbar^2} \sqrt{\frac{\mu_o}{\varepsilon_0}} \int_{\Omega} I(\omega, \vec{k}) |(\vec{p}\vec{e})|^2 d\Omega. \quad (2.37)$$

Здесь использовано соотношение  $\mu_0 \varepsilon_0 = \frac{1}{c^2}$ .

Для того чтобы найти полную скорость поглощения, нужно проинтегрировать (2.37) по всем направлениям распространения волн. Кроме того, падающее излучение обычно бывает неполяризовано. Чтобы это учесть, нужно произвести усреднение по всем направлениям поляризации. Воспользуемся системой координат, изображенной на рис. 2.13. В качестве полярной оси  $z$  выбрано направление  $\vec{k}$ . Векторы поляризации  $\vec{e}_1$  и  $\vec{e}_2$  направлены по  $x$  и  $y$  соответственно. Углы  $\varphi$  и  $\theta$  определяют направление  $\vec{p}$ . Угол  $\varphi'$  определяет направление поляризации падающей волны. Из рисунка видно, что

$$|(\vec{p}\vec{e})|^2 = |p|^2 \sin^2 \theta \cos^2 \varphi'.$$

Усреднение по всем поляризациям дает:

$$\frac{|p|^2}{2\pi} \int_0^{2\pi} \cos^2 \varphi' d\varphi' = \frac{|p|^2}{2}. \quad (2.38)$$

Суммирование по всем направлениям прихода волн приводит к выражению

$$w_{ab} = \frac{\pi}{2\hbar^2} \sqrt{\frac{\mu_o}{\varepsilon_0}} |p|^2 \int_{\Omega} I(\omega, \vec{k}) \sin^3 \theta d\theta d\varphi. \quad (2.39)$$



Рис. 2.13: Система координат в которой удобно произвести усреднение многодогового поля по всем направлениям и поляризациям. Волновой вектор электромагнитной волны  $\vec{k}$  направлен по оси  $z$ , при этом положение матричного элемента дипольного момента  $\vec{p}$  определяется углами  $\theta$  и  $\phi$ . Векторы поляризации  $\vec{e}_1$  и  $\vec{e}_2$  направлены по осям  $x$  и  $y$ . Угол  $\phi'$  определяет направление поляризации электромагнитной волны.

Считая, что излучение приходит со всех направлений и изотропно, получим:

$$w_{ab} = \frac{\pi}{2\hbar^2} \sqrt{\frac{\mu_o}{\varepsilon_0}} |p|^2 I(\omega) \int_0^{2\pi} d\varphi \int_0^\pi \sin^3 \theta d\theta = \frac{\pi}{\hbar^2} \sqrt{\frac{\mu_o}{\varepsilon_0}} \frac{|p|^2}{3} I_0, \quad (2.40)$$

где  $I_0 = 4\pi I(\omega)$  - полный поток энергии, падающий на атом. При выводе (2.40) мы воспользовались следующим соотношением:

$$\int_0^\pi \sin^3 \theta d\theta = \frac{4}{3}$$

Если же излучение приходит из малой области  $\Delta\Omega$  направлений вблизи углов  $\theta_0, \varphi_0$ , то можем написать:

$$\begin{aligned} w_{ab} &= \frac{\pi}{2\hbar^2} \sqrt{\frac{\mu_o}{\varepsilon_0}} |p|^2 \sin^2 \theta_0 \int_{\Delta\Omega} I(\theta, \varphi) d\Omega = \\ &= \frac{\pi}{2\hbar^2} \sqrt{\frac{\mu_o}{\varepsilon_0}} |p|^2 I_0 \sin^2 \theta_0, \end{aligned} \quad (2.41)$$

где  $I_0 = \int_{\Delta\Omega} I(\theta, \varphi) d\Omega$  - полный поток, облучающий атом.

## 2.5.2 Спонтанные переходы

Рассмотрим теперь другую задачу. Определим вероятность излучения фотона или перехода возбужденного атома в нижнее состояние.

Для вероятности излучения атомом фотона в одну моду мы имели выражение (2.23):

$$|C_{b,n+1}(t)|^2 = 4g^2(n+1) \frac{\sin^2((\omega - \omega_{ab})t/2)}{(\omega - \omega_{ab})^2},$$

которое также как (2.29) можно рассматривать в виде суммы двух слагаемых

$$P_b = |C_{b,n+1}(t)|^2 = P_b^{\text{ВН}} + P_b^{\text{СП}}$$

где первое слагаемое

$$P_b^{\text{ВН}} = 4g^2n \frac{\sin^2((\omega - \omega_{ab})t/2)}{(\omega - \omega_{ab})^2}$$

соответствует вынужденному излучению, а второе

$$P_b^{\text{СП}} = 4g^2 \frac{\sin^2((\omega - \omega_{ab})t/2)}{(\omega - \omega_{ab})^2}$$

спонтанному. Член, соответствующий вынужденному излучению, рассматривается таким же образом, как и в случае поглощения фотона. Результат будет, очевидно, тем же самым. Соответствующие формулы будут совпадать с (2.40), (2.41). Отсюда следует, что вероятности вынужденных процессов поглощения и излучения равны между собой. Вероятность спонтанного излучения в единицу времени, очевидно, будет равна

$$w_{\text{СП}} = \frac{2\pi\omega^3}{\hbar\varepsilon_0(2\pi c)^3} \int_{\Omega} |(\vec{p}\vec{e})|^2 d\Omega \quad (2.42)$$

Для того чтобы получить полную вероятность, нужно (2.42) проинтегрировать по всем направлениям, так как спонтанное излучение может происходить в любую моду. Для поляризаций - воспользуемся средним значением (2.38). Таким образом вся процедура сведется к вычислению интеграла

$$w_{\text{СП}} = \frac{|p|^2 \omega^3}{\varepsilon_0 \hbar (2\pi)^2 c^3} \int_0^{2\pi} d\varphi \int_0^\pi \sin^3 \theta d\theta = \frac{4\pi}{3} \frac{|p|^2 \omega^3}{\hbar \varepsilon_0 (2\pi)^2 c^3} \quad (2.43)$$

Окончательно получаем

$$w_{\text{СП}} = \frac{|p|^2 \omega^3}{3\pi c^2 \hbar} \sqrt{\frac{\mu_0}{\varepsilon_0}} \quad (2.44)$$

Здесь использовано соотношение

$$\frac{1}{c} = \sqrt{\mu_0 \varepsilon_0}$$

Формула (2.44) указывает на сильную зависимость вероятности спонтанного перехода от частоты, как  $\omega^3$ . Таким образом, исходя из уравнений квантовой электродинамики, мы непосредственно, не привлекая посторонних соображений, получили выражения для вероятностей вынужденных и спонтанных переходов атомов в единицу времени. Недостатком рассмотрения является использование теории возмущения и, следовательно, необходимость ограничиваться малыми временами. Решая, например, задачу о времени жизни возбужденного атома, нельзя уже ограничиваться малыми временами. В этом случае применяется другое приближение, называемое приближением Вайскопфа-Вигнера [61]. Интересно, что результаты, полученные в этих двух случаях, не противоречат друг другу.

## 2.6 Спонтанное излучение. Приближение Вайскопфа-Вигнера.

Выше нами получена формула для скорости спонтанного излучения, справедливая для достаточно малых времен. В то же время решая, например, задачу о времени жизни возбужденного атома, нельзя ограничиваться малыми временами. В этом случае применяется уже другой метод, называемый приближением Вайскопфа-Вигнера.

Рассмотрим этот метод. Мы выяснили, что атом переходит из возбужденного состояния в основное из-за взаимодействия со всеми модами пространства, даже если они не возбуждены и находятся в вакуумном состоянии. Гамильтониан взаимодействия в этом случае имеет вид

$$\hat{V}_I = \hbar \sum_k g_k \hat{\sigma}^\dagger \hat{a}_k e^{i(\omega_{ab} - \omega_k)t} + \text{э. с.}, \quad (2.45)$$

где  $g_k$  константа взаимодействия с  $k$ -ой модой. От ранее использованного нами гамильтониана (2.14) (2.45) отличается суммированием по всем модам пространства квантования.

Допустим, что в начальный момент времени  $t = 0$  атом возбужден, а в поле отсутствуют фотоны. Тогда начальное состояние имеет вид

$$|\psi(0)\rangle = |a, \{0\}\rangle,$$

то есть атом возбужден, а все моды находятся в вакуумном состоянии. В последующие времена из-за взаимодействия атом-поле, состояние системы будет иметь вид

$$|\psi(t)\rangle = \sum_k C_{bk}(t) |b, 1_k\rangle + C_a(t) |a, \{0\}\rangle, \quad (2.46)$$

где  $|b, 1_k\rangle$  состояние, когда атом находится в основном состоянии, а в  $k$ -ой моде возбужден один фотон.

Уравнение Шредингера в представлении взаимодействия имеет вид

$$\frac{d}{dt} |\psi(t)\rangle = -\frac{i}{\hbar} \hat{V}_I |\psi(t)\rangle. \quad (2.47)$$

Подставляя сюда (2.46) и умножая уравнение (2.47) последовательно на  $\langle a, \{0\}|$  и  $\langle b, 1_k|$  получаем систему уравнений для амплитуд вероятностей  $C_a(t)$  и  $C_{bk}(t)$ .

$$\begin{aligned} \dot{C}_a(t) &= -i \sum_k g_k e^{i(\omega_{ab}-\omega_k)t} C_{bk}(t), \\ \dot{C}_{bk}(t) &= -i g_k e^{-i(\omega_{ab}-\omega_k)t} C_a(t). \end{aligned} \quad (2.48)$$

Проинтегрируем второе уравнение (2.48) по времени от 0 до  $t$ .

$$C_{bk}(t) = -i g_k \int_0^t e^{-i(\omega_{ab}-\omega_k)t'} C_a(t') dt'. \quad (2.49)$$

Подставив (2.49) в первое уравнение системы (2.48), получим следующее интегро-дифференциальное уравнение

$$\dot{C}_a(t) = - \sum_k g_k^2 \int_0^t e^{i(\omega_{ab}-\omega_k)(t-t')} C_a(t') dt'. \quad (2.50)$$

Сделаем теперь ряд упрощений (приближение Вайскопфа-Вигнера). Будем считать распределение мод квазинепрерывным и заменим суммирование по  $k$  интегрированием, используя соотношение (1.46):

$$dN = 2 \left( \frac{L}{2\pi} \right)^3 k^2 dk d\Omega = 2 \frac{V}{(2\pi)^3} k^2 dk d\Omega$$

Тогда получим (1.44)

$$\begin{aligned} & \sum_k g_k^2 \int_0^t e^{i(\omega_{ab}-\omega_k)(t-t')} C_a(t') dt' = \\ &= 2 \frac{V}{(2\pi)^3} \int_{4\pi} d\Omega \int_0^\infty g_k^2 k^2 dk \int_0^t dt' e^{i(\omega_{ab}-\omega_k)(t-t')} C_a(t'). \end{aligned} \quad (2.51)$$

В (2.51)

$$g_k^2 = \frac{\omega_k |p|^2 \sin^2 \theta}{4\hbar \varepsilon_0 V}, \quad (2.52)$$

$\theta$  - угол между направлениями  $\vec{k}$  и  $\vec{p}$ . Выражение (2.52) получено с учетом усреднения по поляризациям (2.38).

Переходя в (2.51) от  $k$  к  $\omega$  с помощью соотношений

$$k = \frac{\omega_k}{c}, \quad k^2 dk = \frac{\omega_k^2 d\omega_k}{c^3}$$

и обозначая для удобства  $\omega_k = \omega$ , получим

$$\dot{C}_a(t) = -2 \frac{V}{(2\pi c)^3} \int_{4\pi} d\Omega \int_0^\infty g^2(\omega) \omega^2 d\omega \int_0^t dt' e^{i(\omega_{ab}-\omega)(t-t')} C_a(t'). \quad (2.53)$$

Для приближенного вычисления интеграла в (2.53) дополнительно используем ряд упрощающих допущений. Проинтегрируем (2.53) сперва по частоте (т. е. меняем порядок интегрирования, считая что это возможно). Из структуры (2.53) видно, что главный вклад в интеграл по времени дает область частот  $\omega \approx \omega_{ab}$ . По этой причине можно принять

$$\omega^2 g^2(\omega) \approx \omega_{ab}^2 g^2(\omega_{ab}).$$

В этом приближении интеграл по частоте будет иметь вид (см. интегральное представление дельта-функции (18.3)):

$$\begin{aligned} \int_0^\infty d\omega e^{i(\omega_{ab}-\omega)(t-t')} &= |\nu = \omega - \omega_{ab}| = \int_{-\omega_{ab}}^\infty d\nu e^{-i\nu(t-t')} \approx \\ &\approx \int_{-\infty}^\infty d\nu e^{-i\nu(t-t')} = \int_{-\infty}^\infty d\nu e^{i\nu(t'-t)} = 2\pi \delta(t' - t). \end{aligned} \quad (2.54)$$

Подставляя (2.54) в уравнение (2.53) и интегрируя по времени, получаем

$$\dot{C}_a(t) = -2 \frac{V}{(2\pi c)^3} \int_{4\pi} d\Omega g^2(\omega_{ab}) \omega_{ab}^2 2\pi C_a(t) = -\frac{\Gamma}{2} C_a(t). \quad (2.55)$$

Подставив сюда выражение для  $g_k^2$  (2.52) и производя интегрирование по углам (по  $d\Omega$ ), найдем выражение для коэффициента затухания  $\Gamma$ :

$$\Gamma = \frac{\omega_{ab}^3 |p|^2}{3\pi c^2 \hbar} \sqrt{\frac{\mu_0}{\varepsilon_0}}. \quad (2.56)$$



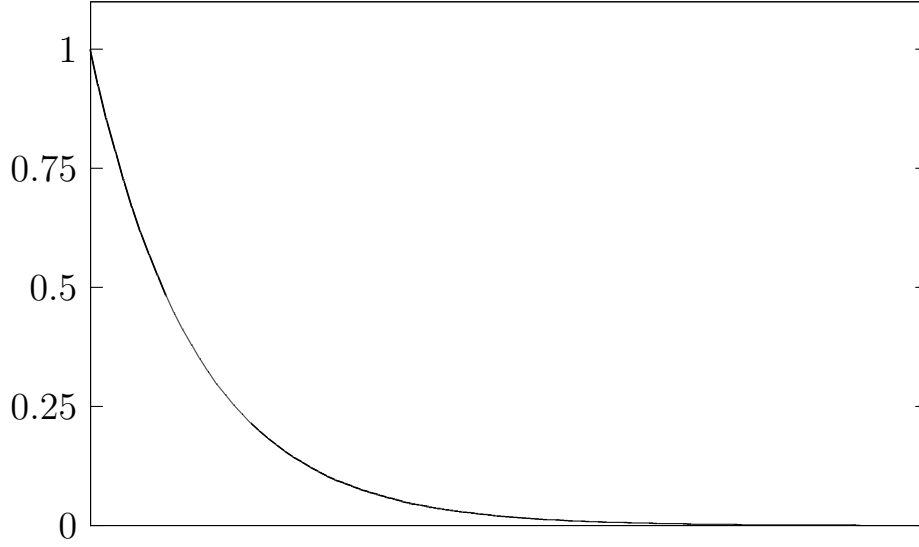


Рис. 2.14: Зависимость вероятности обнаружить атом в возбужденном состоянии  $|C_a|^2$  в приближении Вайскопфа-Вигнера

Заметим, что выражение (2.56) совпадает с полученным ранее другим способом (2.44).

Из (2.55) следует, что  $\Gamma$  характеризует скорость изменения вероятности  $|C_a|^2$ . Действительно из (2.55) имеем:

$$\begin{aligned}\dot{C}_a C_a^* &= -\frac{\Gamma}{2} C_a C_a^*, \\ \dot{C}_a^* C_a &= -\frac{\Gamma}{2} C_a^* C_a,\end{aligned}$$

откуда имеем

$$\frac{dC_a C_a^*}{dt} = -\Gamma (C_a C_a^*),$$

или иначе

$$\frac{d|C_a|^2}{dt} = -\Gamma |C_a|^2.$$

Решение имеет вид (см. рис. 2.14)

$$|C_a|^2 = e^{-\Gamma t},$$

если начальное значение  $|C_a|^2|_{t=0} = 1$ , т. е. атом в начале был возбужден.

**Комментарий 2.6.1** (Приближение Вайскопфа-Вигнера и осцилляции Раби). Если мы сравним рис. 2.8 и рис. 2.14 то сможем увидеть, что эти два графика очень сильно отличаются несмотря на то что описывают вроде

бы одну и ту же модельную систему. В связи с этим возникает вопрос когда мы можем применять одномодовое приближение, и соответственно получать осцилляции Раби (см. [рис. 2.8](#)), а в каких случаях необходимо пользоваться многомодовым приближением типа Вайскопфа-Вигнера (см. [рис. 2.14](#)).

Формально мы можем считать что взаимодействие с каждой модой электромагнитного поля дает свой вклад в результирующие вероятности, вместе с тем в соответствии (2.23) изменение вероятности (при малых  $t$ )

$$\Delta |C_{a,n}(t)|^2 = -\Delta |C_{b,n+1}(t)|^2 \sim (n+1).$$

Т. о. те моды в которых число фотонов велико дает больший вклад, чем те в которых оно мало. Следовательно, если у нас имеется мода с большим числом фотонов  $n \gg 1$ , то влиянием вакуумных мод с числом фотонов  $n = 0$  в этом случае можно пренебречь. В противном случае, особенно если все моды равноправны, необходимо учитывать все моды и применять приближения типа Вайскопфа-Вигнера.

## 2.7 Релаксация динамической системы. Метод матрицы плотности

В квантовой электронике и квантовой оптике мы имеем дело с открытыми системами. Такие системы необходимо рассматривать при помощи матрицы плотности. Рассматривается малая динамическая система (атом, молекулы, мода резонатора и т.п.), слабо связанная с большой системой, называемой резервуаром (диссипативной системой, термостатом), состоящим из большого числа атомов, молекул или осцилляторов, находящихся в равновесии при определенной температуре. Таким образом, в общем случае рассматриваем динамическую систему ( $A$ ), взаимодействующую с резервуаром ( $B$ ) (см. [рис. 2.15](#)). Оператор плотности комбинированной системы ( $AB$ ) обозначим  $\hat{\rho}_{AB}$ . Свернутый по переменным резервуара (термостата) оператор плотности описывает поведение динамической системы с учетом усредненного взаимодействия с термостатом. Имеем:

$$\hat{\rho}_A = \text{Sp}_B \hat{\rho}_{AB} = \sum_{(B)} \langle B | \hat{\rho}_{AB} | B \rangle. \quad (2.57)$$

В начальный момент времени  $t_0$  динамическая система и резервуар рассматриваются как независимые (некоррелированные). Тогда

$$\hat{\rho}_{AB}(t_0) = \hat{\rho}_A(t_0) \otimes \hat{\rho}_B(t_0) \quad (2.58)$$

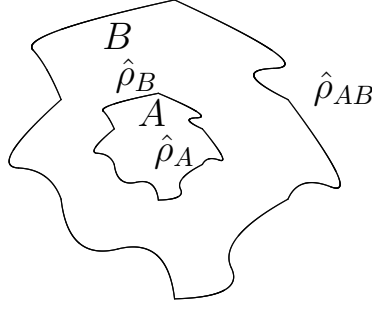


Рис. 2.15: Взаимодействие динамической системы  $A$  с резервуаром  $B$

где  $S\rho_B\hat{\rho}_B = 1$ ,  $\otimes$  - знак внешнего или тензорного произведения.

Уравнение движения оператора плотности в представлении взаимодействия имеет вид

$$\frac{d}{dt}\hat{\rho}_{AB} = -\frac{i}{\hbar} [\hat{V}_{AB}, \hat{\rho}_{AB}],$$

где  $\hat{V}_{AB}$  - гамильтониан взаимодействия между системами  $A$  и  $B$ . Решить это уравнение можно с помощью следующего итерационного процесса.

$$\hat{\rho}_{AB}(t) = \hat{\rho}_{AB}^{(0)}(t) + \hat{\rho}_{AB}^{(1)}(t) + \hat{\rho}_{AB}^{(2)}(t) + \dots, \quad (2.59)$$

где член  $\hat{\rho}_{AB}^{(0)}(t)$  находится в предположении отсутствия взаимодействия, т. е.

$$\hat{\rho}_{AB}^{(0)}(t) = \hat{\rho}_{AB}(t_0) = \hat{\rho}_A(t_0) \otimes \hat{\rho}_B(t_0).$$

Последующие члены итерационного соотношения (2.59) задаются следующим соотношением

$$\begin{aligned} \hat{\rho}_{AB}^{(s)}(t) &= -\frac{i}{\hbar} \int_{t_0}^t dt_s [\hat{V}_{AB}(t_s), \hat{\rho}_{AB}^{(s-1)}(t_s)] = \\ &= \left(-\frac{i}{\hbar}\right)^s \int_{t_0}^t dt_s \int_{t_0}^{t_s} dt_{s-1} \dots \\ &\dots \int_{t_0}^{t_2} dt_1 [\hat{V}_{AB}(t_s), [\hat{V}_{AB}(t_{s-1}), \dots [\hat{V}_{AB}(t_1), \hat{\rho}_{AB}^{(0)}(t_0)] \dots]] = \\ &= \left(-\frac{i}{\hbar}\right)^s \int_{t_0}^t dt_s \int_{t_0}^{t_s} dt_{s-1} \dots \\ &\dots \int_{t_0}^{t_2} dt_1 [\hat{V}_{AB}(t_s), [\hat{V}_{AB}(t_{s-1}), \dots [\hat{V}_{AB}(t_1), \hat{\rho}_A(t_0) \otimes \hat{\rho}_B(t_0)] \dots]] \end{aligned} \quad (2.60)$$

Подставляя (2.60) в (2.59) и производя усреднение по переменным термо-

стата получим

$$\begin{aligned} \hat{\rho}_A(t) = \hat{\rho}_A(t_0) + \\ + Sp_B \sum_{(s)} \left( -\frac{i}{\hbar} \right)^s \int_{t_0}^t dt_s \int_{t_0}^{t_s} dt_{s-1} \dots \\ \dots \int_{t_0}^{t_2} dt_1 \left[ \hat{V}_{AB}(t_s), \left[ \hat{V}_{AB}(t_{s-1}), \dots \left[ \hat{V}_{AB}(t_1), \hat{\rho}_A(t_0) \otimes \hat{\rho}_B(t_0) \right] \dots \right] \right]. \end{aligned} \quad (2.61)$$

Обычно ограничиваются несколькими первыми членами разложения. Например, первые два члена разложения равны

$$\begin{aligned} \hat{\rho}_A(t) = \hat{\rho}_A(t_0) - \frac{i}{\hbar} Sp_B \left\{ \int_{t_0}^t \left[ \hat{V}_{AB}(t_1), \hat{\rho}_A(t_0) \otimes \hat{\rho}_B(t_0) \right] dt_1 \right\} - \\ - \frac{1}{\hbar^2} Sp_B \left\{ \int_{t_0}^t dt_2 \int_{t_0}^{t_2} dt_1 \left[ \hat{V}_{AB}(t_2), \left[ \hat{V}_{AB}(t_1), \hat{\rho}_A(t_0) \otimes \hat{\rho}_B(t_0) \right] \right] \right\}. \end{aligned}$$

## 2.8 Взаимодействие электромагнитного поля резонатора с резервуаром атомов, находящихся при температуре $T$

Применим общий подход, изложенный выше, к системе, состоящей из гармонического осциллятора (электромагнитного поля моды), взаимодействующего с резервуаром в виде атомного пучка двухуровневых атомов, находящихся в равновесии при температуре  $T$ . Как мы увидим в дальнейшем, конкретная модель резервуара для окончательного результата значения не имеет.<sup>1</sup> Рассматриваемая модель изображена на [рис. 2.16](#).

Начальная атомная матрица плотности соответствует распределению Больцмана при температуре  $T$ :

$$\hat{\rho}_{at} = \begin{pmatrix} \rho_{aa} & 0 \\ 0 & \rho_{bb} \end{pmatrix} = z^{-1} \begin{pmatrix} e^{-\frac{\hbar\omega_a}{k_B T}} & 0 \\ 0 & e^{-\frac{\hbar\omega_b}{k_B T}} \end{pmatrix}. \quad (2.62)$$

Здесь  $\hbar\omega_a = E_a$  - энергия верхнего уровня;  $\hbar\omega_b = E_b$  - энергия нижнего уровня;  $z = e^{-\frac{\hbar\omega_a}{k_B T}} + e^{-\frac{\hbar\omega_b}{k_B T}}$  статистическая сумма;  $T$  - температура резервуара. Гамильтониан взаимодействия возьмем в виде (2.14). Положим для простоты, что  $\omega_{ab} = \omega$ , т. е. частота перехода равна частоте моды. Тогда

$$\hat{V} = \hbar g (\hat{\sigma} \hat{a}^\dagger + \hat{\sigma}^\dagger \hat{a}) = \hbar g \begin{pmatrix} 0 & \hat{a} \\ \hat{a}^\dagger & 0 \end{pmatrix} \quad (2.63)$$

<sup>1</sup>Если взаимодействие слабое, т. е. энергия связи мала по сравнению с энергией динамической системы.

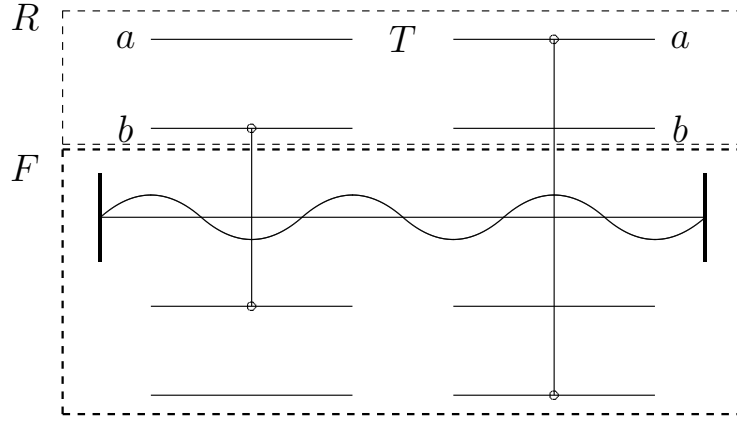


Рис. 2.16: Взаимодействие электромагнитного поля резонатора  $F$  с резервуаром атомов  $R$ , находящихся при температуре  $T$

так как  $\hat{\sigma} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ ;  $\hat{\sigma}^\dagger = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ;  $g$  - константа взаимодействия.

Сохраним в итерационном ряде (2.61) члены до второго порядка включительно. В нашем случае после интегрирования получается простое выражение

$$\begin{aligned} \hat{\rho}_f(t) &= \hat{\rho}_f(t_0 + \tau) = \\ &= \hat{\rho}_f(t_0) + Sp_{at} \left\{ -\frac{i}{\hbar} \tau [\hat{V}, \hat{\rho}_{at,f}] - \frac{1}{2} \left( \frac{\tau}{\hbar} \right)^2 [\hat{V}, [\hat{V}, \hat{\rho}_{at,f}]] \right\}, \end{aligned} \quad (2.64)$$

где  $\hat{\rho}_{at,f}$  - статистический оператор системы атом-поле;  $\hat{\rho}_f$  статистический оператор поля, свернутый по атомным переменным.

При получении (2.64) предполагалось, что атом пучка взаимодействует с полем за время  $\tau$  (время пролета через резонатор). Из начальных условий (во время  $t_0$ ) имеем:

$$\hat{\rho}_{at,f} = \hat{\rho}_f \begin{pmatrix} \rho_{aa} & 0 \\ 0 & \rho_{bb} \end{pmatrix} = \begin{pmatrix} \rho_{aa} \hat{\rho}_f & 0 \\ 0 & \rho_{bb} \hat{\rho}_f \end{pmatrix} \quad (2.65)$$

Член первого порядка в (2.64) дает матрицу с нулевыми диагональными элементами по переменным резервуара. След матрицы по этим переменным очевидно равен нулю

$$\begin{aligned} Sp_{at} [\hat{V}, \hat{\rho}_{at,f}] &= \hbar g Sp_{at} \left\{ \begin{pmatrix} 0 & \hat{a} \rho_{bb} \hat{\rho}_f \\ \hat{a}^\dagger \rho_{aa} \hat{\rho}_f & 0 \end{pmatrix} - \right. \\ &\quad \left. - \begin{pmatrix} 0 & \rho_{aa} \hat{\rho}_f \hat{a} \\ \rho_{bb} \hat{\rho}_f \hat{a}^\dagger & 0 \end{pmatrix} \right\} = 0. \end{aligned} \quad (2.66)$$

Матрица, входящая в член второго порядка, имеет отличные от нуля диагональные элементы, след от нее по переменным резервуара отличен от 0 и

может быть вычислен:

$$\begin{aligned} Sp_{at} \left[ \hat{V}, \left[ \hat{V}, \hat{\rho}_{at,f} \right] \right] &= \hbar^2 g^2 \cdot \\ \cdot Sp_{at} \left( \begin{array}{cc} \hat{a}\hat{a}^\dagger \rho_{aa} \hat{\rho}_f - \hat{a} \rho_{bb} \hat{\rho}_f \hat{a}^\dagger & 0 \\ 0 & \hat{a}^\dagger \hat{a} \rho_{bb} \hat{\rho}_f - \hat{a}^\dagger \rho_{aa} \hat{\rho}_f \hat{a} \end{array} \right) &+ \text{э. с.} \end{aligned} \quad (2.67)$$

Отсюда, используя уравнения (2.64), (2.66), (2.67), получаем окончательное уравнение для статистического оператора поля  $\hat{\rho}$ :

$$\begin{aligned} \hat{\rho}_f(t_0 + \tau) &= \hat{\rho}_f(t_0) - \frac{1}{2} g^2 \tau^2 \{ (\hat{a}\hat{a}^\dagger \hat{\rho}_f - \hat{a}^\dagger \hat{\rho}_f \hat{a}) \rho_{aa} + \\ &+ (\hat{a}^\dagger \hat{a} \hat{\rho}_f - \hat{a} \hat{\rho}_f \hat{a}^\dagger) \rho_{bb} \} + \text{э. с.} \end{aligned} \quad (2.68)$$

Таким образом, статистический оператор моды из-за взаимодействия с одним атомом изменится на величину  $\delta \hat{\rho}_f = \hat{\rho}_f(t_0 + \tau) - \hat{\rho}_f(t_0)$ , определяемую (2.68). Если скорость инжекции атомов в резонатор  $r$  атомов в секунду, за время  $\Delta t$  провзаимодействуют  $r \Delta t$  атомов. Изменение оператора плотности за это время будет равно  $\Delta \hat{\rho}_f = \delta \hat{\rho}_f r \Delta t$ . Определим сглаженную производную как

$$\dot{\hat{\rho}}_f = \frac{\Delta \hat{\rho}_f}{\Delta t} = \delta \hat{\rho}_f r = r (\hat{\rho}_f(t_0 + \tau) - \hat{\rho}_f(t_0)).$$

Обозначим:  $r_a = r \rho_{aa}$  - скорость инжекции атомов, находящихся в верхнем состоянии;  $r_b = r \rho_{bb}$  - скорость инжекции атомов, находящихся в нижнем состоянии. Это приводит нас к окончательному виду уравнения для статистического оператора поля моды резонатора

$$\begin{aligned} \dot{\hat{\rho}}_f &= -\frac{1}{2} R_a (\hat{a}\hat{a}^\dagger \hat{\rho}_f - \hat{a}^\dagger \hat{\rho}_f \hat{a}) - \\ &- \frac{1}{2} R_b (\hat{a}^\dagger \hat{a} \hat{\rho}_f - \hat{a} \hat{\rho}_f \hat{a}^\dagger) + \text{э. с.} \end{aligned} \quad (2.69)$$

Здесь обозначено

$$\begin{aligned} R_a &= r_a g^2 \tau^2, \\ R_b &= r_b g^2 \tau^2. \end{aligned} \quad (2.70)$$

Уравнение (2.69) написано в операторном виде. Его можно написать в различных представлениях.

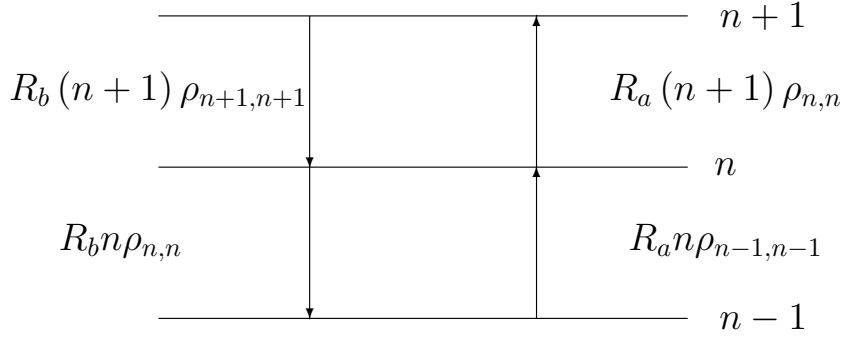


Рис. 2.17: Баланс потоков вероятностей чисел фотонов

## 2.9 Уравнение для матрицы плотности поля в представлении чисел заполнения

В представлении чисел заполнения (чисел фотонов) матричные элементы определяются равенством

$$\rho_{nm} = \langle n | \hat{\rho} | m \rangle.$$

Для получения нужного уравнения помножим (2.69) слева на  $\langle n |$  и справа на  $|m\rangle$ . Пользуясь свойствами операторов  $\hat{a}$  и  $\hat{a}^\dagger$ , получим систему уравнений, связывающих между собой матричные элементы

$$\begin{aligned} \dot{\rho}_{nm} = & -\frac{1}{2} (R_a (n+1+m+1) + R_b (n+m)) \rho_{nm} + \\ & + R_a \sqrt{nm} \rho_{n-1,m-1} + R_b \sqrt{(n+1)(m+1)} \rho_{n+1,m+1}. \end{aligned} \quad (2.71)$$

Для диагональных элементов  $n = m$ , следовательно

$$\begin{aligned} \dot{\rho}_{nn} = & - (R_a (n+1) + R_b (n)) \rho_{nn} + \\ & + R_a n \rho_{n-1,n-1} + R_b (n+1) \rho_{n+1,n+1}. \end{aligned} \quad (2.72)$$

Это уравнение можно рассматривать как баланс потоков вероятностей чисел фотонов. Условно это изображено на рис. 2.17. В тепловом равновесии потоки должны быть равны. Отсюда, используя принцип детального равновесия, получим равенства:

$$\begin{aligned} R_a n \rho_{n-1,n-1} &= R_b n \rho_{nn}, \\ R_a (n+1) \rho_{nn} &= R_b (n+1) \rho_{n+1,n+1} \end{aligned} \quad (2.73)$$

Из (2.73) имеем

$$\rho_{n+1,n+1} = \frac{R_a}{R_b} \rho_{nn} = e^{-\frac{\hbar\omega}{k_B T}} \rho_{nn}, \quad (2.74)$$

так как  $\frac{R_a}{R_b} = \exp\left(-\frac{\hbar\omega}{k_B T}\right)$  (резервуар находится в равновесии при температуре  $T$ ). Используя последовательно (2.74), начиная с  $n = 0$ , получим:

$$\rho_{nn} = \rho_{00} e^{-\frac{n\hbar\omega}{k_B T}} = \left(1 - e^{-\frac{\hbar\omega}{k_B T}}\right) e^{-\frac{n\hbar\omega}{k_B T}}, \quad (2.75)$$

где  $\rho_{00}$  найдено из условия  $\sum_{(n)} \rho_{nn} = 1$ .

Среднее число фотонов в моде, как и следовало ожидать, определяется формулой Планка

$$\bar{n} = \langle n \rangle = \sum_{(n)} n \rho_{nn} = \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1}. \quad (2.76)$$

Из всего сказанного следует, что со временем температура излучения становится равной температуре атомного пучка (резервуара). Изменение среднего числа фотонов во времени получим из уравнения (2.72)

$$\begin{aligned} \frac{d}{dt} \langle n(t) \rangle &= \sum_{(n)} n \dot{\rho} = \\ &= \sum_{(n)} \left( -R_a (n^2 + n) \rho_{nn} - R_b n^2 \rho_{nn} + \right. \\ &\quad \left. + R_b (n^2 + n) \rho_{n+1, n+1} + R_a n^2 \rho_{n-1, n-1} \right). \end{aligned} \quad (2.77)$$

Заменим переменные суммирования  $m = n + 1$  в третьей сумме и  $m = n - 1$  в четвертой сумме. Получим:

$$\begin{aligned} \frac{d}{dt} \langle n \rangle &= -R_a \sum_{(n)} (n^2 + n) \rho_{nn} - R_b \sum_{(n)} n^2 \rho_{nn} + \\ &+ R_b \sum_{(m)} (m^2 - m) \rho_{m, m} + R_a \sum_{(m)} (m^2 + 2m + 1) \rho_{m, m} = \\ &= R_a \sum_{(m)} (m + 1) \rho_{m, m} - R_b \sum_{(m)} m \rho_{m, m} = \\ &= (R_a - R_b) \langle n \rangle + R_a. \end{aligned} \quad (2.78)$$

В равновесии

$$\frac{d}{dt} \langle n \rangle = 0,$$

и мы получаем прежнее соотношение

$$\langle n_{(\infty)} \rangle = \bar{n} = \frac{R_a}{R_b - R_a} = \frac{1}{\frac{R_b}{R_a} - 1} = \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1}. \quad (2.79)$$



**Определение 2.9.1** (Добротность). Добротностью колебательной системы  $Q$  называют [47] число колебаний совершаемое системой за характерное время их затухания  $\tau$ . Т.е. если изменение энергии системы  $U$  (комплексная амплитуда) подчиняется уравнению

$$\frac{dU}{dt} = -\frac{1}{\tau} (U - U_0), \quad (2.80)$$

то

$$U = (U|_{t=0} - U_0) e^{-\frac{t}{\tau}} + U_0$$

Т. о.

$$Q = \omega\tau$$

следовательно уравнение (2.80) может быть переписано в виде

$$\frac{dU}{dt} = -\frac{\omega}{Q} (U - U_0)$$

Уравнение (2.78) описывает изменение числа фотонов (энергии) во времени в результате релаксации (взаимодействия с диссипативной системой). Классическое уравнение, описывающее этот процесс имеет вид (см. опред. 2.9.1)

$$\frac{d}{dt} \langle n \rangle = -\frac{\omega}{Q} \langle n \rangle + \frac{\omega}{Q} \langle n \rangle_{\text{рав.}},$$

где  $\langle n \rangle_{\text{рав.}} = \bar{n}_T$  равновесное значение  $\langle n \rangle$  при температуре  $T$ , а  $Q$  - добротность резонатора (см. опред. 2.9.1). Следовательно можно положить

$$\begin{aligned} R_b - R_a &= \frac{\omega}{Q}, \\ R_a &= \bar{n}_T \frac{\omega}{Q}, \\ R_b &= \frac{\omega}{Q} (1 + \bar{n}_T), \end{aligned} \quad (2.81)$$

т. е. введенные нами величины  $R_a$  и  $R_b$  выражаются через классическую величину  $\frac{\omega}{Q}$ , характеризующую потери в резонаторе.

Другая величина, интересующая нас - это среднее электромагнитное поле

$$\begin{aligned} \bar{E}_{(f)} &= E_0 \sin kz Sp (\hat{\rho} (\hat{a}^\dagger + \hat{a})) = \\ &= E_0 \sin kz Sp (\hat{\rho} \hat{a}) + \text{к.с.} = \\ &= E_1 Sp (\hat{\rho} \hat{a}) + \text{к.с.} = \langle E \rangle + \text{к.с.}, \end{aligned}$$

где  $\langle E \rangle$  - аналитический сигнал классического поля. Уравнение, которому удовлетворяет поле, может быть получено при помощи уравнения движения

матрицы плотности. Запишем уравнение для статистического оператора поля моды (2.69) и используя для  $R_a, R_b$  их выражения через  $Q$  и  $\bar{n}_T$  (2.81), имеем

$$\begin{aligned} \dot{\hat{\rho}} = & -\frac{\omega}{2Q} \bar{n}_T (\hat{a}\hat{a}^\dagger \hat{\rho} - 2\hat{a}^\dagger \hat{\rho} \hat{a} + \hat{\rho} \hat{a}\hat{a}^\dagger) - \\ & -\frac{\omega}{2Q} (\bar{n}_T + 1) (\hat{a}^\dagger \hat{a} \hat{\rho} - 2\hat{a} \hat{\rho} \hat{a}^\dagger + \hat{\rho} \hat{a}^\dagger \hat{a}) \end{aligned} \quad (2.82)$$

Поскольку

$$\langle E \rangle = E_1 Sp(\hat{\rho} \hat{a}), \quad \frac{d\langle E \rangle}{dt} = E_1 Sp\left(\frac{d\hat{\rho}}{dt} \hat{a}\right), \quad (2.83)$$

Следовательно, уравнение (2.82) надо помножить на  $E_1 \hat{a}$  и взять  $Sp$ . В результате получим:

$$\begin{aligned} \langle \dot{E} \rangle = & -\frac{\omega E_1}{2Q} \bar{n}_T \{ Sp(\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} - 2\hat{a}^\dagger \hat{\rho} \hat{a} \hat{a} + \hat{\rho} \hat{a} \hat{a}^\dagger \hat{a}) + \\ & + Sp(\hat{a}^\dagger \hat{a} \hat{\rho} \hat{a} - 2\hat{a} \hat{\rho} \hat{a}^\dagger \hat{a} + \hat{\rho} \hat{a}^\dagger \hat{a} \hat{a}) \} - \\ & -\frac{\omega E_1}{2Q} Sp(\hat{a}^\dagger \hat{a} \hat{\rho} \hat{a} - 2\hat{a} \hat{\rho} \hat{a}^\dagger \hat{a} + \hat{\rho} \hat{a}^\dagger \hat{a} \hat{a}) \end{aligned} \quad (2.84)$$

Известно, что под знаком  $Sp$  можно производить круговую перестановку операторов. Применим это к (2.84). Например

$$\begin{aligned} & Sp(\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} - 2\hat{a}^\dagger \hat{\rho} \hat{a} \hat{a} + \hat{\rho} \hat{a} \hat{a}^\dagger \hat{a}) = \\ & = Sp(\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} - 2\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} + \hat{\rho} \hat{a} \hat{a}^\dagger \hat{a}) = \\ & = Sp(\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} - 2\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} + \hat{\rho} \hat{a} (\hat{a}\hat{a}^\dagger - 1)) = \\ & Sp(\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} - 2\hat{a}\hat{a}^\dagger \hat{\rho} \hat{a} + (\hat{a}\hat{a}^\dagger - 1) \hat{\rho} \hat{a}) = -Sp(\hat{\rho} \hat{a}). \end{aligned} \quad (2.85)$$

Проделав то же самое со второй скобкой (2.84), получим

$$\begin{aligned} & Sp(\hat{a}^\dagger \hat{a} \hat{\rho} \hat{a} - 2\hat{a} \hat{\rho} \hat{a}^\dagger \hat{a} + \hat{\rho} \hat{a}^\dagger \hat{a} \hat{a}) = \\ & = Sp(\hat{\rho} \hat{a} \hat{a}^\dagger \hat{a} - 2\hat{\rho} \hat{a}^\dagger \hat{a} \hat{a} + \hat{\rho} \hat{a}^\dagger \hat{a} \hat{a}) = \\ & = Sp(\hat{\rho} (\hat{a}^\dagger \hat{a} + 1) \hat{a} - 2\hat{\rho} \hat{a}^\dagger \hat{a} \hat{a} + \hat{\rho} \hat{a}^\dagger \hat{a} \hat{a}) = Sp(\hat{\rho} \hat{a}). \end{aligned} \quad (2.86)$$

Подставив (2.85) и (2.86) в (2.84), имеем

$$\begin{aligned} \langle \dot{E} \rangle = & -\frac{\omega E_1}{2Q} \bar{n}_T \{ Sp(\hat{\rho} \hat{a}) - Sp(\hat{\rho} \hat{a}) \} - \\ & -\frac{\omega E_1}{2Q} Sp(\hat{\rho} \hat{a}) = -\frac{\omega}{2Q} \langle E \rangle. \end{aligned} \quad (2.87)$$

Таким образом, мы связали параметры резервуара (параметры пучка) с классической величиной  $Q$  и со средним числом фотонов в моде при температуре резервуара. Это позволяет написать уравнения движения матрицы плотности поля в общем виде, при этом конкретная модель резервуара не имеет значения

$$\begin{aligned} \dot{\rho}_{nm} = & -\frac{\omega}{2Q} (2\bar{n}_T (n+m+1) + n+m) \rho_{nm} + \\ & + \frac{\omega\bar{n}_T}{Q} \sqrt{nm} \rho_{n-1,m-1} + \frac{\omega}{Q} (\bar{n}_T + 1) \sqrt{(n+1)(m+1)} \rho_{n+1,m+1} \end{aligned} \quad (2.88)$$

В операторном виде это уравнение записывается так

$$\begin{aligned} \dot{\rho} = & -\frac{\omega}{2Q} \{ \bar{n}_T (\hat{a}\hat{a}^\dagger\hat{\rho} - \hat{a}^\dagger\hat{\rho}\hat{a}) + \\ & + (\bar{n}_T + 1) (\hat{a}^\dagger\hat{a}\hat{\rho} - \hat{a}\hat{\rho}\hat{a}^\dagger) \} + \text{э. с.} \end{aligned} \quad (2.89)$$

Запись уравнения (2.69), 2.89 в представлении чисел заполнения является одной из многих. Часто удобно пользоваться другими представлениями.

## 2.10 Уравнение движения статистического оператора поля моды в представлении когерентных состояний

В квантовой оптике и квантовой электронике часто удобно пользоваться когерентными состояниями  $|\alpha\rangle$ . В этом случае статистический оператор может быть записан в диагональном представлении (1.118)

$$\hat{\rho}(t) = \int P(\alpha, t) |\alpha\rangle \langle\alpha| d^2\alpha, \quad (2.90)$$

Подставляя это выражение в уравнение движения статистического оператора (2.69), 2.89, получим:

$$\begin{aligned} & \int \dot{P}(\alpha, t) |\alpha\rangle \langle\alpha| d^2\alpha = \\ & = -\frac{1}{2} \int P(\alpha, t) [R_a (\hat{a}\hat{a}^\dagger |\alpha\rangle \langle\alpha| - \hat{a}^\dagger |\alpha\rangle \langle\alpha| \hat{a}) + \\ & \quad + R_b (\hat{a}^\dagger \hat{a} |\alpha\rangle \langle\alpha| - \hat{a} |\alpha\rangle \langle\alpha| \hat{a}^\dagger)] d^2\alpha + \text{э.с.} \end{aligned} \quad (2.91)$$

Справедливы следующие равенства

$$\begin{aligned}\hat{a}^\dagger |\alpha\rangle \langle \alpha| &= \left( \frac{\partial}{\partial \alpha} + \alpha^* \right) |\alpha\rangle \langle \alpha|, \\ |\alpha\rangle \langle \alpha| \hat{a} &= \left( \frac{\partial}{\partial \alpha^*} + \alpha \right) |\alpha\rangle \langle \alpha|,\end{aligned}\quad (2.92)$$

Эти равенства легко доказываются, если воспользоваться одной из форм определения когерентного состояния

$$|\alpha\rangle = e^{\alpha \hat{a}^\dagger - \frac{1}{2} \alpha \alpha^*} |0\rangle.$$

Отсюда имеем

$$|\alpha\rangle \langle \alpha| = e^{\alpha \hat{a}^\dagger - \frac{1}{2} \alpha \alpha^*} |0\rangle \langle 0| e^{\alpha^* \hat{a} - \frac{1}{2} \alpha^* \alpha}.$$

Дифференцируя это выражение по  $\alpha$ , получим:

$$\begin{aligned}\frac{\partial}{\partial \alpha} |\alpha\rangle \langle \alpha| &= (\hat{a}^\dagger - \alpha^*) e^{\alpha \hat{a}^\dagger - \frac{1}{2} \alpha \alpha^*} |0\rangle \langle 0| e^{\alpha^* \hat{a} - \frac{1}{2} \alpha^* \alpha} = \\ &= (\hat{a}^\dagger - \alpha^*) |\alpha\rangle \langle \alpha|\end{aligned}$$

следовательно,

$$\hat{a}^\dagger |\alpha\rangle \langle \alpha| = \left( \frac{\partial}{\partial \alpha} + \alpha^* \right) |\alpha\rangle \langle \alpha|. \quad (2.93)$$

Таким же образом показывается справедливость второго равенства

$$\frac{\partial}{\partial \alpha^*} |\alpha\rangle \langle \alpha| = e^{\alpha \hat{a}^\dagger - \frac{1}{2} \alpha \alpha^*} |0\rangle \langle 0| e^{\alpha^* \hat{a} - \frac{1}{2} \alpha^* \alpha} (\hat{a} - \alpha).$$

Следовательно,

$$|\alpha\rangle \langle \alpha| \hat{a} = \left( \frac{\partial}{\partial \alpha^*} + \alpha \right) |\alpha\rangle \langle \alpha|, \quad (2.94)$$

Используя (2.92) и известные соотношения для операторов рождения и уничтожения  $\hat{a} |\alpha\rangle = \alpha |\alpha\rangle$ ,  $\langle \alpha| \hat{a}^\dagger = \alpha^* \langle \alpha|$ , приведем уравнение (2.91) к виду:

$$\begin{aligned}& \int \dot{P}(\alpha, t) |\alpha\rangle \langle \alpha| d^2 \alpha = \\ &= -\frac{1}{2} R_a \int P(\alpha, t) \left\{ - \left( \frac{\partial^2}{\partial \alpha \partial \alpha^*} + \alpha^* \frac{\partial}{\partial \alpha^*} \right) |\alpha\rangle \langle \alpha| \right\} d^2 \alpha - \\ & \quad - \frac{1}{2} R_b \int P(\alpha, t) \alpha \frac{\partial}{\partial \alpha} |\alpha\rangle \langle \alpha| d^2 \alpha + \text{э.с.}\end{aligned}\quad (2.95)$$

Нам необходимо рассмотреть входящие в (2.95) интегралы, преобразовав их при помощи интегрирования по частям. В интегралах, входящих в (2.95)

$d^2\alpha = dxdy$ , если  $\alpha = x + iy$ ,  $x = \text{Re } \alpha$ ,  $y = \text{Im } \alpha$ . Следовательно для интегрирования по частям нужно подинтегральную функцию выразить через  $x$ ,  $y$ , произвести интегрирование по частям, а, затем вернуться к прежним переменным. Но можно поступить иначе. Формально считаем  $\alpha$  и  $\alpha^*$  независимыми переменными и выражаем  $dxdy$  через  $d\alpha d\alpha^*$ .

$$d^2\alpha = dxdy = d\alpha d\alpha^* |J|,$$

где  $|J|$  якобиан перехода, который в нашем случае является постоянным  $|J| = \frac{1}{2}$ . Теперь можно проинтегрировать по частям, а в окончательном выражении перейти к прежним обозначениям

$$d\alpha d\alpha^* |J| \rightarrow d^2\alpha.$$

Имеем

$$\begin{aligned} & \int P \alpha \frac{\partial}{\partial \alpha} |\alpha\rangle \langle \alpha| d^2\alpha = \\ & = \alpha P |\alpha\rangle \langle \alpha| \Big|_{-\infty}^{+\infty} - \int \frac{\partial}{\partial \alpha} (\alpha P) |\alpha\rangle \langle \alpha| d^2\alpha = \\ & = - \int \frac{\partial}{\partial \alpha} (\alpha P) |\alpha\rangle \langle \alpha| d^2\alpha. \end{aligned} \quad (2.96)$$

При этом мы полагали, что  $\alpha P(\alpha, t) \rightarrow 0$ , при  $|\alpha| \rightarrow \infty$ . Интеграл со второй производной после двойного интегрирования по частям преобразуется к виду:

$$\begin{aligned} & \int P \frac{\partial^2}{\partial \alpha \partial \alpha^*} |\alpha\rangle \langle \alpha| d^2\alpha = \\ & = \int \left( \frac{\partial^2}{\partial \alpha \partial \alpha^*} P \right) |\alpha\rangle \langle \alpha| d^2\alpha \end{aligned} \quad (2.97)$$

Подставляя все это в равенство (2.95), получим:

$$\begin{aligned} & \int \dot{P}(\alpha, t) |\alpha\rangle \langle \alpha| d^2\alpha = \\ & = - \int \left\{ \frac{1}{2} (R_a - R_b) \left[ \frac{\partial}{\partial \alpha} (P\alpha) + c.c. \right] - \right. \\ & \quad \left. - R_a \frac{\partial^2 P}{\partial \alpha \partial \alpha^*} \right\} |\alpha\rangle \langle \alpha| d^2\alpha \end{aligned} \quad (2.98)$$

Это равенство удовлетворится, если множитель при  $|\alpha\rangle \langle \alpha|$  положить равным нулю. Таким образом, получим

$$\dot{P}(\alpha, t) = -\frac{1}{2} (R_a - R_b) \left( \frac{\partial}{\partial \alpha} (\alpha P) + c.c. \right) + R_a \frac{\partial^2 P}{\partial \alpha \partial \alpha^*} \quad (2.99)$$

Это уравнение типа уравнения Фоккера-Планка, которое используется при решении классических задач статистической физики, например, задач о броуновском движении и других аналогичных задач. Решив (2.99) при соответствующих начальных и граничных условиях, легко при помощи (2.90) написать выражение для статистического оператора

$$\hat{\rho}(t) = \int P(\alpha, t) |\alpha\rangle \langle \alpha| d^2\alpha$$

и с помощью (1.122) и (1.128) вычислять средние значения наблюдаемых величин, связанных с рассматриваемой системой

$$\langle O \rangle = \int P(\alpha, t) \langle \alpha | \hat{O} | \alpha \rangle d^2\alpha = \int P(\alpha, t) O^{(n)}(\alpha, \alpha^*) d^2\alpha,$$

где  $O^{(n)}$  нормальное представление оператора  $\hat{O}$  (1.123). Коэффициенты  $R_a$  и  $R_b$ , входящие в (2.99), можно, как и прежде (2.81), выразить через  $Q$  и  $\bar{n}_T$ , тогда уравнение примет вид

$$\frac{\partial}{\partial t} P(\alpha, t) = \frac{1}{2} \frac{\omega}{Q} \left[ \frac{\partial}{\partial \alpha} (\alpha P(\alpha, t)) + \text{к. с.} \right] + \frac{\omega \bar{n}_T}{Q} \frac{\partial^2 P(\alpha, t)}{\partial \alpha \partial \alpha^*}. \quad (2.100)$$

В качестве примера вычислим среднее значение оператора положительно частотной части электрического поля  $E_1 \hat{a}$ .

$$\begin{aligned} \frac{d \langle E_1 \hat{a} \rangle}{dt} &= E_1 \int \alpha \dot{P} d^2\alpha = \\ &= E_1 \frac{1}{2} \frac{\omega}{Q} \int \left[ \frac{\partial}{\partial \alpha} (\alpha P) + \text{к. с.} \right] \alpha d^2\alpha + \\ &\quad + E_1 \frac{\omega \bar{n}_T}{Q} \int \alpha \frac{\partial^2 P}{\partial \alpha \partial \alpha^*} d^2\alpha \end{aligned} \quad (2.101)$$

Интегрируя второй член по  $\alpha^*$  получим

$$\begin{aligned} \int \alpha \frac{\partial^2 P}{\partial \alpha \partial \alpha^*} d^2\alpha &= \frac{\partial P}{\partial \alpha} \alpha \Big|_{-\infty}^{\infty} - \\ &\quad - \int \frac{\partial P}{\partial \alpha} \alpha \frac{\partial \alpha}{\partial \alpha^*} = 0, \end{aligned}$$

т. к.  $\frac{\partial P}{\partial \alpha}$  предполагается достаточно быстро стремящимся к 0 на бесконечности, а  $\frac{\partial \alpha}{\partial \alpha^*} = 0$ , т. к.  $\alpha$  и  $\alpha^*$  - независимые переменные. Первое слагаемое

можно расписать следующим образом

$$\begin{aligned} & \int \alpha \left( \frac{\partial}{\partial \alpha} (\alpha P) + \frac{\partial}{\partial \alpha^*} (\alpha^* P) \right) d^2 \alpha = \\ & = - \int \alpha P \frac{\partial \alpha}{\partial \alpha} d^2 \alpha - \int \alpha^* P \frac{\partial \alpha}{\partial \alpha^*} d^2 \alpha = - \int \alpha P d^2 \alpha = - \langle \hat{a} \rangle. \end{aligned}$$

Таким образом окончательно имеем:

$$\frac{d \langle E_1 \hat{a} \rangle}{dt} = - \frac{\omega}{2Q} \langle E_1 \hat{a} \rangle \quad (2.102)$$

- результат, который мы получили ранее другим путем. Уравнение (2.100) можно записать в различных системах координат, например, в полярной  $\alpha = r e^{i\theta}$ ,  $\alpha^* = r e^{-i\theta}$ . Проведем соответствующие преобразования, получим

$$\begin{aligned} \frac{\partial}{\partial t} P(r, \theta, t) &= \frac{1}{2} \frac{\omega}{Q} \frac{\partial}{\partial r} (r^2 P(r, \theta, t)) + \\ &+ \frac{1}{2} \frac{\omega}{Q} \frac{\bar{n}_T}{2r^2} \left( r \frac{\partial}{\partial r} r \frac{\partial}{\partial r} + \frac{\partial^2}{\partial \theta^2} \right) P(r, \theta, t). \end{aligned} \quad (2.103)$$

Если воспользоваться координатами  $x$  и  $y$ ,  $\alpha = x + iy$ ,  $\alpha^* = x - iy$ , то есть  $x = \frac{1}{2}(\alpha + \alpha^*)$ ,  $y = -\frac{i}{2}(\alpha - \alpha^*)$ , можно уравнение представить в виде

$$\begin{aligned} \frac{\partial}{\partial t} P(x, y, t) &= \frac{1}{2} \frac{\omega}{Q} \left( \frac{\partial}{\partial x} x + \frac{\partial}{\partial y} y \right) P(x, y, t) + \\ &+ \frac{1}{4} \frac{\omega}{Q} \bar{n}_T \left( \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right) P(x, y, t). \end{aligned} \quad (2.104)$$

При решении конкретной задачи удобно воспользоваться уравнением, записанным либо в прямоугольной, либо в полярной системе координат.

## 2.11 Общая теория взаимодействия динамической системы с термостатом

До сих пор мы имели дело с частной моделью взаимодействия моды резонатора (динамической системы) с атомным пучком, находящимся в равновесии при температуре  $T$  (с резервуаром). Здесь мы рассмотрим более общий подход к задаче о взаимодействии динамической системы с резервуаром [52]. Имеем дело с двумя взаимодействующими системами:  $A$  - динамическая система и  $B$  - резервуар (диссипативная система). Системы  $A$  и  $B$  слабо

связаны между собой, то есть энергия связи мала по сравнению с энергией динамической системы. Гамильтониан взаимодействия обозначим  $\hat{V}$ . Диссипативная система  $B$  - обширная система, находящаяся в термодинамическом равновесии при температуре  $T$ . Сперва будем рассматривать системы  $A$  и  $B$  как равноправные. Обозначим статистический оператор полной системы  $\hat{\rho}_{AB}$ . Введем статистические операторы  $\hat{\rho}_A$  и  $\hat{\rho}_B$ , относящиеся соответственно только к системам  $A$ ,  $B$ . С оператором  $\hat{\rho}_{AB}$  они связаны через соотношения

$$\hat{\rho}_A = Sp_B \{ \hat{\rho}_{AB} \}, \quad \hat{\rho}_B = Sp_A \{ \hat{\rho}_{AB} \}, \quad (2.105)$$

Уравнение движения статистического оператора всей объединенной системы имеет в представлении взаимодействия вид

$$i\hbar \dot{\hat{\rho}}_{AB} = [\hat{V}, \hat{\rho}_{AB}]. \quad (2.106)$$

Уравнения движения для свернутых операторов очевидно равны

$$\begin{aligned} i\hbar \dot{\hat{\rho}}_A &= Sp_B [\hat{V}, \hat{\rho}_{AB}], \\ i\hbar \dot{\hat{\rho}}_B &= Sp_A [\hat{V}, \hat{\rho}_{AB}]. \end{aligned} \quad (2.107)$$

Статистический оператор  $\hat{\rho}_{AB}$  представим в следующем виде

$$\hat{\rho}_{AB} = \hat{\rho}_A \otimes \hat{\rho}_B + \hat{\rho}_C, \quad (2.108)$$

где  $\hat{\rho}_C$  является следствием взаимодействия между системами,  $\otimes$  - знак внешнего (тензорного) произведения. В начальный момент  $t_0$  системы предполагаются невзаимодействующими, тогда полный статистический оператор равен внешнему произведению

$$\hat{\rho}_{AB}|_{t=t_0} = \hat{\rho}_A \otimes \hat{\rho}_B,$$

а

$$\hat{\rho}_C|_{t=t_0} = 0.$$

Преобразуем теперь член  $[\hat{V}, \hat{\rho}_A \otimes \hat{\rho}_B]$ , входящий в уравнение (2.107), и получим

$$\begin{aligned} [\hat{V}, \hat{\rho}_A \otimes \hat{\rho}_B] &= \hat{V} \hat{\rho}_A \otimes \hat{\rho}_B - \hat{\rho}_A \otimes \hat{\rho}_B \hat{V} = \\ &= \hat{V} \hat{\rho}_B \otimes \hat{\rho}_A - \hat{\rho}_A \otimes \hat{\rho}_B \hat{V}. \end{aligned} \quad (2.109)$$

так как  $\hat{\rho}_A \otimes \hat{\rho}_B = \hat{\rho}_B \otimes \hat{\rho}_A$  из-за того, что  $\hat{\rho}_A$  и  $\hat{\rho}_B$  действуют на разные переменные. Отсюда, производя операцию  $Sp_B$ , имеем

$$\begin{aligned} Sp_B [\hat{V}, \hat{\rho}_A \otimes \hat{\rho}_B] &= Sp_B (\hat{V} \hat{\rho}_B) \hat{\rho}_A - \\ &- \hat{\rho}_A Sp_B (\hat{\rho}_B \hat{V}) = [\hat{V}_A, \hat{\rho}_A], \end{aligned} \quad (2.110)$$



где  $\hat{V}_A = Sp_B (\hat{V} \hat{\rho}_B)$ . Таким же образом получим

$$Sp_A [\hat{V}, \hat{\rho}_A \otimes \hat{\rho}_B] = [\hat{V}_B, \hat{\rho}_B], \quad (2.111)$$

где  $\hat{V}_B = Sp_A (\hat{V} \hat{\rho}_A)$ . Учитывая равенства (2.108), (2.109), (2.110), (2.111), уравнения движения  $\hat{\rho}_A$  и  $\hat{\rho}_B$  можно представить в виде

$$\begin{aligned} i\hbar \frac{d}{dt} \hat{\rho}_A(t) &= [\hat{V}_A(t), \hat{\rho}_A] + Sp_B [\hat{V}, \hat{\rho}_C], \\ i\hbar \frac{d}{dt} \hat{\rho}_B(t) &= [\hat{V}_B(t), \hat{\rho}_B] + Sp_A [\hat{V}, \hat{\rho}_C]. \end{aligned} \quad (2.112)$$

Из вида (2.112) понятно, что  $\hat{V}_A$  и  $\hat{V}_B$  имеют смысл изменения энергии одной системы связанной с ее взаимодействием с другой, например с взаимодействием динамической системы с термостатом. Эти изменения малы и в нашем случае их можно не учитывать. Таким образом (2.112) преобразуется в

$$\begin{aligned} i\hbar \frac{d}{dt} \hat{\rho}_A(t) &= Sp_B [\hat{V}, \hat{\rho}_C], \\ i\hbar \frac{d}{dt} \hat{\rho}_B(t) &= Sp_A [\hat{V}, \hat{\rho}_C]. \end{aligned} \quad (2.113)$$

Для оператора  $\hat{\rho}_C$ , используя то, что

$$\hat{\rho}_C = \hat{\rho}_{AB} - \hat{\rho}_A \otimes \hat{\rho}_B$$

можем написать уравнение движения следующим образом

$$\begin{aligned} i\hbar \frac{d\hat{\rho}_C}{dt} &= i\hbar \frac{d\hat{\rho}_{AB}}{dt} - i\hbar \frac{d}{dt} (\hat{\rho}_A \otimes \hat{\rho}_B) = \\ &= i\hbar \left( \frac{d\hat{\rho}_{AB}}{dt} - \frac{d\hat{\rho}_A}{dt} \otimes \hat{\rho}_B - \hat{\rho}_A \otimes \frac{d\hat{\rho}_B}{dt} \right). \end{aligned} \quad (2.114)$$

Используя уравнения движения  $\hat{\rho}_{AB}$ ,  $\hat{\rho}_A$ ,  $\hat{\rho}_B$  (2.113), получим для (2.114)

$$\begin{aligned} i\hbar \frac{d\hat{\rho}_C}{dt} &= [\hat{V}, (\hat{\rho}_A \otimes \hat{\rho}_B + \hat{\rho}_C)] - \\ &- \left( Sp_B [\hat{V}, \hat{\rho}_C] \right) \hat{\rho}_B - \hat{\rho}_A \left( Sp_A [\hat{V}, \hat{\rho}_C] \right) \end{aligned} \quad (2.115)$$

Пренебрегая членами второго порядка малости, получим простое уравнение:

$$i\hbar \frac{d\hat{\rho}_C}{dt} = [\hat{V}, (\hat{\rho}_A \otimes \hat{\rho}_B)]. \quad (2.116)$$

Членами первого порядка малости мы считаем  $\hat{V}$ ,  $\hat{\rho}_C$ . Это следует из предположения, что взаимодействие между динамической системой и термостатом малое. Члены, в которые входят произведения типа  $\hat{V}\hat{\rho}_C$ , считаем малым второго порядка. Формальное решение уравнения (2.116) имеет вид

$$\hat{\rho}_C(t) = -\frac{i}{\hbar} \int_{t_0}^t [\hat{V}(t'), (\hat{\rho}_A \otimes \hat{\rho}_B)] dt' \quad (2.117)$$

при начальных условиях  $\hat{\rho}_C(t_0) = 0$ .

До сих пор мы считали, что системы  $A$  и  $B$  равноправны. Теперь учтем, что динамическая система  $A$  - малая, а диссипативная система  $B$  - настолько большая, что взаимодействие ее с динамической системой не может в заметной степени нарушить ее равновесие. Учтем это, положив  $\frac{d\hat{\rho}_B}{dt} = 0$ :

$$\hat{\rho}_B(t') = \hat{\rho}_B(t_0). \quad (2.118)$$

Подставив в уравнение для  $\hat{\rho}_A$  (2.112) равенства (2.115) и (2.117), получим

$$\begin{aligned} \frac{d\hat{\rho}_A}{dt} &= -\frac{1}{\hbar^2} \int_{t_0}^t Sp_B \left[ \hat{V}(t), [\hat{V}(t'), \hat{\rho}_A(t') \otimes \hat{\rho}_B(t_0)] \right] dt' = \\ &= -\frac{1}{\hbar^2} \int_{t_0}^t dt' Sp_B \left\{ [\hat{V}(t) \hat{V}(t') \hat{\rho}_A(t') \otimes \hat{\rho}_B(t_0) - \right. \\ &\quad \left. - \hat{V}(t) \hat{\rho}_A(t') \otimes \hat{\rho}_B(t_0) \hat{V}(t')] - \right. \\ &\quad \left. - [\hat{V}(t') \hat{\rho}_A(t') \otimes \hat{\rho}_B(t_0) \hat{V}(t) - \hat{\rho}_A(t') \otimes \hat{\rho}_B(t_0) \hat{V}(t') \hat{V}(t)] \right\}. \end{aligned} \quad (2.119)$$

Это уравнение для оператора плотности динамической системы  $A$ , взаимодействующей с диссипативной системой  $B$ . При обширной системе  $B$  время корреляции  $\hat{V}(t)$  и  $\hat{V}(t')$  очень мало, значительно меньше характерного времени изменения  $\hat{\rho}_A$ . Следовательно, существенная область интегрирования находится в окрестности  $t' = t$ . Тогда во многих случаях при интегрировании можно положить

$$\hat{\rho}_A(t') = \hat{\rho}_A(t).$$

Более полно с общей теорией взаимодействия динамической системы с термостатом можно познакомиться в [52]. Применим общую теорию к конкретным случаям.

## 2.12 Релаксация атома в случае простейшего резервуара, состоящего из гармонических осцилляторов

Рассмотрим многомодовое электромагнитное поле, описываемое при помощи операторов рождения и уничтожения  $\hat{a}_k^\dagger, \hat{a}_k$ . Частоту  $k$ -ой моды обозначим через  $\omega_k$ .

Это электромагнитное поле взаимодействует с некоторым двухуровневым атомом. Атом может находиться в двух состояниях возбужденном  $|a\rangle$  и невозбужденном  $|b\rangle$ . Операторы перехода по прежнему  $\hat{\sigma}$  и  $\hat{\sigma}^\dagger$ . Частоту перехода обозначим через  $\Omega$ . Гамильтониан взаимодействия в этом случае имеет вид

$$\hat{V}(t) = \hbar \sum_{(k)} g_k \hat{a}_k^\dagger \hat{\sigma} e^{-i(\Omega - \omega_k)t} + \text{э.с.} \quad (2.120)$$

где  $g_k$  - константа взаимодействия.

Таким образом системой  $B$  (резервуаром) у нас будет многомодовое электромагнитное поле, а исследуемой динамической системой  $A$  - двухуровневый атом. Оператор плотности резервуара (электромагнитного поля) обозначим через  $\hat{\rho}_R$ . Оператор плотности исследуемой динамической системы (атома) через  $\hat{\rho}_{at}$ .

Справедливы следующие соотношения:

$$Sp_R \left( \hat{a}_k^\dagger \hat{a}_k \hat{\rho}_R \right) = \bar{n}_k \quad (2.121)$$

где  $\bar{n}_k$  - среднее число фотонов в моде резервуара;

$$\begin{aligned} Sp_R \left( \hat{a}_k \hat{a}_k^\dagger \hat{\rho}_R \right) &= \bar{n}_k + 1, \\ Sp_R \left( \hat{a}_k \hat{a}_k \hat{\rho}_R \right) &= Sp_R \left( \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{\rho}_R \right) = 0. \end{aligned} \quad (2.122)$$

Используя эти равенства, общее уравнение (2.119) можно представить в виде:

$$\begin{aligned} \dot{\hat{\rho}}_{at}(t) = & - \int_{t_0}^t \sum_{(k)} g_k^2 \left\{ \hat{\sigma}^\dagger \hat{\sigma} \hat{\rho}_{at}(t') (\bar{n}_k + 1) e^{i(\Omega - \omega_k)(t-t')} + \right. \\ & + \hat{\sigma} \hat{\sigma}^\dagger \hat{\rho}_{at}(t') \bar{n}_k e^{-i(\Omega - \omega_k)(t-t')} - \hat{\sigma}^\dagger \hat{\rho}_{at}(t') \hat{\sigma} \bar{n}_k e^{i(\Omega - \omega_k)(t-t')} - \\ & \left. - \hat{\sigma} \hat{\rho}_{at}(t') \hat{\sigma}^\dagger (\bar{n}_k + 1) e^{-i(\Omega - \omega_k)(t-t')} \right\} dt' + \text{э.с.} \end{aligned} \quad (2.123)$$

Суммирование по  $k$ , учитывая квазинепрерывный спектр состояний дис-

сипативной системы, можно заменить интегрированием (1.44)

$$\sum_{(k)} \rightarrow \int D(\omega) d\omega,$$

где  $D(\omega)$  спектральная плотность состояний. Заменяем  $D(\omega)$ ,  $\bar{n}(\omega)$ ,  $g^2(\omega)$  на  $D$ ,  $\bar{n}$ ,  $g^2$  - их значения при  $\omega = \Omega$ , считая, что эти функции медленно зависят от частоты. Воспользуемся равенством (см. интегральное представление дельта-функции (18.3))

$$\begin{aligned} \int_0^\infty e^{\pm(\Omega-\omega)(t-t')} d\omega &= |\nu = \omega - \Omega| = \\ &= \int_{-\Omega}^\infty e^{-\nu(t \mp t')} d\nu \approx \int_{-\infty}^\infty e^{-\nu(t \mp t')} d\nu = \\ &= 2\pi\delta(t \mp t') \end{aligned} \quad (2.124)$$

и проведем интегрирование по времени. Это приводит нас к уравнению

$$\begin{aligned} \dot{\hat{\rho}}_{at} &= -\frac{1}{2}\gamma \{ \bar{n} [\hat{\sigma}\hat{\sigma}^\dagger\hat{\rho}_{at} - \hat{\sigma}^\dagger\hat{\rho}_{at}\hat{\sigma}] + \\ &+ (\bar{n} + 1) [\hat{\sigma}^\dagger\hat{\sigma}\hat{\rho}_{at} - \hat{\sigma}\hat{\rho}_{at}\hat{\sigma}^\dagger] \} + \text{э.с.} \end{aligned} \quad (2.125)$$

где  $\gamma = 4\pi Dg^2$ ,  $\bar{n}$  взяты при частоте моды  $\Omega$ . Уравнение (2.125) имеет тот же вид, что и уравнение (2.89), полученное ранее. Уравнения полностью совпадают, если принять  $\gamma = \frac{\omega}{Q}$  и сделать замену  $\hat{\sigma} \rightarrow \hat{a}$ ,  $\hat{\sigma}^\dagger \rightarrow \hat{a}^\dagger$ . Это еще раз подтверждает, что окончательный результат не зависит от природы резервуара.

При температуре резервуара  $T = 0$  фотоны отсутствуют и  $\bar{n} = 0$ . Положим, что в начальный момент атом возбужден

$$\hat{\rho}_{at}(t_0) = 1.$$

Используя свойства (2.10) - (2.9) операторов  $\hat{\sigma}$  и  $\hat{\sigma}^\dagger$ , получим

$$\begin{aligned} \dot{\rho}_{aa} &= \langle a | \dot{\hat{\rho}}_{at} | a \rangle = -\frac{1}{2}\gamma \langle a | \hat{\sigma}^\dagger\hat{\sigma}\hat{\rho}_{at} | a \rangle + \\ &+ \frac{1}{2}\gamma \langle a | \hat{\sigma}\hat{\rho}_{at}\hat{\sigma}^\dagger | a \rangle + \text{к.с.} = \\ &= -\frac{1}{2}\gamma \langle a | \hat{\rho}_{at} | a \rangle + \text{к.с.} = -\gamma\rho_{aa}. \end{aligned} \quad (2.126)$$

Здесь мы использовали соотношения  $\hat{\sigma}^\dagger |a\rangle = 0$ ,  $\hat{\sigma}^\dagger |b\rangle = |a\rangle$ ,  $\hat{\sigma} |a\rangle = |b\rangle$ ,  $\hat{\sigma} |b\rangle = 0$  и сопряженные им. Окончательный результат

$$\dot{\rho}_{aa} = -\gamma\rho_{aa}. \quad (2.127)$$

Это означает, что в результате спонтанной эмиссии вероятность нахождения атома на верхнем уровне экспоненциально убывает.

## 2.13 Затухание моды резонатора. Уравнение Гейзенберга - Ланжевена.

### 2.13.1 Постановка задачи.

Задачу о релаксации поля (моды) резонатора мы рассматриваем, используя метод матрицы плотности, т. е. представление Шредингера. Существует другой подход, принадлежащий Ланжевону, в котором уравнения динамической системы для учета влияния диссипативной системы дополняются случайными силами, статистические свойства которых известны. В квантовом случае динамическими уравнениями являются уравнения Гейзенберга для операторов наблюдаемых величин, а случайные воздействия, связанные с термостатом, учитываются добавлением некоего шумового оператора. Получаемые уравнения носят названия уравнений Гейзенберга-Ланжевена.

Рассмотрим таким методом задачу о релаксации моды резонатора (гармонического осциллятора), взаимодействующей с термостатом. В представлении Гейзенберга операторы зависят от времени и удовлетворяют уравнениям Гейзенберга:

$$\frac{d\hat{O}}{dt} = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{O}],$$

где  $\hat{\mathcal{H}}$  - гамильтониан рассматриваемой системы. Например, для свободного поля ранее мы получили уравнения (1.61):

$$\frac{d\hat{a}}{dt} = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{a}] = -i\omega\hat{a}, \quad \frac{d\hat{a}^\dagger}{dt} = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{a}^\dagger] = i\omega\hat{a}^\dagger,$$

где  $\omega$  - частота моды, а  $\hat{a}$  и  $\hat{a}^\dagger$  операторы уничтожения и рождения.

Рассматриваемая задача схематически изображена на рис. 2.18. Мода электромагнитного поля, рассматриваемая как динамическая система, взаимодействует с обширным резервуаром, состоящим из большого числа гармонических осцилляторов (фононов) и находящимся в равновесии при температуре  $T$ . Гамильтониан такой системы можно представить в виде

$$\hat{\mathcal{H}} = \hat{\mathcal{H}}_0 + \hat{V},$$

где

$$\hat{\mathcal{H}}_0 = \hbar\omega\hat{a}^\dagger\hat{a} + \sum_{(k)} \hbar\omega_k\hat{b}_k^\dagger\hat{b}_k$$

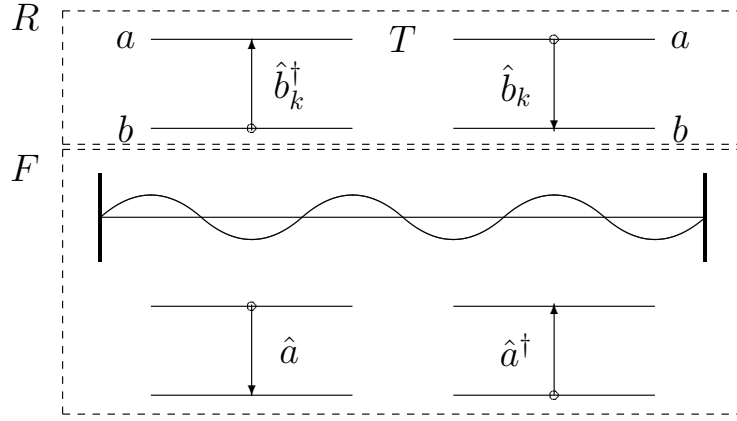


Рис. 2.18: Взаимодействие моды электромагнитного поля резонатора  $F$  с резервуаром атомов  $R$ , находящихся при температуре  $T$ .  $\hat{a}^\dagger$  и  $\hat{a}$  - операторы рождения и уничтожения исследуемой моды электромагнитного поля.  $\hat{b}_k^\dagger$  и  $\hat{b}_k$  - операторы рождения и уничтожения  $k$ -ой моды резервуара (фононов).

гамильтониан системы без учета взаимодействия между ее частями,

$$\hat{V} = \hbar \sum_{(k)} g_k \left( \hat{b}_k^\dagger \hat{a} + \hat{a}^\dagger \hat{b}_k \right) \quad (2.128)$$

гамильтониан взаимодействия между динамической системой и термостатом. Через  $g_k$  в (2.128) обозначена постоянная взаимодействия для  $k$ -ой моды резервуара.  $\hat{a}$ ,  $\hat{a}^\dagger$  - операторы уничтожения и рождения для поля моды,  $\hat{b}_k$ ,  $\hat{b}_k^\dagger$  - операторы уничтожения и рождения для  $k$ -ой моды резервуара (фононов). Вакуумные члены в гамильтониане не учтены, т. к. в ходе вывода уравнений они взаимно сокращаются.

### 2.13.2 Уравнения движения Гейзенберга для операторов.

Уравнения движения Гейзенберга для  $\hat{a}$  и  $\hat{b}_k$

$$\begin{aligned} \frac{d\hat{a}}{dt} &= \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{a}], \\ \frac{d\hat{b}_k}{dt} &= \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{b}_k] \end{aligned}$$

при помощи коммутационных соотношений  $[\hat{a}, \hat{a}^\dagger] = 1$  и  $[\hat{b}_k, \hat{b}_k^\dagger] = 1$  приводятся к виду

$$\begin{aligned}\frac{d\hat{a}(t)}{dt} &= -i\omega\hat{a}(t) - i\sum_{(k)} g_k \hat{b}_k(t), \\ \frac{d\hat{b}_k(t)}{dt} &= -i\omega_k \hat{b}_k(t) - ig_k \hat{a}(t).\end{aligned}\quad (2.129)$$

Из системы (2.129) можно исключить  $\hat{b}_k$ , проинтегрировав второе уравнение и подставив результат в первое уравнение. Интегрирование проще всего выполнить, используя операционное исчисление. Получаем

$$\hat{b}_k(t) = \hat{b}_k(0) e^{-i\omega_k t} - ig_k \int_0^t dt' \hat{a}(t') e^{-i\omega_k(t-t')}$$

и далее

$$\begin{aligned}\frac{d\hat{a}(t)}{dt} &= -i\omega\hat{a}(t) - \sum_{(k)} g_k^2 \int_0^t dt' \hat{a}(t') e^{-i\omega_k(t-t')} + \hat{f}(t), \\ \hat{f}(t) &= -i \sum_{(k)} g_k \hat{b}_k(0) e^{-i\omega_k t}.\end{aligned}\quad (2.130)$$

Оператор  $\hat{f}(t)$  зависит от переменных термостата и является шумовым оператором, описывающим воздействие резервуара на динамическую систему.

Уравнение (2.130) интегродифференциальное. при некоторых приближениях его можно преобразовать в чисто дифференциальное. Сперва перейдем к медленным переменным, записав

$$\begin{aligned}\hat{a}(t) &= \hat{A}(t) e^{-i\omega t}, \\ \hat{f}(t) &= \hat{F}(t) e^{-i\omega t},\end{aligned}$$

где  $\omega$  - частота моды. Отсюда имеем

$$\frac{d\hat{A}(t)}{dt} = - \sum_{(k)} g_k^2 \int_0^t dt' \hat{A}(t') e^{i(\omega - \omega_k)(t-t')} + \hat{F}(t). \quad (2.131)$$

Первый член выражения (2.131) имеет вид, с которым мы сталкивались рассматривая спонтанное излучение методом Вайскопфа-Вигнера. Примененный там подход можно применить и здесь. Из выражения (2.131) видно, что основной вклад дадут члены с частотами, близкими к частоте моды:  $\omega_k \approx \omega$ .

По этой причине все медленно меняющиеся члены можно взять при частоте  $\omega$  и вынести их из под интеграла. Суммирование по  $k$ , считая спектр фононов квазинепрерывным, можно заменить интегрированием по частоте:

$$\begin{aligned} & \sum_{(k)} g_k^2 \int_0^t dt' \hat{A}(t') e^{i(\omega - \omega_k)(t-t')} = \\ & = \int_0^t dt' \hat{A}(t') \int_0^\infty g^2(\omega) D(\omega) e^{i(\omega - \omega')(t-t')} d\omega' = \\ & = g^2(\omega) D(\omega) \int_0^t dt' \hat{A}(t') \int_0^\infty e^{i(\omega - \omega')(t-t')} d\omega', \end{aligned}$$

где  $D(\omega)$  частотная плотность состояний.  $D(\omega)$  и  $g^2(\omega)$  взяты при частоте моды поля и вынесены из под знака интеграла.

Рассмотрим интеграл по частоте. Действуя так же как при рассмотрении спонтанного излучения методом Вайскопфа-Вигнера, получим

$$\begin{aligned} \int_0^\infty e^{-i(\omega' - \omega)(t-t')} d\omega' &= \int_{-\infty}^\infty e^{-i\nu(t-t')} d\nu \approx \int_{-\infty}^\infty e^{-i\nu(t-t')} d\nu = \\ &= \int_{-\infty}^\infty e^{i\nu(t'-t)} d\nu = 2\pi \delta(t' - t). \end{aligned}$$

Следовательно можно написать

$$\begin{aligned} \frac{d\hat{A}(t)}{dt} &= -2\pi g^2(\omega) D(\omega) \int_0^t dt' \hat{A}(t') \delta(t - t') + \hat{F}(t) = \\ &= -2\pi g^2(\omega) D(\omega) \hat{A}(t) + \hat{F}(t). \end{aligned}$$

Обозначим  $2\pi Dg^2|_\omega = \frac{\gamma}{2}$  - коэффициент затухания поля. Получим

$$\frac{d\hat{A}(t)}{dt} = -\frac{\gamma}{2} \hat{A}(t) + \hat{F}(t), \quad (2.132)$$

где  $\hat{F}(t)$  случайный шумовой оператор, свойства которого необходимо определить. Как будет видно из дальнейшего, шумовой оператор обеспечивает сохранение коммутационных соотношений для оператора моды поля.

Изучим теперь статистические свойства, характеризующиеся корреляционными функциями  $\hat{F}$ . Предположим, что резервуар находится в тепловом рав-



новесии при температуре  $T$ . Тогда имеем:

$$\begin{aligned}
\langle \hat{b}_k(0) \rangle_R &= \langle \hat{b}_k^\dagger(0) \rangle_R = 0, \\
\langle \hat{b}_k^\dagger(0) \hat{b}_{k'}(0) \rangle_R &= \bar{n}_k \delta_{kk'}, \\
\langle \hat{b}_k(0) \hat{b}_{k'}^\dagger(0) \rangle_R &= (\bar{n}_k + 1) \delta_{kk'}, \\
\langle \hat{b}_k(0) \hat{b}_{k'}(0) \rangle_R &= \langle \hat{b}_k^\dagger(0) \hat{b}_{k'}^\dagger(0) \rangle_R = 0,
\end{aligned} \tag{2.133}$$

где  $\langle \dots \rangle_R$  означает усреднение по переменным термостата, а  $\bar{n}_k$  - среднее число фононов в моде  $k$ . Шумовой оператор был определен формулой

$$\hat{F}(t) = -i \sum_{(k)} g_k \hat{b}_k(0) e^{-i(\omega_k - \omega)t}. \tag{2.134}$$

Используя (2.133), легко видеть

$$\begin{aligned}
\langle \hat{F}(t) \rangle_R &= \langle \hat{F}^\dagger(t) \rangle_R = 0, \\
\langle \hat{F}^\dagger(t) \hat{F}(t') \rangle_R &= \\
&= \sum_k \sum_{k'} g_k g_{k'} \langle \hat{b}_k^\dagger(0) \hat{b}_{k'}(0) \rangle_R e^{i(\omega_k - \omega)t} e^{-i(\omega_{k'} - \omega)t'} = \\
&= \sum_k g_k^2 \bar{n}_k e^{i(\omega_k - \omega)(t - t')} = \\
&= \int_0^\infty g^2(\omega) D(\omega) \bar{n}_T e^{i(\omega' - \omega)(t - t')} d\omega' = \\
&= 2\pi g^2(\omega) D(\omega) \bar{n}_T \delta(t - t') = \frac{\gamma \bar{n}_T}{2} \delta(t - t'),
\end{aligned} \tag{2.135}$$

где  $\bar{n}_T$  среднее число фононов в моде резервуара при температуре  $T$ , определяемое формулой Планка,  $\gamma = 4\pi g^2(\omega) D(\omega)$ . Если согласно Ланжевону ввести коэффициент диффузии  $\mathcal{D} = \frac{\gamma \bar{n}_T}{2}$ , то последнее уравнение системы (2.135) можно записать в виде

$$\langle \hat{F}^\dagger(t) \hat{F}(t') \rangle_R = \mathcal{D} \delta(t - t').$$

Заметим что  $\langle \dots \rangle_R$  означает усреднение по переменным термостата, следовательно результатом усреднения будет корреляционная функция, зависящая только от переменных динамической системы (поля).

Подобным образом доказывается

$$\left\langle \hat{F}(t) \hat{F}^\dagger(t') \right\rangle_R = \frac{\gamma(\bar{n}_T + 1)}{2} \delta(t - t') \quad (2.136)$$

и

$$\left\langle \hat{F}(t) \hat{F}(t') \right\rangle_R = \left\langle \hat{F}^\dagger(t) \hat{F}^\dagger(t') \right\rangle_R = 0. \quad (2.137)$$

Таким образом, в нашем приближении, шум является  $\delta$ -коррелированным.

Нам еще понадобится корреляционная функция вида  $\left\langle \hat{F}^\dagger(t) \hat{A}(t') \right\rangle_R$  - необходимая для вывода уравнения, которому удовлетворяет  $\left\langle \hat{A}^\dagger(t) \hat{A}(t') \right\rangle_R$ . Для этого проинтегрируем уравнение для  $\hat{A}(t)$  (2.132) и в результате при помощи операционного исчисления получаем

$$\hat{A}(t) = \hat{A}(0) e^{-\frac{\gamma}{2}t} + \int_0^t dt' e^{-\frac{\gamma}{2}(t-t')} \hat{F}(t').$$

Помножим это выражение на  $\hat{F}^\dagger(t)$  и усредним по термостату. Получим

$$\begin{aligned} \left\langle \hat{F}^\dagger(t) \hat{A}(t) \right\rangle_R &= \int_0^t \left\langle \hat{F}^\dagger(t) \hat{F}(t') \right\rangle_R e^{-\frac{\gamma}{2}(t-t')} dt' + \\ &+ \left\langle \hat{F}^\dagger(t) \hat{A}(0) \right\rangle_R e^{-\frac{\gamma}{2}t}. \end{aligned} \quad (2.138)$$

Последний член в (2.138) равен 0, т. к.  $\hat{F}^\dagger(t)$  и  $\hat{A}(0)$  независимы, а их средние равны 0. Принимая во внимание второе уравнение системы (2.135) т. е.  $\left\langle \hat{F}^\dagger(t) \hat{F}(t') \right\rangle_R = \frac{\gamma\bar{n}_T}{2} \delta(t - t')$ , получим

$$\left\langle \hat{F}^\dagger(t) \hat{A}(t) \right\rangle_R = \frac{\gamma\bar{n}_T}{2}.$$

Теперь можно рассмотреть корреляционную функцию  $\left\langle \hat{A}^\dagger(t) \hat{A}(t) \right\rangle_R$ . Дифференцируя эту функцию по времени, получим

$$\frac{d \left\langle \hat{A}^\dagger(t) \hat{A}(t) \right\rangle_R}{dt} = \left\langle \frac{d\hat{A}^\dagger(t)}{dt} \hat{A}(t) \right\rangle_R = \left\langle \frac{d\hat{A}^\dagger(t)}{dt} \hat{A}(t) \right\rangle_R + \left\langle \hat{A}^\dagger(t) \frac{d\hat{A}(t)}{dt} \right\rangle_R. \quad (2.139)$$

Далее воспользуемся уравнением (2.132) и сопряженным ему, в результате получим

$$\frac{d \left\langle \hat{A}^\dagger(t) \hat{A}(t) \right\rangle_R}{dt} = -\gamma \left\langle \hat{A}^\dagger(t) \hat{A}(t) \right\rangle_R + \left\langle \hat{F}^\dagger(t) \hat{A}(t) \right\rangle_R + \left\langle \hat{A}^\dagger(t) \hat{F}(t) \right\rangle_R.$$

Учитывая выражения

$$\left\langle \hat{F}^\dagger(t) \hat{A}(t) \right\rangle_R = \left\langle \hat{A}^\dagger(t) \hat{F}(t) \right\rangle_R = \frac{\gamma \bar{n}_T}{2},$$

окончательно имеем

$$\frac{d \left\langle \hat{A}^\dagger(t) \hat{A}(t) \right\rangle_R}{dt} = -\gamma \left\langle \hat{A}^\dagger(t) \hat{A}(t) \right\rangle_R + \gamma \bar{n}_T.$$

Подобным образом можно получить

$$\frac{d \left\langle \hat{A}(t) \hat{A}^\dagger(t) \right\rangle_R}{dt} = -\gamma \left\langle \hat{A}(t) \hat{A}^\dagger(t) \right\rangle_R + \gamma (\bar{n}_T + 1). \quad (2.140)$$

Вычитая эти выражения одно из другого, получим для коммутатора

$$\frac{d \left\langle [\hat{A}(t), \hat{A}^\dagger(t)] \right\rangle_R}{dt} = \gamma \left( 1 - \left\langle [\hat{A}(t), \hat{A}^\dagger(t)] \right\rangle_R \right). \quad (2.141)$$

Из уравнения (2.141) следует, что если в начальный момент времени

$$\left\langle [\hat{A}(0), \hat{A}^\dagger(0)] \right\rangle_R = 1,$$

т. е. коммутационные соотношения выполняются, то эти соотношения будут выполняться всегда. Другими словами, коммутационные соотношения, усредненные по переменным термостата, сохраняются со временем.

Картина была бы совершенно иная, если бы мы не принимали во внимание квантовые шумы. В этом случае уравнение (2.141) приняло бы вид

$$\frac{d \left\langle [\hat{A}(t), \hat{A}^\dagger(t)] \right\rangle_R}{dt} = -\gamma \left\langle [\hat{A}(t), \hat{A}^\dagger(t)] \right\rangle_R,$$

решение которого имеет вид

$$\left\langle [\hat{A}(t), \hat{A}^\dagger(t)] \right\rangle_R = \left\langle [\hat{A}(0), \hat{A}^\dagger(0)] \right\rangle_R e^{-\gamma t} = e^{-\gamma t}.$$

Это означает, что при достаточно большом времени операторы  $\hat{A}$  и  $\hat{A}^\dagger$  коммутируют, чего на самом деле не наблюдается. По этой причине учет квантового шумового члена обязателен.

Уравнение движения усредненного по переменным термостата поля легко получить из (2.132). Для этого вначале запишем усредненное поле

$$\begin{aligned} \left\langle \hat{E}(t) \right\rangle_R &= \left\langle E_0 \sin kz (\hat{a}(t) + \hat{a}^\dagger(t)) \right\rangle_R = \\ &= E_0 \sin kz \left( \left\langle \hat{A}(t) \right\rangle_R e^{-i\omega t} + \left\langle \hat{A}^\dagger(t) \right\rangle_R e^{i\omega t} \right), \end{aligned}$$

где учтено  $\hat{a} = \hat{A}e^{-i\omega t}$ . Из (2.132) имеем

$$\frac{d\langle \hat{A}(t) \rangle_R}{dt} = -\frac{\gamma}{2} \langle \hat{A}(t) \rangle_R,$$

т. к.  $\langle \hat{F}(t) \rangle_R = 0$ . Таким образом со временем  $\langle \hat{A}(t) \rangle_R$  и  $\langle \hat{A}^\dagger(t) \rangle_R$  а вместе с ними и  $\langle \hat{E}(t) \rangle_R$  стремятся к нулю:

$$\langle \hat{E}(t) \rangle_R \rightarrow 0.$$

### 2.13.3 Флуктационно-диссипационная формула

Нами было получено выражение (2.135):

$$\langle \hat{F}^\dagger(t) \hat{F}(t') \rangle_R = \frac{\gamma \bar{n}_T}{2} \delta(t - t').$$

Интегрируя обе части по  $dt'$ , получим

$$\gamma = \frac{2}{\bar{n}_T} \int_0^\infty \langle \hat{F}^\dagger(t) \hat{F}(t') \rangle_R dt', \quad (2.142)$$

т. е. скорость затухания и шумовые флуктуации связаны между собой соотношением (2.142). Большему затуханию соответствуют большие шумы.

## 2.14 Упражнения

1. Исходя из (2.13), получить выражение (2.14) для оператора  $\hat{V}$  в представлении взаимодействия.
2. Вывести систему уравнений (2.19).
3. Получить формулу (2.64).
4. Вывести из (2.69) уравнение для матрицы плотности в представлении чисел заполнения (2.71).
5. Привести формулу (2.91) к виду (2.95).
6. Интегрируя по частям, получить выражения (2.96), (2.97).
7. Записать общее уравнение (2.99) в полярной системе координат (2.103).

8. Записать общее уравнение (2.99) в прямоугольной системе координат (2.104).
9. Вывести соотношения (2.121) и (2.122).
10. Вывести уравнение (2.123).
11. Доказать (2.136) и (2.137).
12. Получить выражение (2.140).
13. Какова частота перехода  $f_0 = \frac{\omega_o}{2\pi}$  между двумя состояниями атома лития если в результате экспериментов были получены данные, изображенные на рис. 2.19 <sup>2</sup>

---

<sup>2</sup>Взято из заданий [12]

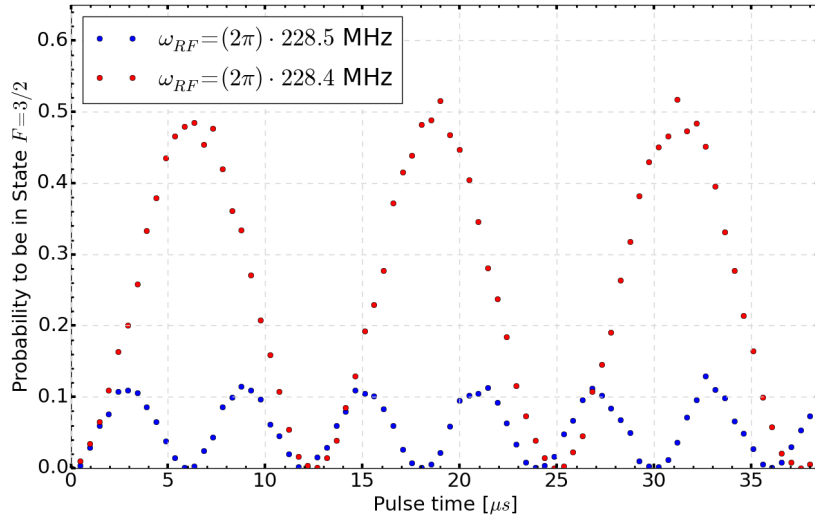


Рис. 2.19: Вы хотите измерить частоту перехода  $f_0 = \frac{\omega_o}{2\pi}$  между двумя состояниями атома лития посредством оценки осцилляций Раби. Вы приготавливаете холодное облако атомов лития в состоянии  $|1\rangle$  (так называемое  $|F = 1/2\rangle$  состояние) и вы можете применять электромагнитный импульс фиксированной интенсивности и изменяемой длительности  $\tau$ . Окончательно вы измеряете число атомов в состоянии  $|2\rangle$  (так называемое  $|F = 3/2\rangle$  состояние). Вы знаете, что разность частот между этими двумя уровнями близка к  $2\pi \cdot 228.5 \text{ МГц}$ , следовательно вы применяете электромагнитный импульс с частотой близкой к этой величине: вначале с частотой  $\omega_1 = 2\pi \cdot 228.5 \text{ МГц}$ , потом вы повторяете измерения с частотой  $\omega_2 = 2\pi \cdot 228.4 \text{ МГц}$ . Результат изображен на представленном рисунке. Какова частота перехода  $f_0 = \frac{\omega_o}{2\pi}$  между двумя состояниями атома лития?

## Часть 2

# Квантовая оптика





## Глава 3

# Квантовая теория лазера

Полуклассическая теория лазера не может ответить на все вопросы, возникающие в связи с его работой. По этой теории лазер до достижения порога не генерирует вообще, а при превышении порога начинает генерировать классическое электромагнитное поле (свет).

В действительности же заметно ниже порога лазер генерирует хаотический свет, а значительно выше порога его излучение близко к классическому. На пороге и вблизи него находится переходная область от хаотического света к упорядоченному излучению. Адекватно описать это может только полностью квантовая теория.

Другая задача, также требующая квантования электромагнитного поля, - это определение предельной (естественной) ширины линии излучения лазера, когда ширина линии определяется квантовыми флуктуациями поля, а различные внешние воздействия, принципиально устранимые, не принимаются во внимание.

Лазер является открытой системой, в которой активные атомы и поле резонатора связаны с большими внешними системами, которые мы будем называть резервуарами, обеспечивающими накачку и потери. Отсюда следует, что лазер, как открытую систему, нужно рассматривать при помощи матрицы плотности.

### 3.1 Модель лазера

Ранее (2.69) мы рассматривали взаимодействие моды резонатора (гармонического осциллятора) с резервуаром, находящимся в тепловом равновесии при температуре  $T$ . Этой же моделью можно воспользоваться и при рассмотрении работы лазера, но ее нужно дополнить еще одним резервуаром, обеспечивающим накачку. См. рис. 3.1: первый резервуар,  $R_1$ , содержит атомы, находящиеся при температуре  $T$ . Второй,  $R_2$ , содержит атомы (другого

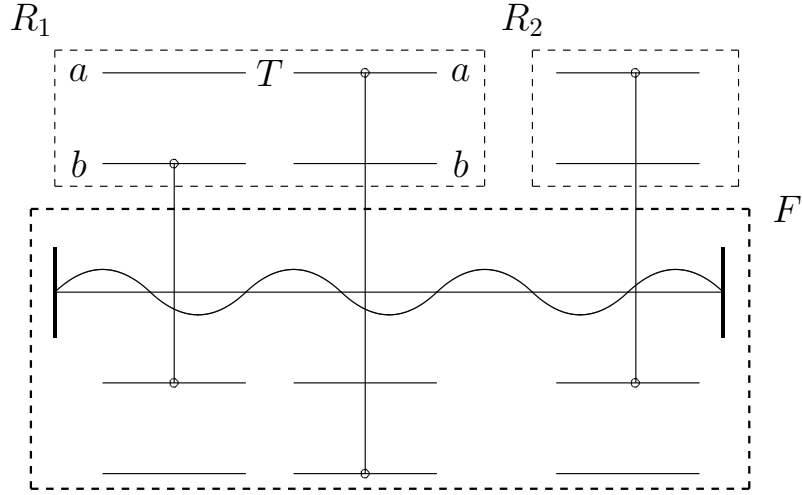


Рис. 3.1: Рассматриваемая модель лазера. Мода резонатора (электромагнитное поле)  $F$  взаимодействует с резервуарами  $R_1$  и  $R_2$ .  $R_1$  содержит атомы находящиеся в тепловом равновесии при температуре  $T$  (потери).  $R_2$  содержит атомы находящиеся в инвертированном состоянии (накачка).

сорта), находящиеся в инвертированном состоянии.

В линейном приближении (во втором порядке теории возмущения) мы задачу о взаимодействии моды резонатора с резервуаром уже решали. Для матрицы плотности, описывающей состояние поля моды резонатора, были получены уравнения:

$$\begin{aligned} \dot{\hat{\rho}} = & -\frac{1}{2} \frac{\omega}{Q} \{ \bar{n}_T (\hat{a} \hat{a}^\dagger \hat{\rho} - \hat{a}^\dagger \hat{\rho} \hat{a}) + \\ & + (\bar{n}_T + 1) (\hat{a}^\dagger \hat{a} \hat{\rho} - \hat{a} \hat{\rho} \hat{a}^\dagger) \} + \text{э. с.} \end{aligned} \quad (3.1)$$

или в другой записи (2.69)

$$\begin{aligned} \dot{\hat{\rho}} = & -\frac{1}{2} R_a (\hat{a} \hat{a}^\dagger \hat{\rho} - \hat{a}^\dagger \hat{\rho} \hat{a}) - \\ & -\frac{1}{2} R_b (\hat{a}^\dagger \hat{a} \hat{\rho} - \hat{a} \hat{\rho} \hat{a}^\dagger) + \text{э. с.} \end{aligned} \quad (3.2)$$

Если ограничиться линейным приближением (по полю), уравнение для матрицы плотности лазера можно написать, используя эти уравнения. Для описания действия резервуара, вносящего потери, удобно использовать (3.1), учтя при этом, что при не слишком высокой температуре  $\bar{n}_T \ll 1$  и  $\bar{n}_T$  можно пренебречь по сравнению с единицей.

Для описания резервуара, обеспечивающего накачку, удобно использовать (3.2), отбросив второе слагаемое, так как для простоты предполагается, что все атомы резервуара накачки находятся в верхнем состоянии.

Все это приводит к следующему уравнению:

$$\begin{aligned} \dot{\hat{\rho}} = & -\frac{1}{2} \frac{\omega}{Q} (\hat{a}^\dagger \hat{a} \hat{\rho} - \hat{a} \hat{\rho} \hat{a}^\dagger) - \\ & -\frac{1}{2} A (\hat{a} \hat{a}^\dagger \hat{\rho} - \hat{a}^\dagger \hat{\rho} \hat{a}) + \text{э. с.} \end{aligned} \quad (3.3)$$

где  $A = R_a$  определяется интенсивностью накачки.

Уравнение (3.3) получено во втором приближении теории возмущения. Оно может описать поведение лазера ниже порога генерации, позволяет определить пороговые условия, но не может описать лазер выше порога генерации.

Положим, что потери линейны, и первый член в (3.3) достаточно точно описывает потери. Второй член в (3.3) должен быть найден в следующем неравном нулю приближении (четвертом приближении теории возмущения).

Процедура нахождения этого приближения аналогична проделанной ранее при выводе уравнений (3.1) - 3.2. Нужно только продолжить ее до членов более высокого порядка. Члены третьего порядка дадут ноль, так как получающаяся матрица имеет нулевые диагональные члены, и след от нее равен нулю. Следующий отличный от нуля член будет четвертого порядка и имеет вид:

$$\begin{aligned} Sp_{at} \left\{ \left( -\frac{i}{\hbar} \right)^4 \int_t^{t+\tau} dt_1 \int_t^{t_1} dt_2 \int_t^{t_2} dt_3 \right. \\ \left. \int_t^{t_3} [\hat{V}, [\hat{V}, [\hat{V}, [\hat{V}, \hat{\rho}_{at}(t) \otimes \hat{\rho}_f(t)]]]] dt_4 \right\} \end{aligned} \quad (3.4)$$

Вычисления, аналогичные проделанным ранее, приводят к выражению (см. [50]):

$$\begin{aligned} \frac{1}{8} B \left[ (\hat{a} \hat{a}^\dagger)^2 \hat{\rho} + 3 \hat{a} \hat{a}^\dagger \hat{\rho} \hat{a} \hat{a}^\dagger - \right. \\ \left. - 4 \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{\rho} \hat{a} \right] + \text{э. с.} \end{aligned} \quad (3.5)$$

С учетом (3.5) уравнение для матрицы плотности (статистического оператора) лазерной моды приобретает вид:

$$\begin{aligned} \dot{\hat{\rho}}(t) = & -\frac{1}{2} \frac{\omega}{Q} (\hat{a}^\dagger \hat{a} \hat{\rho} - \hat{a} \hat{\rho} \hat{a}^\dagger) - \frac{1}{2} A (\hat{a} \hat{a}^\dagger \hat{\rho} - \hat{a}^\dagger \hat{\rho} \hat{a}) + \\ & + \frac{1}{8} B \left[ (\hat{a} \hat{a}^\dagger)^2 \hat{\rho} + 3 \hat{a} \hat{a}^\dagger \hat{\rho} \hat{a} \hat{a}^\dagger - 4 \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{\rho} \hat{a} \right] + \text{э. с.} \end{aligned} \quad (3.6)$$

где  $A$  - линейное (ненасыщенное) усиление,  $B = \frac{g^2 \tau^2 A}{3} = \frac{1}{3} r_a g^4 \tau^4$  - параметр насыщения.

Уравнение (3.6) является уравнением движения матрицы плотности лазерного поля, взаимодействующего с нелинейной средой, состоящей из активных атомов, и с линейными потерями.

Уравнение (3.6) можно записать в различных представлениях. Мы здесь ограничимся представлением чисел заполнения (чисел фотонов в моде) и представлением когерентных состояний.

В первом случае из (3.6) легко получить систему уравнений для матричных элементов  $\langle m | \hat{\rho} | n \rangle = \rho_{mn}$ .

Для диагональных элементов имеем:

$$\begin{aligned} \dot{\rho}_{nn}(t) = & -[A - (n+1)B](n+1)\rho_{nn} + \\ & + (A - nB)n\rho_{n-1,n-1} - \frac{\omega}{Q}n\rho_{nn} + \frac{\omega}{Q}(n+1)\rho_{n+1,n+1}. \end{aligned} \quad (3.7)$$

Заметим, что в уравнение входят только диагональные члены.

Таким же образом получаются уравнения для внедиагональных членов. Они выглядят несколько сложнее и здесь не приводятся.

Для того, чтобы записать уравнение (3.6) в представлении когерентных состояний, можно действовать так же как действовали ранее, когда рассматривали затухание моды резонатора. Запишем

$$\hat{\rho} = \int P(\alpha) |\alpha\rangle \langle \alpha| d^2\alpha$$

и подставим в уравнение (3.6). Далее проделаем знакомую процедуру, использованную при релаксации моды резонатора. Для линейных членов, определяющих потери и ненасыщенное усиление, можно воспользоваться полученными тогда результатами. Дополнительно нужно рассмотреть члены, характеризующие насыщение. Вычисления здесь более громоздкие, хотя принципиально не отличаются от проделанных ранее. Получается довольно сложное уравнение, но если вспомнить, что мы использовали теорию возмущений (малое поле), можно пренебречь малыми, оставив только главные члены [50]. В итоге всего сказанного получается уравнение типа уравнения Фоккера-Планка для квазивероятности  $P(\alpha, t)$ :

$$\frac{\partial}{\partial t} P(\alpha, t) = -\frac{1}{2} \left\{ \frac{\partial}{\partial \alpha} \left[ A - \frac{\omega}{Q} - B|\alpha|^2 \right] \alpha P + \text{к. с.} \right\} + A \frac{\partial^2 P}{\partial \alpha \partial \alpha^*} \quad (3.8)$$

то есть по сравнению с формулой (2.100)  $-\frac{\omega}{Q}$  заменяется на  $A - \frac{\omega}{Q} - B|\alpha|^2$ , где  $A - \frac{\omega}{Q} = G$  - ненасыщенное усиление минус потери.  $B$  - характеризует уменьшение усиления из-за насыщения.

## 3.2 Теория лазерной генерации

При помощи уравнения (3.7) можно получить уравнение для среднего числа фотонов в моде

$$\langle n(t) \rangle = \sum_{(n)} n \rho_{nn}.$$

Для этого нужно помножить уравнение (3.7) на  $n$  и произвести суммирование по всем  $n$ . Имеем

$$\frac{d}{dt} \langle n \rangle = \frac{d}{dt} \sum_n \rho_{nn} n = \sum_n \dot{\rho}_{nn} n.$$

Таким образом из (3.7)

$$\begin{aligned} \frac{d}{dt} \langle n \rangle = & - \sum_n n [A - (n+1) B] (n+1) \rho_{nn} + \\ & + \sum_n n (A - nB) n \rho_{n-1, n-1} - \sum_n n \frac{\omega}{Q} n \rho_{nn} + \\ & + \sum_n n \frac{\omega}{Q} (n+1) \rho_{n+1, n+1}. \end{aligned} \quad (3.9)$$

Заменим в (3.9) индексы суммирования. Во второй сумме  $n-1 = m$ , т. е.  $n = m+1$ . В последней сумме  $n+1 = m$ , т. е.  $n = m-1$ . Подставив это в (3.9) получим

$$\begin{aligned} \frac{d}{dt} \langle n \rangle = & - \sum_n n [A - (n+1) B] (n+1) \rho_{nn} + \\ & + \sum_m (m+1) (A - (m+1) B) (m+1) \rho_{m, m} - \sum_n n \frac{\omega}{Q} n \rho_{nn} + \\ & + \sum_m (m-1) \frac{\omega}{Q} m \rho_{m, m} = \sum_m (A - (m+1) B) (m+1) \rho_{m, m} - \sum_m \frac{\omega}{Q} m \rho_{m, m} = \\ & = \sum_n (A - (n+1) B) (n+1) \rho_{n, n} - \sum_n \frac{\omega}{Q} n \rho_{n, n}. \end{aligned}$$

Здесь мы заменили обратно индекс суммирования  $m$  на  $n$  и объединили суммы. Отсюда имеем

$$\frac{d}{dt} \langle n(t) \rangle = \left( A - \frac{\omega}{Q} \right) \langle n(t) \rangle + A - B \langle (n+1)^2 \rangle \quad (3.10)$$

Здесь первый член  $\left( A - \frac{\omega}{Q} \right)$  соответствует ненасыщенному усилению за вычетом потерь. Член  $B \langle (n+1)^2 \rangle = B [\langle n^2 \rangle + 2 \langle n \rangle + 1]$  характеризует падение усиления из-за насыщения. Член  $A$  учитывает спонтанную эмиссию,

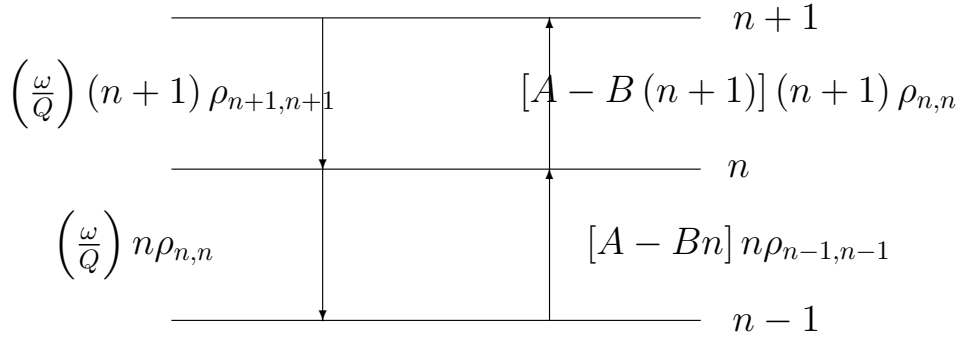


Рис. 3.2: Баланс потоков вероятностей чисел фотонов.

отсутствующую при полуклассическом рассмотрении. В остальном (3.10) напоминает классическое уравнение лазера [48]:

$$\dot{I}_n = 2I_n (\alpha_n - \beta_n I_n).$$

### 3.3 Статистика лазерных фотонов

Для уравнения (3.7) можно наглядно представить потоки вероятностей, изображенные на рис. 3.2.

Член  $\frac{\omega}{Q} n \rho_{nn}$  представляет поток из состояния  $|n\rangle$  в состояние  $|n-1\rangle$  из-за поглощения фотонов атомами первого резервуара. То же самое можно сказать и о члене  $\frac{\omega}{Q} (n+1) \rho_{n+1,n+1}$  - потоке вероятности из состояния  $|n+1\rangle$  в состояние  $|n\rangle$  по тем же причинам.

Член  $[A - (n+1)B] (n+1) \rho_{nn}$  представляет поток из состояния  $|n\rangle$  в состояние  $|n+1\rangle$  и характеризует рождение фотонов из-за взаимодействия с активными атомами, с учетом влияния насыщения. То же относится к члену  $-(A - nB) n \rho_{n-1,n-1}$  потоку вероятности из состояния  $|n-1\rangle$  в состояние  $|n\rangle$ .

$\rho_{nn}$  имеет смысл вероятности обнаружения  $n$  фотонов в лазерной моде. В переходном режиме  $\rho_{nn}(t)$  зависит от времени. В стационарном режиме  $\dot{\rho}_{nn} = 0$  и из уравнения вып. 3.7 можно установить статистику фотонов в режиме стационарной генерации [49].

Приравняем, например, потоки вероятностей между состояниями  $|n+1\rangle$  и  $|n\rangle$  (используя принцип детального равновесия). Получим:

$$\frac{\omega}{Q} (n+1) \rho_{n+1,n+1} = [A - (n+1)B] (n+1) \rho_{nn} \quad (3.11)$$

Равенство (3.11) дает итерационное соотношение

$$\rho_{n+1,n+1} = \frac{A - (n+1)B}{\omega/Q} \rho_{nn} \quad (3.12)$$

которое позволяет выразить  $\rho_{nn}$  через  $\rho_{00}$ . Имеем

$$\rho_{nn} = \rho_{00} \prod_{k=1}^n \frac{A - kB}{\omega/Q} \quad (3.13)$$

$\rho_{00}$  может быть найдено из условия нормировки  $\sum_{(n)} \rho_{nn} = 1$ .

Рассмотрим качественно при помощи (3.13)  $\rho_{nn}$  как функцию  $n$ , когда лазер работает выше порога, т. е. когда  $A > \frac{\omega}{Q}$ . В стационарном режиме усиление равно потерям (в среднем), то есть

$$A - \bar{n}_{st}B = \frac{\omega}{Q},$$

откуда среднее число фотонов в стационарном режиме равно

$$\bar{n}_{st} = \frac{A - \omega/Q}{B}.$$

Для  $n \ll \bar{n}_{st}$ ,  $Bn \ll A$  формулу (3.13) можно представить в виде

$$\rho_{nn} \approx \left( \frac{AQ}{\omega} \right)^n.$$

Эта величина возрастает с ростом  $n$  экспоненциально, так как  $\frac{AQ}{\omega} > 1$ , то есть при малых  $n$  с ростом  $n$  вероятность растет, но рост замедляется по мере увеличения  $n$ . Для больших  $n$  множитель  $\frac{A-nB}{\omega/Q}$  приближается к единице, когда  $n$  приближается к  $\bar{n}_{st}$ . При  $n \approx \bar{n}_{st}$  множитель становится равным 1, и распределение достигает максимума:

$$\left. \frac{A - Bk}{\omega/Q} \right|_{k=\bar{n}_{st}} \rightarrow \frac{A - B\bar{n}_{st}}{\omega/Q} = \frac{A - A + \omega/Q}{\omega/Q} = 1.$$

При  $n > \bar{n}_{st}$  и  $k > \bar{n}_{st}$  множители уменьшаются, достигая нуля при  $k = \frac{A}{B}$ . Заметим, что для  $k = \frac{A}{B}$  множитель становится приблизительно равным нулю, и члены с большими значениями  $k$  следует отбросить, так как  $\rho_{nn}$  не может быть отрицательно. Возникшая трудность связана с тем, что мы пользовались теорией возмущений и, следовательно, полагали, что число фотонов не слишком велико. Наша теория справедлива, пока  $n < \frac{A}{B}$ . Эти трудности исчезают, если пользоваться теорией большого сигнала, развитой в [49]. Из сказанного следует, что  $\rho_{nn}$  как функция  $n$  (распределение фотонов в лазерном поле) сперва растет, достигая максимума вблизи  $n = \bar{n}_{st}$ , а затем убывает до нуля.

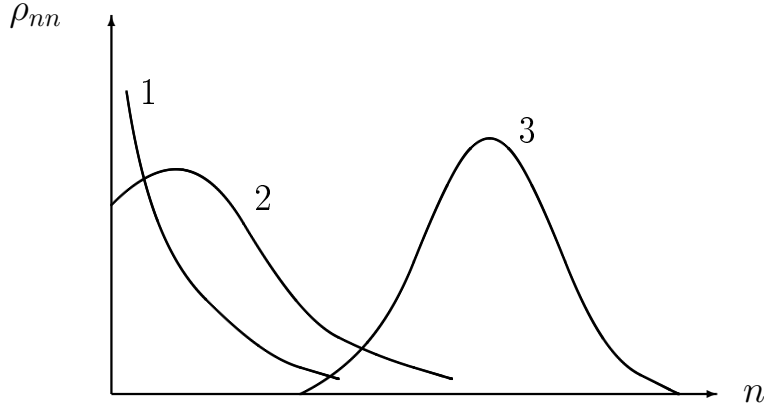


Рис. 3.3: Качественный вид распределения фотонов для трех случаев. График 1:  $A < \frac{\omega}{Q}$  - до порога генерации. График 2:  $A \approx \frac{\omega}{Q}$  - на пороге генерации. График 3:  $A > \frac{\omega}{Q}$  - выше порога генерации.

На рис. 3.3 качественно изображена кривая распределения фотонов для случая превышения порога. На пороге  $A = \frac{\omega}{Q}$ . Тогда сомножитель  $\frac{A-Bk}{\omega/Q} = 1 - \left(\frac{B}{A}\right)k$  при любом  $k$  будет меньше единицы. Кривая распределения будет монотонно убывать. Ниже порога  $A < \frac{\omega}{Q}$ , тогда  $\frac{A-Bk}{\omega/Q} \approx \frac{AQ}{\omega} \ll 1$  и  $\rho_{nn}$  экспоненциально затухает, как  $\left(\frac{AQ}{\omega}\right)^n$ . Зависимость  $\rho_{nn}$  от  $n$  для всех трех случаев может быть численно рассчитана по формуле (3.13). Результаты такого расчета представлены на рис. 3.4.

Из теории большого сигнала [49], которую мы здесь не рассматриваем, следует, что при очень большом превышении порога  $\rho_{nn} \rightarrow e^{-\bar{n}} \frac{\bar{n}^n}{n!}$ , то есть стремится к распределению, характерному для когерентного состояния. При умеренном превышении порога распределение фотонов в лазерном излучении заметно отличается от распределения фотонов в когерентном состоянии. Отличие распределения фотонов в лазерном поле от распределения Пуассона (соответствующего когерентному состоянию) при умеренной накачке наглядно представлено на рис. 3.5.

### 3.4 Теория лазера. Представление когерентных состояний

Нужно воспользоваться уравнением для функции квазивероятности  $P(\alpha, t)$  (3.8):

$$\frac{\partial}{\partial t} P(\alpha, t) = -\frac{1}{2} \left\{ \frac{\partial}{\partial \alpha} \left[ A - \frac{\omega}{Q} - B|\alpha|^2 \right] \alpha P + \text{к. с.} \right\} + A \frac{\partial^2 P}{\partial \alpha \partial \alpha^*}.$$

Для наших целей удобно это уравнение представить в полярных коорди-



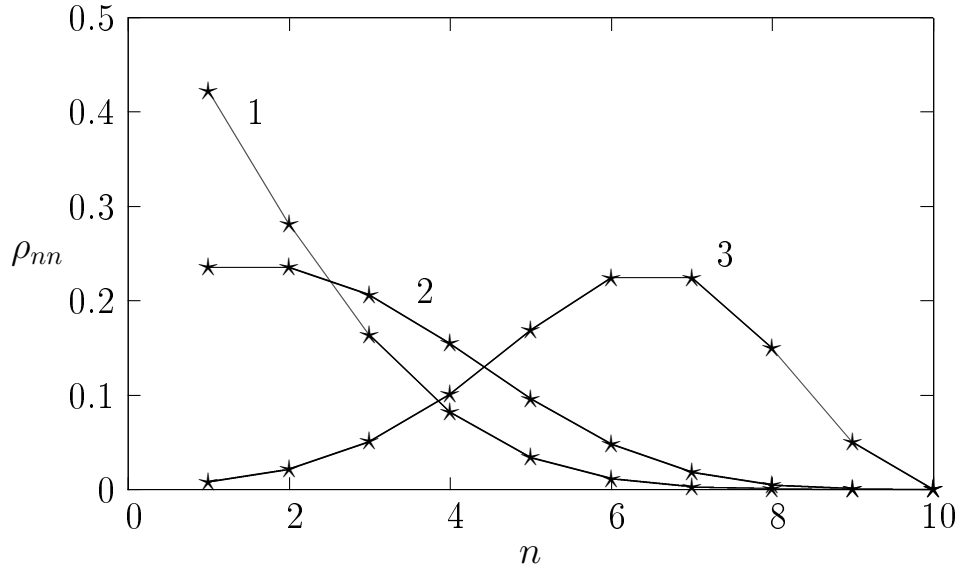


Рис. 3.4: Результаты численного расчета распределения фотонов. График 1, который описывает распределение фотонов до порога генерации, получен при следующих параметрах:  $A = 10$ ,  $\frac{\omega}{Q} = 12$ ,  $B = 1$ . График 2, соответствующий порогу генерации, получен при  $A = 10$ ,  $\frac{\omega}{Q} = 8$ ,  $B = 1$ . Для графика 3 было принято  $A = 10$ ,  $\frac{\omega}{Q} = 3$ ,  $B = 1$ , что соответствует превышению порога.

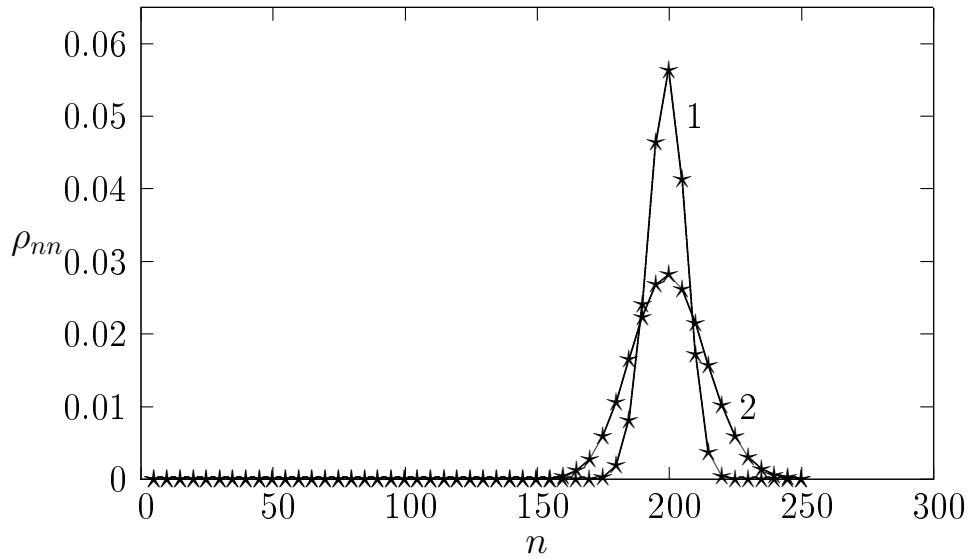


Рис. 3.5: Отличие распределения фотонов в лазерном поле при умеренной накачке (график 1) от распределения Пуассона (график 2).

натах  $\alpha = re^{i\theta}$ . Имеем

$$\begin{aligned} \frac{\partial}{\partial t} P(r, \theta, t) = & -\frac{1}{2r} \cdot \frac{\partial}{\partial r} \left[ r^2 \left( A - \frac{\omega}{Q} - Br^2 \right) P(r, \theta, t) \right] + \\ & + \frac{A}{4r^2} \left( r \frac{\partial}{\partial r} r \frac{\partial}{\partial r} + \frac{\partial^2}{\partial \theta^2} \right) P(r, \theta, t) \end{aligned} \quad (3.14)$$

Допустим, что нас интересует стационарное состояние. Тогда  $\frac{\partial P}{\partial t} = 0$ , а фаза  $\theta$  распределена равномерно от 0 до  $2\pi$ . Из сказанного следует, что  $\frac{\partial^2 P}{\partial \theta^2} = 0$  и квазивероятность  $P(r, \theta, t)$  от  $t$  и  $\theta$  не зависит. Уравнение (3.14) примет вид

$$0 = -\frac{\partial}{\partial r} \left[ r^2 \left( A - \frac{\omega}{Q} - Br^2 \right) P(r) \right] + \frac{1}{2} A \frac{\partial}{\partial r} r \frac{\partial}{\partial r} P(r). \quad (3.15)$$

Это уравнение легко интегрируется. Первое интегрирование дает

$$r \left( A - \frac{\omega}{Q} - Br^2 \right) P(r) = \frac{1}{2} A \frac{\partial}{\partial r} P(r) + C. \quad (3.16)$$

Постоянная  $C = 0$ , так как  $P$  и  $\frac{\partial P}{\partial r}$  должны достаточно быстро стремиться к нулю при  $r \rightarrow \infty$ .

Отсюда следует уравнение

$$\frac{dP}{P} = \frac{2}{A} r \left( A - \frac{\omega}{Q} - Br^2 \right) dr. \quad (3.17)$$

Его решением будет

$$\begin{aligned} P &= N \exp \left( \frac{1}{A} \left[ r^2 \left( A - \frac{\omega}{Q} \right) - \frac{Br^4}{2} \right] \right) = \\ &= N \exp \left( \frac{1}{A} \left[ r^2 G - \frac{Br^4}{2} \right] \right), \end{aligned} \quad (3.18)$$

где  $N$  - нормирующий множитель, равный

$$\frac{1}{N} = 2\pi \int_0^\infty \exp \left( \frac{1}{A} \left[ r^2 G - \frac{Br^4}{2} \right] \right) r dr.$$

Распределение (3.18) является функцией от  $r^2 = |\alpha|^2 = \bar{n}$ . При превышении порога  $A > \frac{\omega}{Q}$ , то есть при  $G > 0$ ,  $P(r)$  с ростом  $r^2$  сперва растет, достигая максимума при  $r^2 = \frac{A - \omega/Q}{B} = \frac{G}{B}$ , а затем убывает.

Этот же результат мы имели ранее. Полученное значение  $r = \sqrt{\frac{G}{B}}$  соответствует при  $G > 0$  наиболее вероятному значению  $|\alpha|$ .

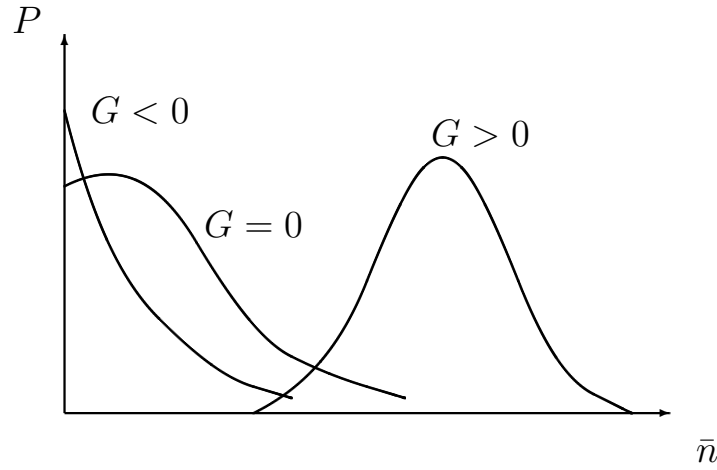


Рис. 3.6: Качественный вид зависимости квазивероятности  $P$  от среднего числа фотонов  $\bar{n} = r^2$  при трех различных значениях параметра  $G$ .  $G < 0$  до порога генерации;  $G \approx 0$  - на пороге генерации;  $G > 0$  - превышение порога генерации.

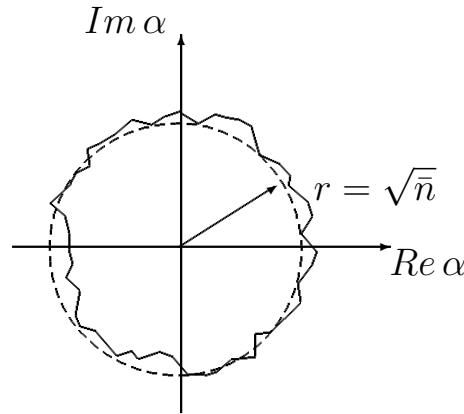


Рис. 3.7: Флуктуация амплитуды поля генерируемого лазером в узкой области в окрестности окружности радиуса  $r = \sqrt{\bar{n}_{st}}$ .

При  $A < \frac{\omega}{Q}$ ,  $G < 0$  лазер находится ниже порога. С ростом  $r^2$  кривая монотонно падает. На пороге  $A = \frac{\omega}{Q}$ ,  $G = 0$  кривая также падает, но при  $r^2 = 0$  имеем экстремум.

На [рис. 3.6](#) представлены зависимости квазивероятности от  $r^2 = |\alpha|^2$ , при различных значениях параметра  $G$ , соответствующих допороговому, пороговому и надпороговому режимам.

На комплексной плоскости  $\alpha = r e^{i\theta}$  при значительном превышении порога область, занятую генерируемым полем, можно наглядно представить, как это сделано на [рис. 3.7](#). Ломаная кривая характеризует распределение амплитуды колебаний, т. е. соответствует амплитудным шумам. Фаза  $\theta$  равновероятна в интервале  $0 - 2\pi$ , поэтому ломаная кривая располагается вблизи окружности  $r = \sqrt{\bar{n}_{st}}$  с радиусом, соответствующим наиболее вероятному значению  $|\alpha|$ .

Из рис. 3.7 видно, что амплитуда флуктуирует в узкой области в окрестности окружности радиуса  $r = \sqrt{\bar{n}_{st}}$ , а фаза свободно диффундирует (блуждает) вдоль этой окружности.

В лазере диффузия фазы происходит медленно, поэтому, если рассматривать не слишком большие промежутки времени, можно считать, что лазер генерирует излучение с хорошо определенной фазой. При усреднении за большой промежуток времени, когда фаза с равной вероятностью может принимать любое значение в интервале  $0 - 2\pi$ , среднее значение лазерного поля за этот промежуток времени будет равно нулю.

Рассмотрим более подробно процесс диффузии фазы. Предположим, что распределение амплитуды у нас установлено и  $P(r)$  соответствует стационарному распределению амплитуды. Тогда

$$P(r, \theta, t) = P(r) P(\theta, t).$$

В этом случае уравнение (3.14) примет вид

$$\frac{\partial P(\theta, t)}{\partial t} = \frac{A}{4r^2} \frac{\partial^2}{\partial \theta^2} P(\theta, t) \quad (3.19)$$

Функция  $P(r)$  сокращается, так как она удовлетворяет стационарному уравнению (3.17).

Уравнение (3.19) можно использовать для получения уравнения, которому удовлетворяет среднее поле. Среднее электрическое поле моды лазера, выраженное через  $P$ , имеет вид

$$\langle \hat{E} \rangle = E_1 \int P(\alpha, t) \alpha d^2 \alpha.$$

В полярных координатах это выглядит так:

$$\langle \hat{E} \rangle = E_1 \int_0^\infty r dr \int_0^{2\pi} r e^{i\theta} P(r, \theta, t) d\theta.$$

Используем теперь уравнение (3.19):

$$\begin{aligned} \frac{\partial \langle \hat{E} \rangle}{\partial t} &= E_1 \frac{\partial}{\partial t} \int_0^\infty r^2 dr \int_0^{2\pi} e^{i\theta} P(r, \theta, t) d\theta = \\ &= E_1 \int_0^\infty r^2 dr \int_0^{2\pi} e^{i\theta} \frac{\partial P}{\partial t} d\theta = \\ &= \frac{E_1 A}{\bar{n}_{st} 4} \int_0^\infty r^2 dr \int_0^{2\pi} e^{i\theta} \frac{\partial^2}{\partial \theta^2} P(r, \theta, t) d\theta. \end{aligned} \quad (3.20)$$

Здесь мы приближенно заменили  $\frac{1}{r^2} \approx \frac{1}{\bar{n}_{st}}$ , считая распределение для амплитуд достаточно узким.

Проинтегрируем внутренний интеграл дважды по частям. Имеем

$$\begin{aligned} \int_0^{2\pi} e^{i\theta} \frac{\partial^2 P}{\partial \theta^2} d\theta &= e^{i\theta} \frac{\partial P}{\partial \theta} \Big|_0^{2\pi} - i \int_0^{2\pi} e^{i\theta} \frac{\partial P}{\partial \theta} d\theta = \\ &= -ie^{i\theta} P \Big|_0^{2\pi} - \int_0^{2\pi} e^{i\theta} P d\theta. \end{aligned} \quad (3.21)$$

Первые слагаемые в (3.21) равны нулю из-за периодичности  $P$ ,  $\frac{\partial P}{\partial \theta}$ . Учитывая (3.21), уравнению (3.20) можно придать вид

$$\begin{aligned} \frac{\partial \langle E \rangle}{\partial t} &= E_1 \int_0^\infty r^2 dr \int_0^{2\pi} e^{i\theta} \frac{\partial P}{\partial t} d\theta = \\ &= -\frac{AE_1}{4\bar{n}_{st}} \int_0^\infty r dr \int_0^{2\pi} r e^{i\theta} P d\theta = -\frac{A}{4\bar{n}_{st}} \langle E \rangle. \end{aligned} \quad (3.22)$$

Решение этого уравнения

$$\langle E(t) \rangle = \langle E(0) \rangle e^{-\frac{D}{2}t}, \quad (3.23)$$

где

$$D = \frac{A}{2\bar{n}_{st}}. \quad (3.24)$$

Таким образом мы получили, что среднее поле действительно стремится к нулю с характерным временем  $\tau = \frac{1}{D}$ . В лазерах этот интервал может быть достаточно большим по сравнению с периодом колебаний.

Для определения естественной ширины спектра излучения лазера необходимо найти корреляционную функцию излучения лазера, ее спектр по теореме Хинчина-Винера (Теорема 15.2.1) будет энергетическим спектром лазерного излучения. Имеем

$$\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \rangle = E_1^2 \int d^2\alpha P(\alpha) \alpha^*(0) \alpha(t) e^{-i\omega_0 t},$$

где  $P(\alpha)$  - квазивероятность состояния лазера, определяемая формулой (3.14). При переходе к полярным координатам (модуль-фаза)  $\alpha = re^{i\theta}$  мы считаем что амплитуда уже установилась и не меняется, а фаза меняется медленно, так что

$$\begin{aligned} \alpha^*(0) &= re^{i\theta(0)} = re^{i0} = r, \\ \alpha(t) &= re^{i\theta(t)} = re^{i\theta}, \end{aligned} \quad (3.25)$$

В (3.25) мы предполагали, что в начальный момент времени  $\theta(0) = 0$ , а в момент времени  $t$  -  $\theta(t) = \theta$ . Таким образом имеем:

$$\left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle = E_1^2 e^{-i\omega_0 t} \int_0^\infty r^3 dr \int_0^{2\pi} d\theta P(re^{i\theta}, t) e^{i\theta}.$$

Выведем уравнение, которому удовлетворяет  $\left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle$ . Имеем уравнение (3.19)  $\frac{\partial P(\theta, t)}{\partial t} = \frac{A}{4\bar{n}_{st}} \frac{\partial^2}{\partial \theta^2} P(\theta, t)$ , следовательно

$$\begin{aligned} \frac{d}{dt} \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle &= -i\omega_0 \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle + \\ &+ E_1^2 e^{-i\omega_0 t} \int_0^\infty r^3 dr \int_0^{2\pi} d\theta \frac{\partial}{\partial t} P(re^{i\theta}, t) e^{i\theta} = \\ &= -i\omega_0 \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle + \\ &+ \frac{E_1^2 A}{4\bar{n}_{st}} \int_0^\infty r^3 dr \int_0^{2\pi} d\theta \frac{\partial^2}{\partial \theta^2} P(re^{i\theta}, t) e^{i\theta}. \end{aligned} \quad (3.26)$$

Проведем в (3.26) дважды интегрирование по частям по  $\theta$ . Получим:

$$\begin{aligned} \int_0^{2\pi} d\theta \frac{\partial^2}{\partial \theta^2} P e^{i\theta} &= \frac{\partial}{\partial \theta} P e^{i\theta} \Big|_0^{2\pi} - i \int_0^{2\pi} d\theta \frac{\partial}{\partial \theta} P e^{i\theta} = \\ &= -i \int_0^{2\pi} d\theta \frac{\partial}{\partial \theta} P e^{i\theta} = -i P e^{i\theta} \Big|_0^{2\pi} - \int_0^{2\pi} d\theta P e^{i\theta} = - \int_0^{2\pi} d\theta P e^{i\theta}. \end{aligned}$$

Подставляя получившийся результат в исходное выражение (3.26), получим:

$$\begin{aligned} \frac{d}{dt} \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle &= -i\omega_0 \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle - \\ &- \frac{E_1^2 A}{4\bar{n}_{st}} \int_0^\infty r^3 dr \int_0^{2\pi} d\theta P(re^{i\theta}, t) e^{i\theta} = \\ &= -i\omega_0 \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle - \frac{A}{4\bar{n}_{st}} \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle. \end{aligned}$$

Решение этого уравнения имеет вид

$$r_+(t) = \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \right\rangle = \left\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(0) \right\rangle e^{-i\omega_0 t - \frac{D}{2} t}, \quad (3.27)$$

где

$$\frac{D}{2} = \frac{A}{4\bar{n}_{st}}.$$

Выражение (3.27) определяет корреляционную функцию  $r(t)$  в области  $t \geq 0$ . В случае  $t \leq 0$ , с учетом (15.5), корреляционная функция может быть записана в виде

$$r_-(t) = r_-(-|t|) = r_+^*(|t|). \quad (3.28)$$

С учетом выражений (3.27) и (3.28) можно написать следующее выражение для фурье образа корреляционной функции, которая согласно теореме Хинчина-Винера (Теорема 15.2.1) определяет энергетический спектр  $S(\omega)$ :

$$\begin{aligned} S(\omega) &= \tilde{r}(\omega) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} e^{i\omega t} r(t) dt = \\ &= \frac{1}{2\pi} \int_{-\infty}^0 e^{i\omega t} r_-(t) dt + \frac{1}{2\pi} \int_0^{+\infty} e^{i\omega t} r_+(t) dt = \\ &= \frac{1}{2\pi} \int_0^{+\infty} e^{-i\omega t} r_+^*(t) dt + \frac{1}{2\pi} \int_0^{+\infty} e^{i\omega t} r_+(t) dt = \\ &= \frac{1}{\pi} \operatorname{Re} \int_0^{+\infty} e^{i\omega t} r_+(t) dt = \\ &= \frac{1}{\pi} \operatorname{Re} \int_0^{+\infty} e^{i\omega t} \langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(t) \rangle dt = \\ &= \frac{\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(0) \rangle}{\pi} \operatorname{Re} \int_0^{+\infty} e^{(i(\omega - \omega_0) - \frac{D}{2})t} dt = \\ &= \frac{\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(0) \rangle}{\pi} \operatorname{Re} \frac{1}{\frac{D}{2} - i(\omega - \omega_0)} = \\ &= \frac{\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(0) \rangle}{\pi} \operatorname{Re} \frac{\frac{D}{2} + i(\omega - \omega_0)}{(\omega - \omega_0)^2 + (D/2)^2} = \\ &= \frac{\langle \hat{E}^{(-)}(0) \hat{E}^{(+)}(0) \rangle}{\pi} \frac{D/2}{(\omega - \omega_0)^2 + (D/2)^2}. \end{aligned} \quad (3.29)$$

При выводе (3.29) использовалось определение преобразования Фурье (18.1) из разд. 18.1.

Получилось, что линия генерации лоренцовская, а ширина линии равна  $D$  (рис. 3.8). Поскольку мы рассматривали только "естественную", принципиально не устранимую причину уширения линии генерации, связанную с квантовыми флуктуациями, и пренебрегали принципиально устранимыми техническими причинами, полученная ширина получилась предельно узкой.

Здесь мы рассмотрели простейшую модель лазера. Более реалистическая модель трехуровневой системы рассмотрена в [43]. Результаты, полученные

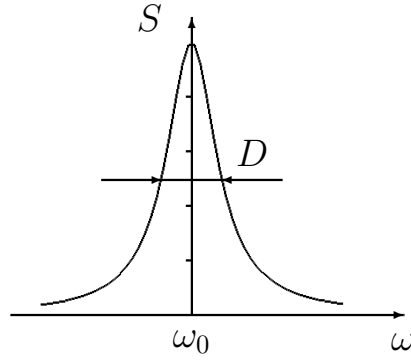


Рис. 3.8: К вычислению ширины линии генерации лазера. Зависимость спектральной плотности мощности  $S(\omega)$  от частоты  $\omega$ . Ширина линии определяется по половине мощности, т.е. рассматриваются те величины  $\omega$  при которых  $\frac{S(\omega)}{S(\omega_0)} \geq \frac{1}{2}$ . Из (3.29) следует, что границам интервала соответствуют частоты  $\omega = \omega_0 \pm \frac{D}{2}$ . Т.е. ширина линии -  $D$ .

для различных моделей лазера, хорошо согласуются между собой и соответствуют результатам, полученным с использованной нами простейшей модели.

### 3.5 Упражнения

1. Вывести (3.5) из (3.4).
2. Из (3.6) получить выражение для диагональных элементов матрицы плотности (3.7).
3. Из (3.6) получить выражение для оператора плотности в представлении когерентных состояний (3.8).
4. Представить уравнение (3.8) в полярных координатах.
5. Получить уравнение (3.19) из общего уравнения (3.14).
6. Воспользовавшись формулами (3.24) и (3.29), оценить "естественную" ширину линии генерации лазера для  $A \approx \frac{\omega}{Q}$  (малое превышение порога),  $\frac{\omega}{Q} = \Delta\omega = 10^6 \text{ Гц}$ ,  $n_{st} = 10^6 - 10^7$  фотонов в моде.



## Глава 4

# Квантовая теория лазера в представлении Гейзенберга

До сих пор мы рассматривали квантовую теорию лазера, используя представление Шредингера, в котором от времени зависит матрица плотности, а операторы от времени не зависят. Как мы видели на примере задачи о затухании моды резонатора, возможен другой подход, использующий представление Гейзенберга [53], когда от времени зависят операторы, а матрица плотности от времени не зависит. В ряде случаев такой подход может оказаться более удобным для исследования тонких вопросов квантовой теории лазеров, таких например, как генерация лазером поля в сжатом состоянии.

### 4.1 Модель лазера

Схема лазерных уровней изображена на [рис. 4.1](#). Уровень  $c$  - основной уровень, уровень  $b$  - нижний рабочий уровень,  $a$  - верхний рабочий уровень. На самом деле схема - четырехуровневая. Накачка ведется некогерентным светом через достаточно широкую линию поглощения, изображенную на рисунке пунктиром. Но так как предполагается высокая скорость безизлучательного перехода на верхний рабочий уровень, можно считать, что накачка происходит прямо на уровень  $a$ . Наличие четвертого уровня позволяет сильно уменьшить обратный переход с уровня  $a$  на основной уровень  $c$ . На [рис. 4.1](#) обозначены переходы, которые будут учитываться в теории.  $\gamma_a$  и  $\gamma_b$  характеризуют релаксацию населенностей с уровней  $a$  и  $b$  за счет связи с диссипативной системой.  $r_a$  - скорость накачки верхнего рабочего уровня  $a$  за счет некогерентной оптической накачки. Переход  $a \rightarrow c$  вынужденный переход, вызываемый генерируемым лазером полем.

Схема лазера представлена на [рис. 4.2](#). Схема содержит резонатор  $F$ , в котором возбуждается генерируемая мода, взаимодействующая с активными

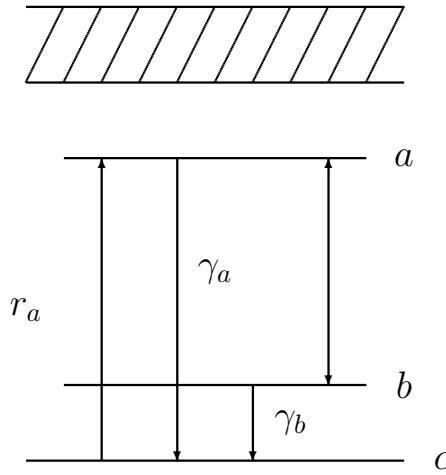


Рис. 4.1: Схема лазерных уровней. Уровень  $c$  - основной уровень, уровень  $b$  - нижний рабочий уровень,  $a$  - верхний рабочий уровень.  $\gamma_a$  и  $\gamma_b$  характеризуют релаксацию населенностей с уровней  $a$  и  $b$  за счет связи с диссипативной системой.  $r_a$  - скорость накачки верхнего рабочего уровня  $a$  за счет некогерентной оптической накачки.

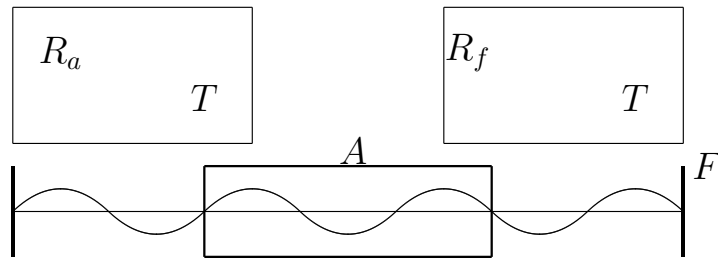


Рис. 4.2: Модель лазера. Через  $F$  обозначен резонатор, в котором возбуждается генерируемая мода, взаимодействующая с активными атомами рабочей среды  $A$ . Кроме того, имеются два резервуара при температуре  $T$ :  $R_a$ , который связан с активными атомами, и  $R_F$ , связанный с модой.

атомами рабочей среды, схема которой представлена на [рис. 4.1](#). Кроме того, имеются два резервуара при температуре  $T$   $R_a$  (связан с активными атомами) и  $R_F$  (связан с модой), вызывающие релаксацию атомов и поля моды.

## 4.2 Уравнение Гейзенберга для лазерной системы

Рассматриваемая система состоит из 4-х подсистем, которые связаны между собой посредством 3-х гамильтонианов взаимодействия. Первая из подсистем представляет собой моду электромагнитного поля с частотой  $\omega$  (на

рис. 4.2 обозначена через  $F$ ), которая описывается операторами рождения и уничтожения моды:  $\hat{a}^\dagger$  и  $\hat{a}$ .

Мода электромагнитного поля связана с резервуаром  $R_F$  (см. рис. 4.2), который представляет собой совокупность гармонических осцилляторов с частотой  $\omega_k^{(F)}$ , описываемых операторами рождения и уничтожения  $\hat{b}_k^\dagger, \hat{b}_k$ . При этом справедливы следующие коммутационные соотношения

$$\begin{aligned} [\hat{b}_k, \hat{b}_{k'}^\dagger] &= \delta_{kk'}, \\ [\hat{b}_k, \hat{b}_{k'}] &= 0, \\ [\hat{b}_k^\dagger, \hat{b}_{k'}^\dagger] &= 0. \end{aligned}$$

Атомная подсистема состоит из большого числа атомов. Атом  $j$  может находиться в следующих основных состояниях:  $|a\rangle^j, |b\rangle^j$  и  $|c\rangle^j$ . Поведение этого атома может быть описано с помощью операторов проектирования в состояния  $|a\rangle^j$  и  $|b\rangle^j$ :

$$\hat{\sigma}_a^j = |a\rangle^j \langle a|^j, \quad \hat{\sigma}_b^j = |b\rangle^j \langle b|^j,$$

а также операторов перехода

$$\begin{aligned} \hat{\sigma}_{a \rightarrow b}^j &= \hat{\sigma}_{ab}^j = |b\rangle^j \langle a|^j, \quad \hat{\sigma}_{b \rightarrow a}^j = \hat{\sigma}_{ba}^j = \left(\hat{\sigma}_{ab}^j\right)^\dagger, \\ \hat{\sigma}_{a \rightarrow c}^j &= \hat{\sigma}_{ac}^j = |c\rangle^j \langle a|^j, \quad \hat{\sigma}_{c \rightarrow a}^j = \hat{\sigma}_{ca}^j = \left(\hat{\sigma}_{ac}^j\right)^\dagger, \\ \hat{\sigma}_{b \rightarrow c}^j &= \hat{\sigma}_{bc}^j = |c\rangle^j \langle b|^j, \quad \hat{\sigma}_{c \rightarrow b}^j = \hat{\sigma}_{cb}^j = \left(\hat{\sigma}_{bc}^j\right)^\dagger. \end{aligned}$$

Атомная подсистема связана с резервуаром  $R_A$ , который состоит из большого числа гармонических осцилляторов каждый из которых имеет частоту  $\omega_k^{(A)}$  и описывается операторами рождения и уничтожения  $\hat{c}_k^\dagger, \hat{c}_k$  удовлетворяющими следующим коммутационным соотношениям:

$$\begin{aligned} [\hat{c}_k, \hat{c}_{k'}^\dagger] &= \delta_{kk'}, \\ [\hat{c}_k, \hat{c}_{k'}] &= 0, \\ [\hat{c}_k^\dagger, \hat{c}_{k'}^\dagger] &= 0. \end{aligned}$$

В общем случае уравнение Гейзенберга имеет вид:

$$\frac{d\hat{O}}{dt} = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{O}], \quad (4.1)$$

где  $\hat{\mathcal{H}}$  - гамильтониан системы,  $\hat{O}$  - оператор некоторой наблюдаемой, относящейся к этой системе. В целях упрощения мы будем использовать представление взаимодействия в котором уравнение (4.1) перепишется в виде:

$$\frac{d\hat{O}_I}{dt} = \frac{i}{\hbar} [\hat{V}_I, \hat{O}_I], \quad (4.2)$$

где операторы взаимодействия  $\hat{V}_I$  и наблюдаемой  $\hat{O}_I$  в представлении взаимодействия записываются следующим образом:

$$\begin{aligned} \hat{O}_I &= e^{i\frac{\hat{\mathcal{H}}_0 t}{\hbar}} \hat{O} e^{-i\frac{\hat{\mathcal{H}}_0 t}{\hbar}}, \\ \hat{V}_I &= e^{i\frac{\hat{\mathcal{H}}_0 t}{\hbar}} \hat{V} e^{-i\frac{\hat{\mathcal{H}}_0 t}{\hbar}}. \end{aligned} \quad (4.3)$$

Через  $\hat{\mathcal{H}}_0$  в (4.3) обозначен полный гамильтониан рассматриваемой системы без учета взаимодействия между ее частями.

В дальнейшем все операторы у нас будут предполагаться записанными в представлении взаимодействия (4.3) при этом индекс  $I$  будет опускаться.

Гамильтониан взаимодействия между  $j$ -м атомом и модой электромагнитного поля в представлении взаимодействия имеет вид (см. 2.14):

$$\hat{V}_{AF}^j = \Delta(t - t_j) g \hbar \left( \hat{a}^\dagger \hat{\sigma}_{ab}^j e^{i(\omega - \omega_{ab})t} + \left( \hat{\sigma}_{ab}^j \right)^\dagger \hat{a} e^{-i(\omega - \omega_{ab})t} \right), \quad (4.4)$$

где  $\Delta(t - t_j)$  ступенчатая функция описывающая процесс инжекции атомов, т. е. учитывающая тот факт, что взаимодействие между  $j$ -м атомом и полем начинается в момент времени  $t_j$ :

$$\Delta(t - t_j) = \begin{cases} 1; & t \geq t_j \\ 0; & t < t_j \end{cases}$$

Полный гамильтониан взаимодействия будет суммой гамильтонианов отдельных атомов (4.4):

$$\hat{V}_{AF} = g \hbar \sum_j \Delta(t - t_j) \left( \hat{a}^\dagger \hat{\sigma}_{ab}^j + \left( \hat{\sigma}_{ab}^j \right)^\dagger \hat{a} \right). \quad (4.5)$$

В (4.5) мы предполагаем что частота моды электромагнитного поля совпадает с частотой перехода:  $\omega = \omega_{ab}$ .

Гамильтониан взаимодействия поля с резервуаром  $R_F$  записывается следующим образом:

$$\hat{V}_{FR_F} = \hbar \sum_k g_k^{(F)} \left( \hat{b}_k^\dagger \hat{a} e^{i(\omega_k^{(F)} - \omega)t} + \hat{a}^\dagger \hat{b}_k e^{-i(\omega_k^{(F)} - \omega)t} \right). \quad (4.6)$$

Сложнее дело обстоит с гамильтонианом взаимодействия атомной подсистемы с резервуаром  $R_A$ . Исходя из рассматриваемой модели (см. [рис. 4.2](#)) мы имеем дело с двумя переходами:  $a \rightarrow c$  и  $b \rightarrow c$ . Соответственно полный гамильтониан запишется в виде

$$\hat{V}_{AR_A} = \hat{V}_{AR_A}^{a \rightarrow c} + \hat{V}_{AR_A}^{b \rightarrow c}.$$

Предполагая в дальнейшем, что константы взаимодействия для рассматриваемых переходов одинаковыми и вещественными, получим

$$\begin{aligned} \hat{V}_{AR_A}^{a \rightarrow c} &= \hbar \sum_{k,j} g_k^{(A)} \left( \hat{c}_k^\dagger \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{ac})t} + (\hat{\sigma}_{ac}^j)^\dagger \hat{c}_k e^{-i(\omega_k^{(A)} - \omega_{ac})t} \right), \\ \hat{V}_{AR_A}^{b \rightarrow c} &= \hbar \sum_{k,j} g_k^{(A)} \left( \hat{c}_k^\dagger \hat{\sigma}_{bc}^j e^{i(\omega_k^{(A)} - \omega_{bc})t} + (\hat{\sigma}_{bc}^j)^\dagger \hat{c}_k e^{-i(\omega_k^{(A)} - \omega_{bc})t} \right). \end{aligned} \quad (4.7)$$

В (4.7) суммирование предполагается по всем атомам (индекс  $j$ ) и по всем модам резервуара ( $k$ ), через  $\omega_{ac}$  и  $\omega_{bc}$  обозначены частоты переходов.

### 4.2.1 Уравнение движения атомной подсистемы

Прежде всего рассмотрим уравнения которым удовлетворяют операторы  $\hat{c}_k$  и  $\hat{c}_k^\dagger$ . Поскольку эти операторы входят только в гамильтониан  $\hat{V}_{AR_A}$ , то уравнение движения имеет вид

$$\begin{aligned} \frac{d\hat{c}_k}{dt} &= \frac{i}{\hbar} \left[ \hat{V}_{AR_A}, \hat{c}_k \right] = \\ &= \frac{i}{\hbar} \sum_{k',j} g_{k'}^{(A)} \left[ \hat{c}_{k'}^\dagger, \hat{c}_k \right] \left( \hat{\sigma}_{ac}^j e^{i(\omega_{k'}^{(A)} - \omega_{ac})t} + \hat{\sigma}_{bc}^j e^{i(\omega_{k'}^{(A)} - \omega_{bc})t} \right) + \\ &+ \frac{i}{\hbar} \sum_{k',j} g_{k'}^{(A)} \left( (\hat{\sigma}_{ac}^j)^\dagger e^{-i(\omega_{k'}^{(A)} - \omega_{ac})t} + (\hat{\sigma}_{bc}^j)^\dagger e^{-i(\omega_{k'}^{(A)} - \omega_{bc})t} \right) [\hat{c}_{k'}, \hat{c}_k] = \\ &= -i \sum_{k',j} g_{k'}^{(A)} \delta_{kk'} \left( \hat{\sigma}_{ac}^j e^{i(\omega_{k'}^{(A)} - \omega_{ac})t} + \hat{\sigma}_{bc}^j e^{i(\omega_{k'}^{(A)} - \omega_{bc})t} \right) = \\ &= -i g_k^{(A)} \sum_j \left( \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{ac})t} + \hat{\sigma}_{bc}^j e^{i(\omega_k^{(A)} - \omega_{bc})t} \right). \end{aligned} \quad (4.8)$$

Формальное интегрирование (4.8) дает

$$\begin{aligned} \hat{c}_k(t) &= \hat{c}_k(0) - \\ &- i g_k^{(A)} \sum_j \int_0^t dt' \left( \hat{\sigma}_{ac}^j(t') e^{i(\omega_k^{(A)} - \omega_{ac})t'} + \hat{\sigma}_{bc}^j(t') e^{i(\omega_k^{(A)} - \omega_{bc})t'} \right), \end{aligned} \quad (4.9)$$

откуда для эрмитово сопряженного оператора  $\hat{c}_k^\dagger$  имеем

$$\begin{aligned} \hat{c}_k^\dagger(t) &= \hat{c}_k^\dagger(0) + \\ &+ i g_k^{(A)} \sum_j \int_0^t dt' \left( \hat{\sigma}_{ca}^j(t') e^{-i(\omega_k^{(A)} - \omega_{ac})t'} + \hat{\sigma}_{cb}^j(t') e^{-i(\omega_k^{(A)} - \omega_{bc})t'} \right), \end{aligned} \quad (4.10)$$

где введены следующие обозначения  $\hat{\sigma}_{ca}^j = (\hat{\sigma}_{ac}^j)^\dagger$  и  $\hat{\sigma}_{cb}^j = (\hat{\sigma}_{bc}^j)^\dagger$ .

Следующим шагом будет получение уравнений которым удовлетворяют операторы  $\hat{\sigma}_a^j$  и  $\hat{\sigma}_b^j$ . Для  $\hat{\sigma}_a^j$  имеем

$$\frac{d\hat{\sigma}_a^j}{dt} = \frac{i}{\hbar} [\hat{V}_{AF}, \hat{\sigma}_a^j] + \frac{i}{\hbar} [\hat{V}_{AR_A}, \hat{\sigma}_a^j]. \quad (4.11)$$

Для первого члена суммы (4.11) справедливо

$$\frac{i}{\hbar} [\hat{V}_{AF}, \hat{\sigma}_a^j] = \frac{i}{\hbar} g \hbar \sum_i \Delta(t - t_i) \left( \hat{a}^\dagger [\hat{\sigma}_{ab}^i, \hat{\sigma}_a^j] + [(\hat{\sigma}_{ab}^i)^\dagger, \hat{\sigma}_a^j] \hat{a} \right),$$

откуда с учетом коммутационных соотношений

$$\begin{aligned} [\hat{\sigma}_{ab}^i, \hat{\sigma}_a^j] &= |b^i\rangle \langle a^i| a^j \rangle \langle a^j| - |a^j\rangle \langle a^j| b^i \rangle \langle a^i| = \delta_{ij} \hat{\sigma}_{ab}^j, \\ [(\hat{\sigma}_{ab}^i)^\dagger, \hat{\sigma}_a^j] &= |a^i\rangle \langle b^i| a^j \rangle \langle a^j| - |a^j\rangle \langle a^j| a^i \rangle \langle b^i| = -\delta_{ij} (\hat{\sigma}_{ab}^j)^\dagger \end{aligned}$$

получим

$$\frac{i}{\hbar} [\hat{V}_{AF}, \hat{\sigma}_a^j] = i g \Delta(t - t_j) \left( \hat{a}^\dagger \hat{\sigma}_{ab}^j - (\hat{\sigma}_{ab}^j)^\dagger \hat{a} \right). \quad (4.12)$$

Для второго члена суммы (4.11) имеем

$$\begin{aligned} &\frac{i}{\hbar} [\hat{V}_{AR_A}, \hat{\sigma}_a^j] = \\ &= i \sum_{k,i} g_k^{(A)} \hat{c}_k^\dagger \left( [\hat{\sigma}_{ac}^i, \hat{\sigma}_a^j] e^{i(\omega_k^{(A)} - \omega_{ac})t} + [\hat{\sigma}_{bc}^i, \hat{\sigma}_a^j] e^{i(\omega_k^{(A)} - \omega_{bc})t} \right) + \\ &+ i \sum_{k,i} g_k^{(A)} \left( [(\hat{\sigma}_{ac}^i)^\dagger, \hat{\sigma}_a^j] e^{-i(\omega_k^{(A)} - \omega_{ac})t} + [(\hat{\sigma}_{bc}^i)^\dagger, \hat{\sigma}_a^j] e^{-i(\omega_k^{(A)} - \omega_{bc})t} \right) \hat{c}_k, \end{aligned}$$

которое с помощью коммутационных соотношений

$$\begin{aligned} [\hat{\sigma}_{ac}^i, \hat{\sigma}_a^j] &= \delta_{ij} \hat{\sigma}_{ac}^j, \\ [(\hat{\sigma}_{ac}^i)^\dagger, \hat{\sigma}_a^j] &= -\delta_{ij} (\hat{\sigma}_{ac}^j)^\dagger, \\ [\hat{\sigma}_{bc}^i, \hat{\sigma}_a^j] &= 0, \\ [(\hat{\sigma}_{bc}^i)^\dagger, \hat{\sigma}_a^j] &= 0 \end{aligned} \quad (4.13)$$

переписывается в виде

$$\begin{aligned} \frac{i}{\hbar} \left[ \hat{V}_{AR_A}, \hat{\sigma}_a^j \right] = & i \sum_k g_k^{(A)} \hat{c}_k^\dagger \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{ac})t} - \\ & - i \sum_k g_k^{(A)} (\hat{\sigma}_{ac}^i)^\dagger \hat{c}_k e^{-i(\omega_k^{(A)} - \omega_{ac})t}. \end{aligned} \quad (4.14)$$

Объединяя вместе (4.12) и (4.14) получим

$$\frac{d\hat{\sigma}_a^j}{dt} = ig\Delta(t - t_j) \hat{a}^\dagger \hat{\sigma}_{ab}^j + i \sum_k g_k^{(A)} \hat{c}_k^\dagger \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{ac})t} + \text{э. с.} \quad (4.15)$$

При помощи (4.10) можно вычислить второе слагаемое (4.15):

$$\begin{aligned} i \sum_k g_k^{(A)} \hat{c}_k^\dagger \hat{\sigma}_{ac}^i e^{i(\omega_k^{(A)} - \omega_{ac})t} = & i \sum_k g_k^{(A)} \hat{c}_k^\dagger(0) \hat{\sigma}_{ac}^i e^{i(\omega_k^{(A)} - \omega_{ac})t} - \\ & - \sum_{k,i} \left( g_k^{(A)} \right)^2 \int_0^t dt' \hat{\sigma}_{ca}^i(t') \hat{\sigma}_{ac}^j(t) e^{i(\omega_k^{(A)} - \omega_{ac})(t-t')} - \\ & - \sum_{k,i} \left( g_k^{(A)} \right)^2 \int_0^t dt' \hat{\sigma}_{cb}^i(t') \hat{\sigma}_{ac}^j(t) e^{i(\omega_k^{(A)} - \omega_{bc})(t-t')} e^{i(\omega_{bc} - \omega_{ac})t}. \end{aligned}$$

Обозначив

$$\hat{f}_a^j(t) = i \sum_k g_k^{(A)} \hat{c}_k^\dagger(0) \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{ac})t} \quad (4.16)$$

получим

$$\begin{aligned}
& i \sum_k g_k^{(A)} \hat{c}_k^\dagger \hat{\sigma}_{ac}^i e^{i(\omega_k^{(A)} - \omega_{ac})t} = \hat{f}_a^j - \\
& - \sum_i \int_0^t dt' \sum_k \left(g_k^{(A)}\right)^2 \hat{\sigma}_{ca}^i(t') \hat{\sigma}_{ac}^j(t) e^{i(\omega_k^{(A)} - \omega_{ac})(t-t')} - \\
& - e^{i(\omega_{bc} - \omega_{ac})t} \sum_i \int_0^t dt' \sum_k \left(g_k^{(A)}\right)^2 \hat{\sigma}_{cb}^i(t') \hat{\sigma}_{ac}^j(t) e^{i(\omega_k^{(A)} - \omega_{bc})(t-t')} = \\
& = \hat{f}_a^j - D(\omega_{ac}) \left(g^{(A)}(\omega_{ac})\right)^2 \sum_i \int_0^t dt' \int_0^\infty d\omega' \hat{\sigma}_{ca}^i(t') \hat{\sigma}_{ac}^j(t) e^{i(\omega' - \omega_{ac})(t-t')} - \\
& - D(\omega_{bc}) \left(g^{(A)}(\omega_{bc})\right)^2 e^{i(\omega_{bc} - \omega_{ac})t} \cdot \\
& \cdot \sum_i \int_0^t dt' \int_0^\infty d\omega' \hat{\sigma}_{cb}^i(t') \hat{\sigma}_{ac}^j(t) e^{i(\omega' - \omega_{bc})(t-t')} \approx \\
& \approx \hat{f}_a^j - \frac{\gamma_a}{2} \sum_i \int_0^t dt' \hat{\sigma}_{ca}^i(t') \hat{\sigma}_{ac}^j(t) \delta(t - t') - \\
& - \frac{\gamma_b}{2} e^{i(\omega_{bc} - \omega_{ac})t} \sum_i \int_0^t dt' \hat{\sigma}_{cb}^i(t') \hat{\sigma}_{ac}^j(t) \delta(t - t') = \\
& = \hat{f}_a^j - \frac{\gamma_a}{2} \hat{\sigma}_a^j(t) - \frac{\gamma_b}{2} e^{i(\omega_{bc} - \omega_{ac})t} \hat{\sigma}_{ba}^j(t) \approx \\
& \approx \hat{f}_a^j - \frac{\gamma_a}{2} \hat{\sigma}_a^j(t) \quad (4.17)
\end{aligned}$$

где

$$\gamma_a = 4\pi D(\omega_{ac}) \left(g^{(A)}(\omega_{ac})\right)^2$$

и

$$\gamma_b = 4\pi D(\omega_{bc}) \left(g^{(A)}(\omega_{bc})\right)^2.$$

При выводе (4.17) мы также пренебрегли быстро осциллирующим членом  $\frac{\gamma_b}{2} e^{i(\omega_{bc} - \omega_{ac})t} \hat{\sigma}_{ba}^j(t)$  по сравнению с  $\frac{\gamma_a}{2} \hat{\sigma}_a^j(t)$ . Таким образом в результате получаем

$$\frac{d\hat{\sigma}_a^j}{dt} = -\gamma_a \hat{\sigma}_a^j + ig\Delta(t - t_j) \left(\hat{a}^\dagger \hat{\sigma}_{ab}^j - \left(\hat{\sigma}_{ab}^j\right)^\dagger \hat{a}\right) + \hat{f}_a^j. \quad (4.18)$$

По аналогии, можно получить выражение для  $\hat{\sigma}_b^j$ :

$$\frac{d\hat{\sigma}_b^j}{dt} = -\gamma_b \hat{\sigma}_b^j - ig\Delta(t - t_j) \left(\hat{a}^\dagger \hat{\sigma}_{ab}^j - \left(\hat{\sigma}_{ab}^j\right)^\dagger \hat{a}\right) + \hat{f}_b^j, \quad (4.19)$$



где

$$\hat{f}_b^j(t) = i \sum_k g_k^{(A)} \hat{c}_k^\dagger(0) \hat{\sigma}_{bc}^i e^{i(\omega_k^{(A)} - \omega_{bc})t} + \text{э. с.} \quad (4.20)$$

Для  $\hat{\sigma}_{ab}^j$  имеем

$$\frac{d\hat{\sigma}_{ab}^j}{dt} = \frac{i}{\hbar} [\hat{V}_{AF}, \hat{\sigma}_{ab}^j] + \frac{i}{\hbar} [\hat{V}_{AR_A}, \hat{\sigma}_{ab}^j]. \quad (4.21)$$

Для первого члена суммы (4.21) справедливо

$$\frac{i}{\hbar} [\hat{V}_{AF}, \hat{\sigma}_{ab}^j] = \frac{i}{\hbar} g \hbar \sum_i \Delta(t - t_i) \left( \hat{a}^\dagger [\hat{\sigma}_{ab}^i, \hat{\sigma}_{ab}^j] + [(\hat{\sigma}_{ab}^i)^\dagger, \hat{\sigma}_{ab}^j] \hat{a} \right),$$

Откуда с учетом

$$[(\hat{\sigma}_{ab}^i)^\dagger, \hat{\sigma}_{ab}^j] = |a^i\rangle \langle b^i| b^j \rangle \langle a^j| - |b^j\rangle \langle a^j| a^i \rangle \langle b^i| = -\delta_{ij} (\hat{\sigma}_a^j - \hat{\sigma}_b^j)$$

получим

$$\frac{i}{\hbar} [\hat{V}_{AF}, \hat{\sigma}_{ab}^j] = ig \Delta(t - t_j) (\hat{\sigma}_a^j - \hat{\sigma}_b^j) \hat{a}. \quad (4.22)$$

Для второго члена суммы (4.21) имеем

$$\begin{aligned} & \frac{i}{\hbar} [\hat{V}_{AR_A}, \hat{\sigma}_{ab}^j] = \\ &= i \sum_{k,i} g_k^{(A)} \hat{c}_k^\dagger \left( [\hat{\sigma}_{ac}^i, \hat{\sigma}_{ab}^j] e^{i(\omega_k^{(A)} - \omega_{ac})t} + [\hat{\sigma}_{bc}^i, \hat{\sigma}_{ab}^j] e^{i(\omega_k^{(A)} - \omega_{bc})t} \right) + \\ &+ i \sum_{k,i} g_k^{(A)} \left( [(\hat{\sigma}_{ac}^i)^\dagger, \hat{\sigma}_{ab}^j] e^{-i(\omega_k^{(A)} - \omega_{ac})t} + [(\hat{\sigma}_{bc}^i)^\dagger, \hat{\sigma}_{ab}^j] e^{-i(\omega_k^{(A)} - \omega_{bc})t} \right) \hat{c}_k, \end{aligned}$$

которое с помощью коммутационных соотношений

$$\begin{aligned} [\hat{\sigma}_{ac}^i, \hat{\sigma}_{ab}^j] &= 0, \\ [(\hat{\sigma}_{ac}^i)^\dagger, \hat{\sigma}_{ab}^j] &= -\delta_{ij} (\hat{\sigma}_{bc}^j)^\dagger, \\ [\hat{\sigma}_{bc}^i, \hat{\sigma}_{ab}^j] &= \delta_{ij} \hat{\sigma}_{ac}^j, \\ [(\hat{\sigma}_{bc}^i)^\dagger, \hat{\sigma}_{ab}^j] &= 0 \end{aligned} \quad (4.23)$$

переписывается в виде

$$\begin{aligned} \frac{i}{\hbar} \left[ \hat{V}_{AR_A}, \hat{\sigma}_{ab}^j \right] = & i \sum_k g_k^{(A)} \hat{c}_k^\dagger \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{bc})t} - \\ & - i \sum_k g_k^{(A)} \left( \hat{\sigma}_{bc}^j \right)^\dagger \hat{c}_k e^{-i(\omega_k^{(A)} - \omega_{ac})t}, \end{aligned} \quad (4.24)$$

Объединяя вместе (4.22) и (4.24) получим

$$\begin{aligned} \frac{d\hat{\sigma}_{ab}^j}{dt} = & ig\Delta(t - t_j) \left( \hat{\sigma}_a^j - \hat{\sigma}_b^j \right) \hat{a} + \\ & + i \sum_k g_k^{(A)} \hat{c}_k^\dagger \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{bc})t} - i \sum_k g_k^{(A)} \left( \hat{\sigma}_{bc}^j \right)^\dagger \hat{c}_k e^{-i(\omega_k^{(A)} - \omega_{ac})t} \end{aligned} \quad (4.25)$$

Подставив в (4.25) выражения для  $\hat{c}_k$  (4.9) и  $\hat{c}_k^\dagger$  (4.10) и пренебрегая быстро осциллирующими членами имеем:

$$\begin{aligned} \frac{d\hat{\sigma}_{ab}^j}{dt} = & ig\Delta(t - t_j) \left( \hat{\sigma}_a^j - \hat{\sigma}_b^j \right) \hat{a} - \\ & - \frac{\gamma_b}{2} \int_0^\infty dt' \hat{\sigma}_{cb}^j(t') \hat{\sigma}_{ac}^j(t) \delta(t - t') - \\ & - \frac{\gamma_a}{2} \int_0^\infty dt' \hat{\sigma}_{cb}^j(t) \hat{\sigma}_{ac}^j(t') \delta(t - t') + \hat{f}_{ab}^j, \end{aligned} \quad (4.26)$$

где

$$\begin{aligned} \hat{f}_{ab}^j(t) = & i \sum_k g_k^{(A)} \hat{c}_k^\dagger(0) \hat{\sigma}_{ac}^j e^{i(\omega_k^{(A)} - \omega_{bc})t} - \\ & - i \sum_k g_k^{(A)} \left( \hat{\sigma}_{bc}^j \right)^\dagger \hat{c}_k(0) e^{-i(\omega_k^{(A)} - \omega_{ac})t}. \end{aligned} \quad (4.27)$$

В дальнейшем мы будем пользоваться предположением о том, что

$$\gamma_a = \gamma_b = \gamma. \quad (4.28)$$

Приняв во внимание

$$\hat{\sigma}_{cb}^j \hat{\sigma}_{ac}^j = \hat{\sigma}_{ab}^j,$$

в результате из (4.26) получим

$$\begin{aligned} \frac{d\hat{\sigma}_{ab}^j}{dt} = & ig\Delta(t - t_j) \left( \hat{\sigma}_a^j - \hat{\sigma}_b^j \right) \hat{a} - \gamma \hat{\sigma}_{cb}^j \hat{\sigma}_{ac}^j + \hat{f}_{ab}^j = \\ = & ig\Delta(t - t_j) \left( \hat{\sigma}_a^j - \hat{\sigma}_b^j \right) \hat{a} - \gamma \hat{\sigma}_{ab}^j + \hat{f}_{ab}^j \end{aligned} \quad (4.29)$$

Для шумового оператора  $\hat{f}_{ab}^j$  можно записать следующие корреляционные функции:

$$\begin{aligned}\left\langle \left( \hat{f}_{ab}^i(t_1) \right)^\dagger \hat{f}_{ab}^j(t_2) \right\rangle &= \delta_{ij} \frac{\gamma}{2} \langle \hat{\sigma}_a^j \rangle \delta(t_1 - t_2), \\ \left\langle \hat{f}_{ab}^j(t_1) \left( \hat{f}_{ab}^i(t_2) \right)^\dagger \right\rangle &= \delta_{ij} \frac{\gamma}{2} \langle \hat{\sigma}_b^j \rangle \delta(t_1 - t_2).\end{aligned}\quad (4.30)$$

Действительно для первого соотношения (4.30) предполагая среднее число фононов в моде резервуара равным 0 в начальный момент времени:

$$\left\langle \hat{c}_{k_1}^\dagger(0) \hat{c}_{k_2}(0) \right\rangle = 0,$$

так что

$$\left\langle \hat{c}_{k_1}(0) \hat{c}_{k_2}^\dagger(0) \right\rangle = \delta_{k_1, k_2},$$

получим

$$\begin{aligned}& \left\langle \left( \hat{f}_{ab}^i(t_1) \right)^\dagger \hat{f}_{ab}^j(t_2) \right\rangle = \\ &= \sum_{k_1, k_2} g_{k_1}^{(A)} g_{k_2}^{(A)} \left\langle \hat{c}_{k_1}(0) \hat{c}_{k_2}^\dagger(0) \right\rangle \left\langle (\hat{\sigma}_{ac}^i)^\dagger \hat{\sigma}_{ac}^j \right\rangle e^{-i(\omega_{k_1}^{(A)} - \omega_{bc})t_1} e^{i(\omega_{k_2}^{(A)} - \omega_{bc})t_2} + \\ &+ \sum_{k_1, k_2} g_{k_1}^{(A)} g_{k_2}^{(A)} \left\langle \hat{c}_{k_1}^\dagger(0) \hat{c}_{k_2}(0) \right\rangle \left\langle \hat{\sigma}_{bc}^i (\hat{\sigma}_{bc}^j)^\dagger \right\rangle e^{i(\omega_{k_1}^{(A)} - \omega_{ac})t_1} e^{-i(\omega_{k_2}^{(A)} - \omega_{ac})t_2} = \\ &= \sum_k \left( g_k^{(A)} \right)^2 \left\langle (\hat{\sigma}_{ac}^i)^\dagger \hat{\sigma}_{ac}^j \right\rangle e^{-i(\omega_k^{(A)} - \omega_{bc})(t_1 - t_2)} = \\ &= \delta_{ij} \sum_k \left( g_k^{(A)} \right)^2 \langle \hat{\sigma}_a^j \rangle e^{-i(\omega_k^{(A)} - \omega_{bc})(t_1 - t_2)} = \delta_{ij} \frac{\gamma}{2} \langle \hat{\sigma}_a^j \rangle \delta(t_1 - t_2).\end{aligned}$$

## 4.2.2 Уравнения движения для макро-величин

От уравнений движения, описывающих поведение отдельного атома (4.18, 4.19, 4.29), следует перейти к уравнениям, описывающим поведение всей атомной подсистемы в целом. Для этого от операторов  $\hat{\sigma}_a^j$ ,  $\hat{\sigma}_b^j$  и  $\hat{\sigma}_{ab}^j$  мы перейдем к новым операторам которые определяют совокупное воздействие всех атомов:

$$\begin{aligned}\hat{N}_a &= \sum_j \Delta(t - t_j) \hat{\sigma}_a^j, \\ \hat{N}_b &= \sum_j \Delta(t - t_j) \hat{\sigma}_b^j, \\ \hat{N}_{ab} &= \sum_j \Delta(t - t_j) \hat{\sigma}_{ab}^j.\end{aligned}\quad (4.31)$$

Рассмотрим далее  $\frac{d\hat{N}_a}{dt}$ :

$$\begin{aligned}\frac{d\hat{N}_a}{dt} &= \sum_j \frac{d\Delta(t-t_j)}{dt} \hat{\sigma}_a^j + \sum_j \Delta(t-t_j) \frac{d\hat{\sigma}_a^j}{dt} = \\ &= \sum_j \delta(t-t_j) \hat{\sigma}_a^j + \sum_j \Delta(t-t_j) \frac{d\hat{\sigma}_a^j}{dt}.\end{aligned}\quad (4.32)$$

Подставляя далее (4.18) в (4.32) и принимая во внимание (4.28) получим:

$$\begin{aligned}\frac{d\hat{N}_a}{dt} &= \sum_j \delta(t-t_j) \hat{\sigma}_a^j - \gamma \sum_j \Delta(t-t_j) \hat{\sigma}_a^j + \\ &+ ig \sum_j \Delta(t-t_j) \left( \hat{a}^\dagger \hat{\sigma}_{ab}^j - \left( \hat{\sigma}_{ab}^j \right)^\dagger \hat{a} \right) + \sum_j \Delta(t-t_j) \hat{f}_a^j = \\ &= \sum_j \delta(t-t_j) \hat{\sigma}_a^j - \gamma \hat{N}_a + \\ &+ ig \left( \hat{a}^\dagger \hat{N}_{ab} - \hat{N}_{ab}^\dagger \hat{a} \right) + \sum_j \Delta(t-t_j) \hat{f}_a^j\end{aligned}\quad (4.33)$$

Рассмотрим далее среднее значение от первого члена (4.33):

$$\begin{aligned}\left\langle \sum_j \delta(t-t_j) \hat{\sigma}_a^j(t) \right\rangle &= \left\langle \sum_j \delta(t-t_j) \hat{\sigma}_a^j(t_j) \right\rangle = \\ &= \left\langle \sum_j \delta(t-t_j) \langle \hat{\sigma}_a^j(t_j) \rangle \right\rangle_T,\end{aligned}\quad (4.34)$$

где  $\langle \dots \rangle_T$  означает усреднение по моментам инъекции атомов:

$$\langle \dots \rangle_T = r_a \int_{-\infty}^{\infty} (\dots) dt_j, \quad (4.35)$$

где  $r_a$  скорость инъекции атомов. Для среднего значения оператора  $\hat{\sigma}_a^j$  предполагая, что в момент времени  $t_j$   $j$ -й атом инжектируется в возбужденном состоянии, имеем

$$\langle \hat{\sigma}_a^j(t_j) \rangle = \langle a | \hat{\sigma}_a^j | a \rangle = 1. \quad (4.36)$$

Подставив (4.35) и (4.36) в (4.34) получим

$$\left\langle \sum_j \delta(t-t_j) \hat{\sigma}_a^j(t) \right\rangle = r_a. \quad (4.37)$$

Далее добавим и вычтем среднее (4.37) из (4.33), в результате получим:

$$\frac{d\hat{N}_a}{dt} = r_a - \gamma\hat{N}_a + ig \left( \hat{a}^\dagger \hat{N}_{ab} - \hat{N}_{ab}^\dagger \hat{a} \right) + \hat{F}_a, \quad (4.38)$$

где введен новый шумовой оператор  $\hat{F}_a$ , который учитывает не только квантовые флуктуации, но флуктуации моментов инжекции активных атомов:

$$\hat{F}_a = \sum_j \delta(t - t_j) \hat{\sigma}_a^j - r_a + \sum_j \Delta(t - t_j) \hat{f}_a^j, \quad (4.39)$$

при этом очевидно что среднее значение данного оператора равно 0:

$$\langle \hat{F}_a \rangle = \left\langle \sum_j \delta(t - t_j) \hat{\sigma}_a^j \right\rangle - r_a + \left\langle \sum_j \Delta(t - t_j) \hat{f}_a^j \right\rangle = 0.$$

Из (4.19, 4.29) можно получить следующие соотношения для  $\hat{N}_b$  и  $\hat{N}_{ab}$ :

$$\begin{aligned} \frac{d\hat{N}_b}{dt} &= -\gamma\hat{N}_b - ig \left( \hat{a}^\dagger \hat{N}_{ab} - \hat{N}_{ab}^\dagger \hat{a} \right) + \hat{F}_b, \\ \frac{d\hat{N}_{ab}}{dt} &= -\gamma\hat{N}_{ab} + ig \left( \hat{N}_a - \hat{N}_b \right) \hat{a} + \hat{F}_{ab}, \end{aligned} \quad (4.40)$$

где введены следующие шумовые операторы

$$\begin{aligned} \hat{F}_b &= \sum_j \Delta(t - t_j) \hat{f}_b^j + \sum_j \delta(t - t_j) \hat{\sigma}_b^j, \\ \hat{F}_{ab} &= \sum_j \Delta(t - t_j) \hat{f}_{ab}^j + \sum_j \delta(t - t_j) \hat{\sigma}_{ab}^j. \end{aligned} \quad (4.41)$$

С учетом того, что

$$\langle \hat{\sigma}_b^j(t_j) \rangle = \langle \hat{\sigma}_{ab}^j(t_j) \rangle = 0,$$

эти операторы обладают нулевым средним.

Для коррелятора  $\langle \hat{F}_{ab}^\dagger(t_1) \hat{F}_{ab}(t_2) \rangle$  из (4.30) можно получить следующее соотношение

$$\begin{aligned} \langle \hat{F}_{ab}^\dagger(t_1) \hat{F}_{ab}(t_2) \rangle &= \sum_{ij} \Delta(t_1 - t_i) \Delta(t_2 - t_j) \left\langle \left( \hat{f}_{ab}^i \right)^\dagger \hat{f}_{ab}^j \right\rangle + \\ &\quad + \sum_{ij} \delta(t_1 - t_i) \delta(t_2 - t_j) \left\langle \left( \hat{\sigma}_{ab}^i \right)^\dagger \hat{\sigma}_{ab}^j \right\rangle = \\ &= \frac{\gamma}{2} \delta(t_1 - t_2) \sum_j \Delta(t_1 - t_j) \langle \hat{\sigma}_a^j \rangle + \delta(t_1 - t_2) \sum_j \delta(t_1 - t_j) \langle \hat{\sigma}_a^j \rangle = \\ &= \left( \frac{\gamma}{2} \bar{N}_a + r_a \right) \delta(t_1 - t_2), \end{aligned} \quad (4.42)$$

где через  $\bar{N}_a$  обозначено среднее число атомов в возбужденном состоянии в рассматриваемый момент времени  $t_1$

$$\bar{N}_a(t_1) = \sum_j \delta(t_1 - t_j) \langle \hat{\sigma}_a^j \rangle$$

Аналогично для коррелятора  $\langle \hat{F}_{ab}(t_1) \hat{F}_{ab}^\dagger(t_2) \rangle$  из (4.30) можно получить следующее соотношение

$$\begin{aligned} \langle \hat{F}_{ab}(t_1) \hat{F}_{ab}^\dagger(t_2) \rangle &= \sum_{ij} \Delta(t_1 - t_i) \Delta(t_2 - t_j) \langle \hat{f}_{ab}^i (\hat{f}_{ab}^j)^\dagger \rangle + \\ &\quad + \sum_{ij} \delta(t_1 - t_i) \delta(t_2 - t_j) \langle \hat{\sigma}_{ab}^j (\hat{\sigma}_{ab}^i)^\dagger \rangle = \\ &= \frac{\gamma}{2} \delta(t_1 - t_2) \sum_j \Delta(t_1 - t_j) \langle \hat{\sigma}_b^j \rangle + \delta(t_1 - t_2) \sum_j \delta(t_1 - t_j) \langle \hat{\sigma}_b^j \rangle = \\ &= \frac{\gamma}{2} \bar{N}_b \delta(t_1 - t_2), \end{aligned} \quad (4.43)$$

где опять же введено среднее число атомов в невозбужденном состоянии:

$$\bar{N}_b(t_1) = \sum_j \delta(t_1 - t_j) \langle \hat{\sigma}_b^j \rangle$$

В дальнейшем будет удобно использовать оператор разности населенностей  $\hat{N}_z = \hat{N}_a - \hat{N}_b$ , для которого из (4.38) и (4.40) получим:

$$\frac{d\hat{N}_z}{dt} = r_a - \gamma \hat{N}_z + 2ig \left( \hat{a}^\dagger \hat{N}_{ab} - \hat{N}_{ab}^\dagger \hat{a} \right) + \hat{F}_z, \quad (4.44)$$

где

$$\hat{F}_z = \hat{F}_a - \hat{F}_b. \quad (4.45)$$

### 4.2.3 Уравнения движения электромагнитного поля

Так же как и в случае атомной подсистемы рассмотрение начнем с уравнений которым удовлетворяют операторы резервуара  $R_A$ :  $\hat{b}_k$ . Так как исследуемые операторы входят только в гамильтониан  $\hat{V}_{FR_F}$  то уравнение движения имеет вид

$$\frac{d\hat{b}_k}{dt} = \frac{i}{\hbar} \left[ \hat{V}_{FR_F}, \hat{b}_k \right]. \quad (4.46)$$

Подставляя в (4.46) выражение для гамильтониана (4.6) получим

$$\begin{aligned} \frac{d\hat{b}_k}{dt} &= \frac{i}{\hbar} [\hat{V}_{FR_F}, \hat{b}_k] = \\ &= \frac{i}{\hbar} \sum_{k',j} g_{k'}^{(F)} [\hat{b}_{k'}^\dagger, \hat{b}_{k'}] \hat{a} e^{i(\omega_{k'}^{(F)} - \omega)t} = -i g_k^{(F)} \hat{a} e^{i(\omega_k^{(F)} - \omega)t}. \end{aligned} \quad (4.47)$$

Формальное интегрирование (4.47) дает нам

$$\hat{b}_k(t) = \hat{b}_k(0) - i g_k^{(F)} \int_0^t dt' \hat{a}(t') e^{i(\omega_k^{(F)} - \omega)t'}. \quad (4.48)$$

Оператор моды электромагнитного поля  $\hat{a}$  присутствует в гамильтонианах  $\hat{V}_{AF}$  и  $\hat{V}_{FR_F}$ , т. о. с учетом выражений для этих гамильтонианов (4.5) и (4.6) и принимая во внимание определение (4.31) имеем

$$\begin{aligned} \frac{d\hat{a}}{dt} &= \frac{i}{\hbar} [\hat{V}_{AF}, \hat{a}] + \frac{i}{\hbar} [\hat{V}_{FR_F}, \hat{a}] = \\ &= \frac{i}{\hbar} \hbar g \sum_j \Delta(t - t_j) [\hat{a}^\dagger, \hat{a}] \hat{\sigma}_{ab}^j + \\ &+ \frac{i}{\hbar} \sum_k g_k^{(F)} [\hat{a}^\dagger, \hat{a}] \hat{b}_k e^{-i(\omega_k^{(F)} - \omega)t} = \\ &= -i g \sum_j \Delta(t - t_j) \hat{\sigma}_{ab}^j - i \sum_k g_k^{(F)} \hat{b}_k e^{-i(\omega_k^{(F)} - \omega)t} = \\ &= -i g \hat{N}_{ab} - i \sum_k g_k^{(F)} \hat{b}_k e^{-i(\omega_k^{(F)} - \omega)t}. \end{aligned} \quad (4.49)$$

Подставив (4.48) в (4.49) получим

$$\begin{aligned} \frac{d\hat{a}}{dt} &= -i g \hat{N}_{ab} - 2\pi D(\omega) \left( g^{(F)}(\omega) \right)^2 \int_0^t dt' \hat{a}(t') \delta(t - t') - \\ &- i \sum_k g_k^{(F)} \hat{b}_k(0) e^{-i(\omega_k^{(F)} - \omega)t}. \end{aligned}$$

Обозначая через

$$\gamma^{(F)} = 4\pi D(\omega) \left( g^{(F)}(\omega) \right)^2 = \frac{\omega}{Q}$$

и вводя шумовой оператор

$$\hat{F}_F(t) = -i \sum_k g_k^{(F)} \hat{b}_k(0) e^{-i(\omega_k^{(F)} - \omega)t} \quad (4.50)$$

окончательно получим

$$\frac{d\hat{a}}{dt} = -\frac{1}{2}\frac{\omega}{Q}\hat{a} - ig\hat{N}_{ab} + \hat{F}_F. \quad (4.51)$$

В силу того, что определение шумового оператора (4.50) совпадает с определением (2.134), то мы можем написать корреляционные соотношения в виде (2.135) и (2.136):

$$\begin{aligned} \langle \hat{F}_F^\dagger(t_1) \hat{F}_F(t_2) \rangle &= \frac{\gamma \bar{n}_T}{2} \delta(t_1 - t_2) = \frac{1}{2} \frac{\omega}{Q} \bar{n}_T \delta(t_1 - t_2), \\ \langle \hat{F}_F(t_1) \hat{F}_F^\dagger(t_2) \rangle &= \frac{1}{2} \frac{\omega}{Q} (\bar{n}_T + 1) \delta(t_1 - t_2), \end{aligned} \quad (4.52)$$

где  $\bar{n}_T$  среднее число фононов в моде резервуара при температуре  $T$ .

### 4.3 Система уравнений Гейзенберга-Ланжевена, описывающая лазер

Объединив полученные нами уравнения (4.51), (4.40) и (4.44) мы можем записать следующую систему:

$$\begin{aligned} \frac{d\hat{a}}{dt} &= -\frac{1}{2}\frac{\omega}{Q}\hat{a} - ig\hat{N}_{ab} + \hat{F}_F, \\ \frac{d\hat{N}_{ab}}{dt} &= -\gamma\hat{N}_{ab} + ig\hat{N}_z\hat{a} + \hat{F}_{ab}, \\ \frac{d\hat{N}_z}{dt} &= r_a - \gamma\hat{N}_z + 2ig\left(\hat{a}^\dagger\hat{N}_{ab} - \hat{N}_{ab}^\dagger\hat{a}\right) + \hat{F}_z, \end{aligned} \quad (4.53)$$

которую мы будем называть системой уравнений Гейзенберга-Ланжевена, описывающих работу лазера.

По своему виду эти уравнения (4.53) очень похожи на уравнения лазера, полученные в полуклассическом приближении. Различие заключается в том, что вместо классических величин в уравнении стоят операторы, которые могут не коммутировать между собой, следовательно при преобразовании нужно соблюдать порядок следования сомножителей. Кроме того, в уравнениях появляются Ланжевенские члены, описывающие квантовые шумы, имеющиеся в лазерной системе.

К уравнениям (4.53) можно применить те же приближения, которые применяются в полуклассическом случае.



Если, как это обычно бывает, можно применить адиабатическое приближение, пренебрегая во втором уравнении (4.53) производной  $\frac{d\hat{N}_{ab}}{dt}$  по сравнению с членом  $\gamma\hat{N}_{ab}$  получим

$$\hat{N}_{ab} = \frac{1}{\gamma} \left( ig\hat{N}_z\hat{a} + \hat{F}_{ab} \right).$$

Подставляя это выражение для  $\hat{N}_{ab}$  в оставшиеся два уравнения системы (4.53) получим новую систему уравнений:

$$\begin{aligned} \frac{d}{dt}\hat{a} &= -\frac{1}{2} \left( \frac{\omega}{Q} \right) \hat{a} + \frac{g^2}{\gamma} \hat{N}_z\hat{a} + \hat{F}_F - i\frac{g}{\gamma} \hat{F}_{ab}, \\ \frac{d}{dt}\hat{N}_z &= r_a - \gamma\hat{N}_z - \frac{4g^2}{\gamma} \hat{N}_z\hat{a}^\dagger\hat{a} + \\ &+ \hat{F}_z + \frac{2ig}{\gamma} \left( \hat{a}^\dagger\hat{F}_{ab} - \hat{F}_{ab}^\dagger\hat{a} \right). \end{aligned} \quad (4.54)$$

Если ввести новое обозначение

$$\hat{F}_\Sigma = - \left( \frac{g}{\gamma} \hat{F}_{ab} + i\hat{F}_F \right), \quad (4.55)$$

то систему (4.54) можно переписать в виде

$$\begin{aligned} \frac{d}{dt}\hat{a} &= -\frac{1}{2} \left( \frac{\omega}{Q} \right) \hat{a} + \frac{g^2}{\gamma} \hat{N}_z\hat{a} + i\hat{F}_\Sigma, \\ \frac{d}{dt}\hat{N}_z &= r_a - \gamma\hat{N}_z - \frac{4g^2}{\gamma} \hat{N}_z\hat{a}^\dagger\hat{a} + \\ &+ \hat{F}_z + \frac{2ig}{\gamma} \left( \hat{a}^\dagger\hat{F}_{ab} - \hat{F}_{ab}^\dagger\hat{a} \right). \end{aligned} \quad (4.56)$$

Для шумового оператора (4.55) при помощи (4.42), (4.43) и (4.52) можно написать следующие корреляционные соотношения:

$$\begin{aligned} \left\langle \hat{F}_\Sigma^\dagger(t_1) \hat{F}_\Sigma(t_2) \right\rangle &= \frac{g^2}{\gamma^2} \left\langle \hat{F}_{ab}^\dagger(t_1) \hat{F}_{ab}(t_2) \right\rangle + \left\langle \hat{F}_F^\dagger(t_1) \hat{F}_F(t_2) \right\rangle = \\ &= \frac{1}{2} \left( \frac{g^2}{\gamma} \bar{N}_a + 2\frac{g^2}{\gamma^2} r_a + \frac{\omega}{Q} \bar{n}_T \right) \delta(t_1 - t_2), \\ \left\langle \hat{F}_\Sigma(t_1) \hat{F}_\Sigma^\dagger(t_2) \right\rangle &= \frac{1}{2} \left( \frac{g^2}{\gamma} \bar{N}_b + \frac{\omega}{Q} (\bar{n}_T + 1) \right) \delta(t_1 - t_2) \end{aligned} \quad (4.57)$$

Уравнения (4.56) напоминают полуклассическое уравнение лазера, и для их решения можно в значительной мере воспользоваться такими же приближениями и приемами которые используются при решении полуклассической задачи.

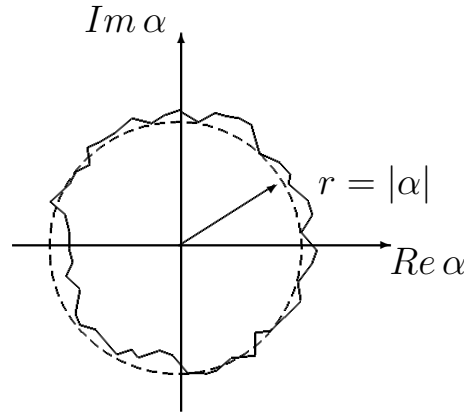


Рис. 4.3: При наличии источников шумового воздействия (Ланжевеновских сил) неопределенность амплитуды занимает узкую область вблизи окружности  $|\alpha| = \text{const}$ , а фаза свободно диффундирует (блуждает) по этой окружности.

## 4.4 Естественная ширина линии излучения

Уравнения (4.56) пригодны для решения многих задач, связанных с квантовой природой лазера: определение статистики лазерных фотонов в различных режимах работы, определение ширины линии излучения и с некоторыми добавлениями для решения более тонких вопросов, например исследование вопроса непосредственной генерации лазером сжатого состояния (подробнее о сжатых состояниях см. гл. 9).

Здесь мы рассмотрим только задачу об естественной ширине линии излучения лазера. Будем рассматривать стационарный режим работы лазера который достаточно удален от порога генерации. В этом случае задачу можно сильно упростить, т. к. ширина линии мало зависит от флуктуация разности населенностей уровней и флуктуаций амплитуды генерируемого излучения, как мы это установили рассматривая эту задачу ранее методом матрицы плотности. Основное влияние на ширину линии оказывает флуктуация (дрейф) фазы. Наглядно это можно представить на плоскости комплексной амплитуды, как это изображено на рис. 4.3.

Если бы не было источников шумового воздействия (Ланжевеновских сил) генерирующее поле имело бы определенную амплитуду и фазу. В реальности, при их наличии неопределенность амплитуды будет занимать узкую область вблизи окружности  $|\alpha| = \text{const}$ , а фаза будет свободно диффундировать (блуждать) по этой окружности.

В связи со сказанным, упрощение уравнений сведется к следующему. Уравнение для населенности заменим усредненным уравнением

$$r_a - \gamma \bar{N}_z - \frac{4g^2}{\gamma} \bar{N}_z \bar{n} = 0, \quad (4.58)$$

где  $\bar{N}_z$  - усредненное значение населенности,  $\bar{n} = \langle \hat{a}^\dagger \hat{a} \rangle$  - среднее число фотонов в генерируемой моде. Ноль справа означает, что рассматривается установившийся режим.

Из (4.58) находим  $\bar{N}_z$

$$\bar{N}_z = \frac{r_a}{\gamma \left( 1 + \left( \frac{2g}{\gamma} \right)^2 \bar{n} \right)} \approx \frac{r_a}{\gamma} \left( 1 - \left( \frac{2g}{\gamma} \right)^2 \bar{n} \right). \quad (4.59)$$

Окончательное значение в (4.59) получено в приближении, что второй член в скобке мал по сравнению с 1 (лазер не на пороге). Подставив этот результат в уравнение для поля получим

$$\begin{aligned} \frac{d}{dt} \hat{a} = & -\frac{1}{2} \left( \frac{\omega}{Q} \right) \hat{a} + r_a \frac{g^2}{\gamma^2} \hat{a} - \\ & - 4r_a \frac{g^4}{\gamma^4} \bar{n} \hat{a} + i\hat{F}_\Sigma, \end{aligned} \quad (4.60)$$

где первый член справа соответствует потерям в резонаторе, второй - усилению активной средой, третий характеризует степень насыщенности уровней.

Корреляционная функция поля, которую нам надо определить выражается следующим равенством

$$I(t, 0) = \langle \hat{a}^\dagger(t) \hat{a}(0) \rangle,$$

где  $\hat{a}(t)$  удовлетворяет уравнению (4.60).

В нашем приближении, когда мы пренебрегаем амплитудными флуктуациями, но не пренебрегаем диффузией фазы, оператор  $\hat{a}$  можно представить в виде

$$\begin{aligned} \hat{a}(t) &= A e^{i\hat{\varphi}(t)}, \\ \hat{a}^\dagger(t) &= A e^{-i\hat{\varphi}(t)}, \end{aligned} \quad (4.61)$$

где  $A$  среднее значение амплитуды, а  $\hat{\varphi}(t)$  - оператор фазы. Тогда корреляционная функция может быть представлена в виде

$$\begin{aligned} \langle \hat{a}^\dagger(t) \hat{a}(0) \rangle &= |A|^2 \langle e^{-i(\hat{\varphi}(t) - \hat{\varphi}(0))} \rangle = \\ &= |A|^2 \langle e^{-\frac{1}{2}(\hat{\varphi}(t) - \hat{\varphi}(0))^2} \rangle. \end{aligned} \quad (4.62)$$

Последнее следует из того, что

$$\langle e^{-i(\Delta\varphi)} \rangle = \langle e^{-\frac{1}{2}(\Delta\varphi)^2} \rangle,$$

где  $\Delta\varphi = \hat{\varphi}(t) - \hat{\varphi}(0)$ , и что можно доказать, разложив экспоненту в ряд и усреднив каждый член ряда, а затем просуммировав результат.

Имеем

$$\Delta\varphi = \int_0^t \frac{d\varphi}{dt} dt,$$

тогда

$$\langle (\Delta\varphi)^2 \rangle = \int_0^t dt_1 \left\langle \frac{d\varphi}{dt} \right\rangle \int_0^t dt_2 \left\langle \frac{d\varphi}{dt} \right\rangle,$$

где  $\frac{d\varphi}{dt}$  можно получить из уравнения (4.60) посредством следующих соотношений

$$\begin{aligned} i \frac{d\varphi}{dt} &= \frac{1}{\hat{a}} \frac{d\hat{a}}{dt} = -\frac{1}{2} \left( \frac{\omega}{Q} \right) + r_a \frac{g^2}{\gamma^2} - \\ &\quad - 4r_a \frac{g^4}{\gamma^4} \bar{n} + i \frac{\hat{F}_\Sigma}{\hat{a}}, \\ -i \frac{d\varphi}{dt} &= \frac{1}{\hat{a}^\dagger} \frac{d\hat{a}^\dagger}{dt} = -\frac{1}{2} \left( \frac{\omega}{Q} \right) + r_a \frac{g^2}{\gamma^2} - \\ &\quad - 4r_a \frac{g^4}{\gamma^4} \bar{n} - i \frac{\hat{F}_\Sigma^\dagger}{\hat{a}^\dagger}, \end{aligned} \quad (4.63)$$

т. о. вычитая второе уравнение (4.63) из первого получим

$$2 \frac{d\varphi}{dt} = \frac{\hat{F}_\Sigma}{\hat{a}} + \frac{\hat{F}_\Sigma^\dagger}{\hat{a}^\dagger}. \quad (4.64)$$

Подставив теперь (4.61) в (4.64) имеем:

$$\frac{d\varphi}{dt} = \frac{1}{2A} \left\{ e^{i\hat{\varphi}(t)} \hat{F}_\Sigma^\dagger(t) + e^{-i\hat{\varphi}(t)} \hat{F}_\Sigma(t) \right\}.$$

Остается вычислить  $\langle (\Delta\varphi)^2 \rangle$ . Это приводит к двойному интегралу

$$\begin{aligned} \langle (\Delta\varphi)^2 \rangle &= \frac{1}{4A^2} \int_0^t dt_1 \int_0^t dt_2 \left\langle \left( e^{i\hat{\varphi}(t_1)} \hat{F}_\Sigma^\dagger(t_1) + e^{-i\hat{\varphi}(t_1)} \hat{F}_\Sigma(t_1) \right) \right. \\ &\quad \left. \left( e^{i\hat{\varphi}(t_2)} \hat{F}_\Sigma^\dagger(t_2) + e^{-i\hat{\varphi}(t_2)} \hat{F}_\Sigma(t_2) \right) \right\rangle = \\ &= \frac{1}{4} \frac{1}{\bar{n}} \int_0^t dt_1 \int_0^t dt_2 \left\langle \hat{F}_\Sigma^\dagger(t_1) \hat{F}_\Sigma(t_2) e^{-i(\hat{\varphi}(t_1) - \hat{\varphi}(t_2))} + \text{э. с.} \right\rangle. \end{aligned}$$

Откуда с помощью (4.57) можно получить

$$\langle (\Delta\varphi)^2 \rangle = \frac{1}{4} \frac{1}{\bar{n}} \left( \frac{g^2}{2\gamma} (\bar{N}_a + \bar{N}_b) + \frac{g^2}{\gamma^2} r_a + \frac{\omega}{Q} \left( \bar{n}_T + \frac{1}{2} \right) \right) t. \quad (4.65)$$

Из уравнений (4.38) и (4.40) можно записать уравнение для  $\bar{N}_a + \bar{N}_b$ :

$$\frac{d(\bar{N}_a + \bar{N}_b)}{dt} = r_a - \gamma(\bar{N}_a + \bar{N}_b),$$

откуда в установившемся режиме:

$$r_a = \gamma(\bar{N}_a + \bar{N}_b).$$

Подставив теперь это соотношение в (4.65) получим:

$$\langle (\Delta\varphi)^2 \rangle = \frac{1}{4} \frac{1}{\bar{n}} \left( \frac{3g^2}{2\gamma} (\bar{N}_a + \bar{N}_b) + \frac{\omega}{Q} \left( \bar{n}_T + \frac{1}{2} \right) \right) t. \quad (4.66)$$

Рассмотрим лазер на пороге:

$$A = R_a \approx \frac{\omega}{Q},$$

подставляя сюда выражение для  $R_a$  (2.70) в котором принимаем  $\tau \approx \frac{1}{\gamma}$ :

$$r_a \frac{g^2}{\gamma^2} \approx \frac{\omega}{Q}.$$

Используя это соотношение из (4.59) имеем:

$$\bar{N}_z \approx \frac{r_a}{\gamma} \approx \frac{\omega}{Q} \frac{\gamma}{g^2},$$

откуда

$$\frac{g^2}{\gamma} \approx \frac{\omega}{Q} \frac{1}{\bar{N}_z}.$$

Таким образом (4.66) перепишется в виде

$$\langle (\Delta\varphi)^2 \rangle = \frac{1}{4} \frac{1}{\bar{n}} \frac{\omega}{Q} \left( \frac{3}{2} \frac{\bar{N}_a + \bar{N}_b}{\bar{N}_z} + \bar{n}_T + \frac{1}{2} \right) t. \quad (4.67)$$

Если теперь в (4.67) принять предположение о полной инверсии:  $\bar{N}_b = 0$ , а также если пренебречь  $\bar{n}_T$  по сравнению с 1, то получим

$$\langle (\Delta\varphi)^2 \rangle \approx \frac{1}{2} \frac{1}{\bar{n}} \frac{\omega}{Q} t. \quad (4.68)$$

Подставив это в (4.62) получим

$$\langle \hat{a}^\dagger(t) \hat{a}(0) \rangle = |A|^2 e^{-\frac{1}{4} \frac{1}{\bar{n}} \frac{\omega}{Q} t}, \quad (4.69)$$

которое совпадает с выражением (3.27), полученным нами ранее, если принять пороговый режим генерации:

$$A \approx \frac{\omega}{Q}.$$

Таким образом выражение для естественной ширины линии будет тем же самым:

$$D \approx \frac{1}{2} \frac{1}{\bar{n}} \frac{\omega}{Q}.$$

## 4.5 Упражнения

1. Доказать коммутационные соотношения (4.13) и (4.23).
2. Получить уравнения движения оператора  $\hat{\sigma}_b^j$ : (4.19) и (4.20).
3. Вывести соотношения (4.40) для операторов  $\hat{N}_b$  и  $\hat{N}_{ab}$ .
4. Доказать второе соотношение (4.30).
5. Доказать (4.62).
6. Доказать (4.65).

## Глава 5

# Оптика фотонов (квантовые явления в оптике)

Мы будем рассматривать те оптические явления, в которых в той или иной степени проявляются квантовые свойства света.

Несмотря на то, что большое число оптических явлений можно рассматривать с классических позиций, многие явления могут быть до конца поняты и описаны только в рамках полностью квантового описания.

Квантовое рассмотрение позволяет более полно понять суть интерференционных опытов и на этой основе понять связь между классическим и квантовым описаниями. Кроме того, квантовый подход позволяет рассматривать эксперименты нового типа, в которых изучается статистика фотонов в световых пучках и ее связь со спектральными свойствами света.

### 5.1 Фотоэффект

Для регистрации фотонов используется фотоэффект, в котором, как известно, при поглощении фотона связанный электрон переходит в свободное состояние и регистрируется соответствующим образом. Одним из приборов, применяемых для этих целей, является фотоумножитель, схематически изображенный на [рис. 5.1](#). Принцип действия его хорошо известен. Могут применяться и полупроводниковые лавинные фотодиоды, снабженные усилителем. Рассмотрим связь скорости фотоэлектронных переходов со световым полем. Оператор электрического поля можно разложить на частотно-положительную и частотно-отрицательную части ([1.88](#)):

$$\hat{E}(\vec{r}, t) = \hat{E}^{(+)}(\vec{r}, t) + \hat{E}^{(-)}(\vec{r}, t), \quad (5.1)$$

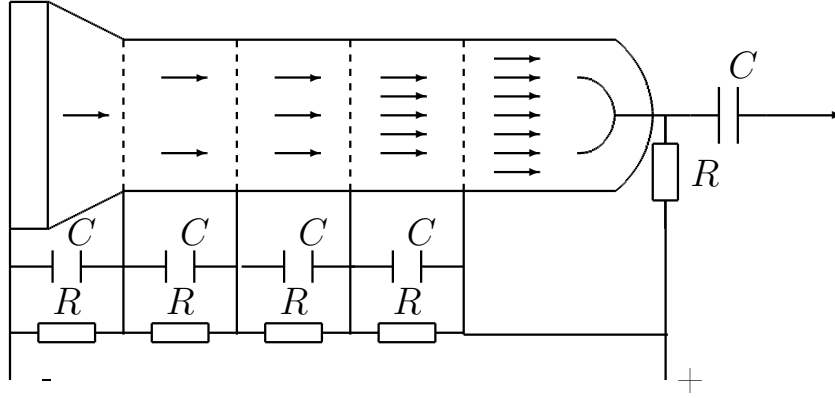


Рис. 5.1: Фотоумножитель

где в частотно-положительную часть входят операторы поглощения, а в частотно-отрицательную - операторы рождения.

При разложении поля по плоским волнам имеем:

$$\begin{aligned}\hat{\vec{E}}^{(+)}(\vec{r}, t) &= \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k \vec{e}_k e^{-i\omega_k t + i(\vec{k}\vec{r})}, \\ \hat{\vec{E}}^{(-)}(\vec{r}, t) &= \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k^\dagger \vec{e}_k^* e^{i\omega_k t - i(\vec{k}\vec{r})}.\end{aligned}\quad (5.2)$$

Рассматриваем приближение электродипольного взаимодействия, то есть считаем, что размеры атома (или другой электронной системы), с которым взаимодействует свет, много меньше длины волны. Гамильтониан взаимодействия в этом случае имеет вид:

$$\hat{\mathcal{H}}_{ED} = -\left(\hat{\vec{p}}\hat{\vec{E}}\right), \quad (5.3)$$

где  $\hat{\vec{p}}$  - оператор дипольного момента системы. Кроме этого мы предполагаем, что учитываются только те процессы, которые сопровождаются уничтожением фотонов. Таким образом в (5.3) надо оставить только операторы уничтожения  $\hat{a}$ , т. е. заменить  $\hat{\vec{E}}$  на  $\hat{\vec{E}}^{(+)}$ :

$$\hat{\mathcal{H}}_{ED} = -\left(\hat{\vec{p}}\hat{\vec{E}}^{(+)}\right). \quad (5.4)$$

Положим, что первоначально атом находится в основном состоянии, а многомодовое поле содержит  $\{n_k\}$  фотонов, то есть начальным вектором состояния является

$$|i\rangle = |\{n_k\}\rangle |b\rangle \quad (5.5)$$



После взаимодействия система атом-поле будет находиться в состоянии  $|f\rangle$  (детализировать его мы не будем). Вероятность перехода в единицу времени в первом порядке теории возмущений в соответствии с золотым правилом Ферми (Теорема 14.9.1) дается квадратом модуля матричного элемента перехода:

$$\begin{aligned} \left| \langle f | \hat{\mathcal{H}}_{ED} | i \rangle \right|^2 &= \langle f | \left( \hat{p} \hat{E}^{(+)} \right) | i \rangle \langle f | \left( \hat{p} \hat{E}^{(+)} \right) | i \rangle^* = \\ &= \langle f | \left( \hat{p} \hat{E}^{(+)} \right) | i \rangle \langle i | \left( \hat{p} \hat{E}^{(-)} \right) | f \rangle = \langle i | \left( \hat{p} \hat{E}^{(-)} \right) | f \rangle \langle f | \left( \hat{p} \hat{E}^{(+)} \right) | i \rangle \end{aligned} \quad (5.6)$$

Конечное состояние неизвестно. Оно может быть любым, и необходимо просуммировать (5.6) по всем конечным состояниям (сложить вероятности). Считаем систему конечных состояний полной, то есть  $\sum_{(f)} |f\rangle \langle f| = \hat{I}$ . Отсюда имеем:

$$\begin{aligned} \sum_{(f)} \langle i | \left( \hat{p} \hat{E}^{(-)} \right) | f \rangle \langle f | \left( \hat{p} \hat{E}^{(+)} \right) | i \rangle &= \langle i | \hat{p}_E^2 \hat{E}^{(-)} \hat{E}^{(+)} | i \rangle = \\ &= \langle \{n_k\} | \hat{E}^{(-)} \hat{E}^{(+)} | \{n_k\} \rangle \langle b | \hat{p}_E^2 | b \rangle = \alpha \langle \{n_k\} | \hat{E}^{(-)} \hat{E}^{(+)} | \{n_k\} \rangle, \end{aligned} \quad (5.7)$$

где  $\hat{p}_E$  - проекция дипольного момента на направление поля,  $\alpha$  - некоторая константа взаимодействия, которая от величины поля не зависит. Обобщим теперь (5.7) на случай смешанного начального состояния. Допустим, что нам известна вероятность  $P_{\{n_k\}}$  состояния  $|\{n_k\}\rangle$ . Матрица плотности этого состояния может быть представлена в виде

$$\hat{\rho} = \sum_{\{n_k\}} P_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}|. \quad (5.8)$$

Для получения результата в случае смешанного состояния нужно усреднить (5.7) при помощи вероятностей  $P_{\{n_k\}}$ . Имеем для скорости фотоотсчетов:

$$\begin{aligned} W &= \alpha \sum_{\{n_k\}} P_{\{n_k\}} \langle \{n_k\} | \hat{E}^{(-)} \hat{E}^{(+)} | \{n_k\} \rangle = \\ &= \alpha Sp \left( \hat{\rho} \hat{E}^{(-)} \hat{E}^{(+)} \right) \end{aligned} \quad (5.9)$$

- в произвольном представлении, так как  $Sp$  не зависит от представления.

Таким образом, в общем случае статистически смешанного состояния средняя скорость счета фотонов пропорциональна ожидаемому значению операторов  $\hat{E}^{(-)} \hat{E}^{(+)}$  в начальном состоянии поля, где  $\hat{\rho}$  - статистический оператор начального состояния поля.

Мы рассмотрели в качестве фотоприемника атом или аналогичную микросистему. Реальный фотоприемник содержит много атомов. Если допустить, что приемник содержит  $N$  невзаимодействующих между собой атомов, а размеры его достаточно малы, чтобы можно было с хорошей точностью считать все атомы находящимися при одинаковых условиях, то в этом случае можно считать, что вероятность (5.9) можно просто увеличить в  $N$  раз.

Выясним, какой смысл имеет оператор  $\hat{E}^{(-)}\hat{E}^{(+)}$ . Введем оператор

$$\hat{\vec{J}} = 2\varepsilon_0 \left( \hat{E}^{(-)}\hat{E}^{(+)} \right) c\vec{k}_0, \quad (5.10)$$

где  $\vec{k}_0$  - единичный вектор направления, в котором распространяется волна; векторный оператор  $\hat{\vec{J}}$  можно рассматривать как оператор потока энергии в направлении  $\vec{k}_0$ . Например, для одномодового поля этот оператор равен

$$\hat{\vec{J}} = \frac{c\hbar\omega_k}{V} \vec{k}_0 \hat{n}_k, \quad (5.11)$$

$\vec{k}_0$  - единичный вектор направления  $\vec{k}$ . Среднее значение оператора  $\hat{\vec{J}}$  в состоянии с определенным числом фотонов равно

$$\langle \hat{\vec{J}} \rangle = \frac{c\hbar\omega_k}{V} n_k \vec{k}_0,$$

В одномодовом смешанном состоянии имеем

$$\langle \hat{\vec{J}} \rangle = \frac{c\hbar\omega_k}{V} \bar{n} \vec{k}_0, \quad \text{где } \bar{n} = \sum_{(n_k)} P_{n_k} n_k.$$

Из приведенных примеров видно, что  $\hat{\vec{J}}$  действительно имеет смысл оператора потока энергии. В одномодовом случае интенсивность не зависит от времени. В многомодовом случае интенсивность может меняться во времени и пространстве. Из всего сказанного можно сделать вывод, что скорость фотоэмиссии пропорциональна среднему потоку фотонов, т. е. интенсивности света. При полуклассическом рассмотрении этому соответствует усредненный за период поток энергии.

## 5.2 Когерентные свойства света

Когерентные свойства света определяют интерференционные явления в оптике, которые хорошо описываются классической волновой теорией. В клас-

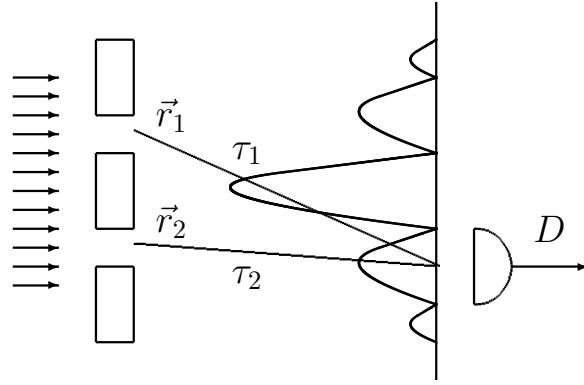


Рис. 5.2: Интерференционный опыт Юнга.  $\vec{r}_{1,2}$  - координаты двух отверстий,  $\tau_{1,2}$  - задержки при распространении света от отверстий к экрану,  $D$  - фотодетектор.

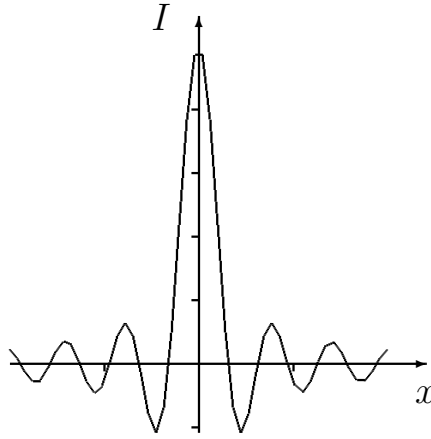


Рис. 5.3: Классическая интерференционная картина. Зависимость интенсивности света  $I$  от координаты на экране  $x$ .

сической волновой оптике когерентные свойства света описываются соответствующими функциями когерентности [59, 50, 60]. Рассмотрим явление интерференции с квантовой точки зрения. Для этого рассмотрим интерференционный опыт Юнга (см. рис. 5.2). На экране (фотопластинке) попадание фотона фиксируется темной точкой. Для того чтобы получить интерференционную картину, сходную с классической, нужно достаточное время. Тогда отдельные точки сольются в полосы и картина ничем не будет отличаться от классической (рис. 5.3).

Операторы поля на экране можно представить в виде суперпозиции полей, прошедших через отверстия 1, 2:

$$\hat{E}^{(+)}(\vec{r}, t) = \gamma \left[ \hat{E}^{(+)}(\vec{r}_1, t_1) + \hat{E}^{(+)}(\vec{r}_2, t_2) \right], \quad (5.12)$$

где  $\vec{r}_1, \vec{r}_2$  - координаты отверстий;  $t_1 = t - \tau_1$ ,  $t_2 = t - \tau_2$ ;  $\tau_1, \tau_2$  - задержка при распространении света от отверстий к экрану; коэффициент  $\gamma$  характеризует ослабление поля при распространении от отверстий к экрану. При помощи

фотодетектора  $D$  исследуем интенсивность света в различных точках экрана.

Скорость счета фотонов будет, как мы знаем, пропорциональна

$$W = \alpha Sp \left( \hat{\rho} \hat{E}^{(-)}(\vec{r}, t) \hat{E}^{(+)}(\vec{r}, t) \right) = \\ \alpha |\gamma|^2 Sp \left[ \hat{\rho} \left( \hat{E}^{(-)}(\vec{r}_1, t_1) + \hat{E}^{(-)}(\vec{r}_2, t_2) \right) \left( \hat{E}^{(+)}(\vec{r}_1, t_1) + \hat{E}^{(+)}(\vec{r}_2, t_2) \right) \right].$$

При почленном перемножении получим:

$$W = g Sp \left[ \hat{\rho} \left( \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_1, t_1) + \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_2, t_2) + \right. \right. \\ \left. \left. + \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) + \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_1, t_1) \right) \right], \quad (5.13)$$

где введено следующее обозначение:  $g = \alpha |\gamma|^2$ .

Первые два члена дают интенсивность полей, прошедших через первое и второе отверстия при закрытом другом отверстии. Два последних члена описывают интерференцию. Так как

$$\left( \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_1, t_1) \right)^\dagger = \left( \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) \right)$$

то  $Sp \left( \hat{\rho} \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_1, t_1) \right)$  и  $Sp \left( \hat{\rho} \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) \right)$  будут комплексно сопряженными величинами. Член

$$Sp \left[ \hat{\rho} \left( \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) + \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_1, t_1) \right) \right]$$

дает интерференционный осциллирующий член (рис. 5.3). Огибающая интерференционного члена пропорциональна выражению

$$\left| Sp \left[ \hat{\rho} \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) \right] \right| \quad (5.14)$$

Отсюда следует определение функции когерентности первого порядка

$$G(\vec{r}_1, t_1, \vec{r}_2, t_2) = G_{12}^1 = \\ = \frac{\left| Sp \left[ \hat{\rho} \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) \right] \right|}{\sqrt{Sp \left[ \hat{\rho} \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_1, t_1) \right] Sp \left[ \hat{\rho} \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_2, t_2) \right]}} \quad (5.15)$$

Это выражение напоминает классическое определение функции когерентности, но здесь вместо аналитического сигнала стоят операторы поля и производится квантовое усреднение при помощи матрицы плотности.

Рассмотрим для примера некоторые частные случаи. Начнем с одномодового поля, находящегося в состояниях  $|n\rangle$  либо  $|\alpha\rangle$ . В этом случае имеем:

$$\begin{aligned}\hat{E}^{(+)}(\vec{r}, t) &= \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k \vec{e}_k e^{-i\omega_k t + i(\vec{k}\vec{r})}, \\ \hat{E}^{(-)}(\vec{r}, t) &= \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k^\dagger \vec{e}_k^* e^{i\omega_k t - i(\vec{k}\vec{r})} = \left( \hat{E}^{(+)}(\vec{r}, t) \right)^\dagger.\end{aligned}\quad (5.16)$$

Используя эти выражения для вычисления функции когерентности (5.15), получим  $G_{12}^1 = 1$ , так как  $\langle n | \hat{a}^\dagger \hat{a} | n \rangle = n$  и  $|e^{-ix}| = 1$ . То же самое получим и для случая когерентного состояния:  $G_{12}^1 = 1$ , так как  $\langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^2$ .

Вообще одномодовое поле, возбуждаемое в произвольное чистое состояние, обладает полной когерентностью первого порядка. Более того, одномодовое поле, возбуждаемое в произвольное статистическое смешанное состояние, имеет полную когерентность. В этом случае нужно вычислить  $Sp(\hat{\rho} \hat{a}^\dagger \hat{a})$ , где  $\hat{\rho} = \sum_{(m)} \sum_{(l)} \rho_{ml} |m\rangle \langle n|$ . Имеем

$$\begin{aligned}Sp(\hat{\rho} \hat{a}^\dagger \hat{a}) &= \sum_{(n)} \sum_{(m)} \sum_{(l)} \rho_{ml} \langle n | m \rangle \langle l | \hat{a}^\dagger \hat{a} | n \rangle = \\ &= \sum_{(n)} \sum_{(l)} \rho_{nl} \langle l | n \rangle n = \sum_{(n)} \rho_{nn} n = \bar{n}.\end{aligned}\quad (5.17)$$

Аналогичное выражение получаем в знаменателе, следовательно,  $G_{12}^{(1)} = 1$ .

Чаще имеют дело с многомодовыми состояниями поля, поэтому рассмотрим когерентность света в этом случае. Рассмотрим два предельных случая: свет, находящийся в когерентном состоянии, и полностью хаотический свет.

В первом случае вектор состояния равен

$$|\{\alpha_k\}\rangle = |\{\alpha_{k_1}\}\rangle |\{\alpha_{k_2}\}\rangle \dots |\{\alpha_{k_s}\}\rangle \dots$$

Используя свойства когерентных состояний

$$\hat{E}^{(+)}(\vec{r}, t) |\{\alpha_k\}\rangle = E(\vec{r}, t) |\{\alpha_k\}\rangle$$

и

$$\langle \{\alpha_k\} | \hat{E}^{(-)}(\vec{r}, t) = E^*(\vec{r}, t) \langle \{\alpha_k\} |,$$

получим:

$$\langle \{\alpha_k\} | \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) | \{\alpha_k\} \rangle = E^*(\vec{r}_1, t_1) E(\vec{r}_2, t_2)$$

где  $E$  - собственное значение оператора  $\hat{E}^{(+)}$ , являющееся аналитическим сигналом классического поля. Отсюда имеем

$$G_{12}^{(1)} = \frac{|E^*(\vec{r}_1, t_1) E(\vec{r}_2, t_2)|}{\sqrt{E^*(\vec{r}_1, t_1) E(\vec{r}_1, t_1) E^*(\vec{r}_2, t_2) E(\vec{r}_2, t_2)}} = 1 \quad (5.18)$$

то есть многомодовое поле, находящееся в когерентном состоянии, полностью когерентно.

В случае произвольного состояния многомодового поля имеем только частичную когерентность. Рассмотрим наиболее часто встречающийся случай хаотического света (излучение нагретого тела, газового разряда и т.п.), когда свет излучается множеством независимых источников (атомов, ионов, молекул). Выражение для матрицы плотности в этом случае имеет вид (1.114):

$$\begin{aligned} \hat{\rho} &= \sum_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| \prod_{\{n_k\}} \frac{\bar{n}_k^{n_k}}{(1 + \bar{n}_k)^{n_k+1}} = \\ &= \sum_{\{n_k\}} \rho_{\{n_k\}, \{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| \end{aligned} \quad (5.19)$$

где

$$\begin{aligned} \rho_{\{n_k\}, \{n_k\}} &= P_{\{n_k\}} = \prod_k \frac{\bar{n}_k^{n_k}}{(1 + \bar{n}_k)^{n_k+1}} = \prod_k P_{n_k}, \\ \sum_{\{n_k\}} \dots &= \sum_{n_1} \sum_{n_2} \dots \sum_{n_k} \dots \end{aligned}$$

Операторы электрического поля равны

$$\begin{aligned} \hat{E}^{(+)} &= \sum_{(k)} \sqrt{\frac{\hbar \omega_k}{2 \varepsilon_0 V}} \vec{e}_k \hat{a}_k e^{-i \omega_k t + i(\vec{k} \vec{r})}, \\ \hat{E}^{(-)} &= \sum_{(k)} \sqrt{\frac{\hbar \omega_k}{2 \varepsilon_0 V}} \vec{e}_k^* \hat{a}_k^\dagger e^{i \omega_k t - i(\vec{k} \vec{r})}, \end{aligned} \quad (5.20)$$

откуда следует:

$$\begin{aligned} &Sp \left( \hat{\rho} \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) \right) = \\ &= \sum_{\{n_{k'}\}} \sum_{\{n_k\}} \langle \{n_{k'}\} | \{n_k\} \rangle P_{\{n_k\}} \langle \{n_k\} | \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) | \{n_{k'}\} \rangle = \\ &= \sum_{\{n_k\}} \langle \{n_k\} | \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) | \{n_k\} \rangle P_{\{n_k\}}. \end{aligned} \quad (5.21)$$

Произведение операторов равно

$$\hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) = \sum_{(k)} \sum_{(k')} \frac{\hbar \sqrt{\omega_k \omega_{k'}}}{2\varepsilon_0 V} (\vec{e}_k \vec{e}_{k'}) \hat{a}_k^\dagger \hat{a}_{k'} e^{-ix_2 + ix_1}, \quad (5.22)$$

где  $x_1 = \omega_k t_1 - (\vec{k} \vec{r}_1)$ ,  $x_2 = \omega_k t_2 - (\vec{k} \vec{r}_2)$ . Усреднению подлежит оператор  $\hat{a}_k^\dagger \hat{a}_{k'}$ . Поскольку

$$|\{n_k\}\rangle = |n_{k_1}\rangle |n_{k_2}\rangle \dots,$$

то

$$\langle \{n_k\} | \hat{a}_k^\dagger \hat{a}_{k'} | \{n_k\} \rangle = n_k \delta_{kk'},$$

и, следовательно,

$$\begin{aligned} Sp \left( \hat{\rho} \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) \right) &= \\ &= \sum_k \sum_{\{n_k\}} \frac{\hbar \omega_k}{2\varepsilon_0 V} n_k e^{-i(x_2 - x_1)} P_{\{n_k\}} = \\ &= \sum_k \frac{\hbar \omega_k}{2\varepsilon_0 V} \sum_{\{n_k\}} n_k \prod_k P_{n_k} = \sum_k \frac{\hbar \omega_k}{2\varepsilon_0 V} \bar{n}_k e^{-i(x_2 - x_1)}, \end{aligned}$$

поскольку

$$\begin{aligned} \sum_{\{n_k\}} n_k \prod_k P_{n_k} &= \sum_{n_1} P_{n_1} \sum_{n_2} P_{n_2} \dots \sum_{n_k} n_k P_{n_k} \dots = \\ &= \sum_{n_k} n_k P_{n_k} = \bar{n}_k, \end{aligned}$$

т. к.

$$\sum_{n_k} P_{n_k} = 1.$$

Отсюда получаем

$$G_{12}^{(1)} = \frac{\left| \sum_k \frac{\hbar \omega_k}{2\varepsilon_0 V} \bar{n}_k e^{-i\omega_k(t_2 - t_1) + i(\vec{k}, \vec{r}_2 - \vec{r}_1)} \right|}{\sum_k \frac{\hbar \omega_k}{2\varepsilon_0 V} \bar{n}_k} \quad (5.23)$$

Суммирование по  $k$  можно заменить интегрированием по частоте. Используя выражение для плотности состояний, получим:

$$\begin{aligned} \sum_k (\dots) &= \frac{L^3}{(2\pi)^3} \int \int \int (\dots) dk_x dk_y dk_z = \\ &= \frac{V}{(2\pi)^3} \int_\Omega d\Omega \int \omega^2 (\dots) d\omega. \end{aligned}$$

Это приводит нас к выражению

$$G_{12}^{(1)} = \frac{\left| \int d\Omega \int \omega^3 \bar{n}(\omega, \Omega) e^{-i\omega(t_2-t_1)+i(\vec{k}, \vec{r}_2-\vec{r}_1)} d\omega \right|}{\int d\Omega \int \omega^3 \bar{n}(\omega, \Omega) d\omega}. \quad (5.24)$$

Если линия узкая по сравнению с несущей частотой, то есть  $\bar{n}(\omega, \Omega)$  имеет узкий пик около частоты  $\sim \omega_0$ , функцию  $\omega^3$  можно вынести из-под интеграла и сократить; кроме того, если световой пучок узкий, то есть область интегрирования по  $\Omega$  мала, выражение (5.24) можно упростить

$$G_{12}^{(1)} = \frac{\left| \int \bar{N}(\omega) e^{-i\omega(t_2-t_1)+i(\vec{k}, \vec{r}_2-\vec{r}_1)} d\omega \right|}{\int \bar{N}(\omega) d\omega}, \quad (5.25)$$

где  $\bar{N}(\omega) = \int_{\Delta\Omega} \bar{n}(\omega, \Omega) d\Omega$ . Например, когда спектральная линия лоренцовская, имеем:

$$\bar{N}(\omega) = \bar{N}_0 \frac{\gamma}{(\omega_0 - \omega)^2 + \gamma^2}.$$

Рассмотренную задачу можно решить, используя представление когерентных состояний. Тогда

$$\hat{\rho} = \int \cdots \int P(\{\alpha_k\}) |\{\alpha_k\}\rangle \langle \{\alpha_k\}| d^2\{\alpha_k\},$$

где

$$P(\{\alpha_k\}) = \prod_k \frac{1}{\pi \bar{n}_k} e^{-\frac{|\alpha_k|^2}{\bar{n}_k}} = \prod_k P_k(\alpha_k).$$

Имеем

$$\begin{aligned} & Sp \left( \hat{\rho} \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) \right) = \\ & = \int \cdots \int P(\{\alpha_k\}) \langle \{\alpha_k\} | \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) | \{\alpha_k\} \rangle d^2\{\alpha_k\}. \end{aligned} \quad (5.26)$$

Произведение операторов равно

$$\hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) = \sum_k \sum_{k'} \frac{\hbar \sqrt{\omega_k \omega_{k'}}}{2\varepsilon_0 V} (\vec{e}_k \vec{e}_{k'}) \hat{a}_k^\dagger \hat{a}_{k'} e^{-ix_2 + ix_1}.$$

Произведение операторов записано у нас в нормальном виде (операторы поглощения стоят у нас справа от операторов рождения), поэтому матричный



элемент, входящий в (5.26), легко записать, заменив  $\hat{a}_{k'} \rightarrow \alpha_{k'}$ ,  $\hat{a}_k^\dagger \rightarrow \alpha_k^*$ . Отсюда имеем

$$\begin{aligned} Sp \left( \hat{\rho} \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) \right) = \\ = \sum_{k \neq k'} \frac{\hbar \sqrt{\omega_k \omega_{k'}}}{2\varepsilon_0 V} (\vec{e}_k \vec{e}_{k'}) e^{-ix_2 + ix_1} \cdot \\ \cdot \int P(\alpha_k) \alpha_k^* d^2 \alpha_k \int P(\alpha_{k'}) \alpha_{k'} d^2 \alpha_{k'} + \\ + \sum_k \frac{\hbar \omega_k}{2\varepsilon_0 V} e^{-ix_2 + ix_1} \int |\alpha_k|^2 d^2 \alpha_k. \end{aligned} \quad (5.27)$$

При выводе (5.27) использовалось следующее соотношение

$$\int P(\alpha_k) d^2 \alpha_k = 1.$$

Далее можно воспользоваться следующими соотношениями

$$\begin{aligned} \int P(\alpha_k) \alpha_k d^2 \alpha_k &= 0, \\ \int |\alpha_k|^2 d^2 \alpha_k &= \bar{n}_k, \end{aligned}$$

которые легко доказать, перейдя к полярным координатам:

$$\alpha = |\alpha| e^{i\theta} = r e^{i\theta}.$$

В результате для (5.27) получим

$$Sp \left( \hat{\rho} \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_2) \right) = \sum_k \frac{\hbar \omega_k}{2\varepsilon_0 V} e^{-ix_2 + ix_1} \bar{n}_k.$$

Воспользовавшись этими результатами, совпадающими с тем, что было получено ранее, используя представление чисел заполнения  $n$ , мы получим те же окончательные выражения (5.24) и (5.25).

### 5.3 Когерентность второго порядка

Когерентность второго порядка может быть введена на основе анализа различных экспериментов, где измеряется скорость одновременной регистра-

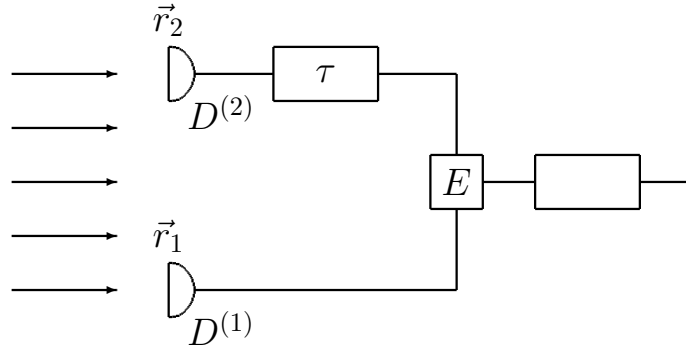


Рис. 5.4: Схема измерения когерентности второго порядка. Два фотодетектора  $D^{(1)}$  и  $D^{(2)}$  находятся в точках пространства, определяемых векторами  $\vec{r}_1$  и  $\vec{r}_2$ . Сигнал с  $D^{(2)}$  пропускается через задержку  $\tau$ , таким образом схема совпадений  $E$  регистрирует одновременное поглощение двух фотонов, одного в точке  $\vec{r}_1$  и в момент времени  $t_1 = t$ , а второго в точке  $\vec{r}_2$  и в момент времени  $t_2 = t - \tau$ .

ции фотонов двумя детекторами. Анализ приводит к следующему определению степени когерентности второго порядка:

$$G^{(2)}(\vec{r}_1, t_1, \vec{r}_2, t_2) = G_{12}^{(2)} = \frac{\langle \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) \rangle}{\langle \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_1, t_1) \rangle \langle \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(+)}(\vec{r}_2, t_2) \rangle}. \quad (5.28)$$

Угловые скобки означают квантово-механическое усреднение по ансамблю при помощи статистического оператора (матрицы плотности)

$$\langle (\dots) \rangle = Sp \{ \hat{\rho} (\dots) \}$$

Выражение (5.28) напоминает классическое выражение, определяющее когерентность второго порядка, однако в нем на месте классических полей стоят операторы, а усреднение производится при помощи матрицы плотности.

Формулу (5.28) можно обосновать следующим образом. Рассмотрим оператор  $\hat{E}^{(+)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2)$ . Он соответствует поглощению одного фотона в точке  $\vec{r}_1$  и в момент времени  $t_1 = t$  и второго фотона в точке  $\vec{r}_2$  в момент времени  $t_2 = t - \tau$ . Реализовать такую процедуру можно при помощи схемы, изображенной на рис. 5.4. Точки  $\vec{r}_1$  и  $\vec{r}_2$  определяются положением фотоприемников. Времена  $t_1 = t$  и  $t_2 = t - \tau$  определяются совпадением фотоотсчетов.  $\tau$  - регулируемая задержка. Результат с двух детекторов подается на схему совпадений.

Применим к оператору  $\hat{E}^{(+)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2)$  процедуру, которую мы применяли при рассмотрении фотоэффекта. Вероятность регистрации первого фотона во время  $t_1 = t$ , а второго во время  $t_2 = t - \tau$  в интервале  $\Delta t$  равна

$$w(\vec{r}_1, \vec{r}_2, t_1, t_2) \Delta t = \alpha \left| \langle f | \hat{E}^{(+)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) | i \rangle \right|^2 \Delta t,$$

где  $|i\rangle$  начальное состояние системы,  $|f\rangle$  конечное состояние системы,  $\alpha$  - величина, зависящая от свойств фотодетекторов. Тогда скорость счета (число отсчетов в единицу времени) после суммирования по конечным состояниям определяется формулой

$$w(\vec{r}_1, \vec{r}_2, t_1, t_2) = \alpha \langle i | \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) | i \rangle.$$

Здесь нас интересует только полевая часть, атомная часть выражается коэффициентом  $\alpha$ .

Если начальное поле находится в статистически смешанном состоянии, то усреднение надо проводить при помощи статистического оператора начального поля. Тогда будем иметь

$$w(\vec{r}_1, \vec{r}_2, t_1, t_2) = \alpha Sp \left\{ \hat{\rho} \hat{E}^{(-)}(\vec{r}_2, t_2) \hat{E}^{(-)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_1, t_1) \hat{E}^{(+)}(\vec{r}_2, t_2) \right\}.$$

При помощи этого выражения для нормированной степени когерентности получим формулу (5.28).

Приведем некоторые примеры вычисления степени когерентности второго порядка. Начнем с простого. Найдем когерентность второго порядка для одномодового состояния с определенным числом фотонов. Для этого нужно рассмотреть матричный элемент

$$\langle n | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} | n \rangle = n(n-1).$$

Это выражение будет стоять в числителе. В знаменателе будем иметь

$$(\langle n | \hat{a}^\dagger \hat{a} | n \rangle)^2 = n^2.$$

Числовые коэффициенты в числителе и знаменателе сокращаются. Получаем:

$$\begin{aligned} G_{12}^{(2)} &= \frac{n(n-1)}{n^2} = \frac{n-1}{n} \text{ для } n > 2, \\ G_{12}^{(2)} &= 0 \text{ для } n = 1, \\ G_{12}^{(2)} &\text{ не определено для } n = 0. \end{aligned} \tag{5.29}$$

Стоит отметить очевидный факт в (5.29): если у нас имеется один фотон то вероятность зарегистрировать 2 фотона равняется 0, что приводит к  $G_{12}^{(2)} = 0$  при  $n = 1$ .

Рассмотрим еще один простой случай: одномодовое поле в когерентном состоянии. Имеем

$$\begin{aligned} \langle \alpha | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} | \alpha \rangle &= (\alpha^* \alpha)^2 \text{ - в числителе,} \\ (\langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle)^2 &= (\alpha^* \alpha)^2 \text{ - в знаменателе.} \end{aligned}$$

Все вместе дает

$$G_{12}^{(2)} = 1.$$

До сих пор мы рассматривали когерентность чистых состояний. Перейдем к рассмотрению смешанных состояний. Рассмотрим одномодовый хаотический свет, матрица плотности которого равна

$$\hat{\rho} = \sum_n \frac{\bar{n}^n}{(\bar{n} + 1)^{n+1}} |n\rangle \langle n| = \sum_n \rho_{nn} |n\rangle \langle n|.$$

Отсюда получим

$$\begin{aligned} Sp \{ \hat{\rho} \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \} &= \sum_n \sum_m \langle n | m \rangle \langle m | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} | m \rangle \rho_{mm} = \\ &= \sum_n \rho_{nn} (n - 1) n = \bar{n}^2 - \bar{n}. \end{aligned} \quad (5.30)$$

Для хаотического света имеет место соотношение

$$\bar{n}^2 = 2 (\bar{n})^2 + \bar{n}. \quad (5.31)$$

Действительно

$$\begin{aligned} \bar{n}^2 &= \sum_n n^2 \frac{\bar{n}^n}{(\bar{n} + 1)^{n+1}} = \frac{\bar{n}}{(\bar{n} + 1)} \sum_n n^2 \frac{\bar{n}^{n-1}}{(\bar{n} + 1)^n} = \\ &= \frac{\bar{n}}{(\bar{n} + 1)} \sum_{m=n-1} (m + 1)^2 \frac{\bar{n}^m}{(\bar{n} + 1)^{m+1}} = \\ &= \frac{\bar{n}}{(\bar{n} + 1)} \sum_m (m^2 + 2m + 1) \frac{\bar{n}^m}{(\bar{n} + 1)^{m+1}} = \\ &= \frac{\bar{n}}{(\bar{n} + 1)} (\bar{n}^2 + 2\bar{n} + 1), \end{aligned}$$

таким образом получим

$$\bar{n}^2 (\bar{n} + 1) = \bar{n} (\bar{n}^2 + 2\bar{n} + 1)$$

откуда и следует искомое выражение (5.31):

$$\bar{n}^2 = 2(\bar{n})^2 + \bar{n}.$$

Таким образом из (5.30) и (5.31) имеем

$$Sp\{\dots\} = 2(\bar{n})^2$$

В знаменателе имеем  $(\bar{n})^2$ . Отсюда получаем, что для хаотического света

$$G_{12}^{(2)} = 2, \quad (5.32)$$

из чего следует, что пары фотонов регистрируются чаще, чем это наблюдается при более упорядоченном свете. Физически это связано с флуктуациями хаотического света. В связи с этим иногда говорят о склонности фотонов к группировке. Вообще же для произвольного одномодового поля когерентность второго порядка равна

$$G^{(2)} = \frac{\bar{n}^2 - \bar{n}}{(\bar{n})^2}. \quad (5.33)$$

Более подробно мы рассмотрим этот вопрос в третьей части данной книги (см. гл. 8 Неклассический свет).

На практике чаще имеют дело с многомодовыми полями. Определим степень когерентности второго порядка в двух предельных случаях: многомодового когерентного состояния и многомодового хаотического света. Первый случай рассматривается просто. Вектор состояния в этом случае можно представить в виде

$$|\{\alpha_k\}\rangle = |\{\alpha_{k_1}\}\rangle |\{\alpha_{k_2}\}\rangle \dots |\{\alpha_{k_s}\}\rangle \dots \quad (5.34)$$

Используя равенства

$$\hat{E}^{(+)}(x) |\{\alpha_k\}\rangle = E(x) |\{\alpha_k\}\rangle$$

и

$$\langle\{\alpha_k\}|\hat{E}^{(-)}(x) = \langle\{\alpha_k\}|E^*(x),$$

где  $x = (t, r)$ ,  $E(x)$  - аналитический сигнал (частотно-положительная часть) классического поля, получаемого из оператора  $\hat{E}^{(+)}$  заменой  $\hat{a}_k \rightarrow \alpha_k$ . Отсюда получим:

$$\begin{aligned} \langle\{\alpha_k\}|\hat{E}^{(-)}(x_2)\hat{E}^{(-)}(x_1)\hat{E}^{(+)}(x_1)\hat{E}^{(+)}(x_2)|\{\alpha_k\}\rangle = \\ = E^*(x_2)E^*(x_1)E(x_1)E(x_2). \end{aligned}$$

Таким же образом убеждаемся, что в знаменателе будет стоять величина  $E^*(x_1) E(x_1) E^*(x_2) E(x_2)$ . Следовательно, в этом случае

$$G_{12}^{(2)} = 1, \quad (5.35)$$

Сложнее рассмотреть случай хаотического многомодового светового поля. В этом случае статистический оператор будет иметь вид (1.114)

$$\begin{aligned} \hat{\rho} &= \sum_{\{n_k\}} P_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| = \sum_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| \prod_{\{n_k\}} \frac{\bar{n}_k^{n_k}}{(1 + \bar{n}_k)^{n_k+1}} = \\ &= \sum_{\{n_k\}} |\{n_k\}\rangle \langle \{n_k\}| \prod_{\{n_k\}} P_{\{n_k\}}. \end{aligned} \quad (5.36)$$

При перемножении операторов электрического поля получим четырехкратную сумму, так как  $\hat{E}^{(+)}$  и  $\hat{E}^{(-)}$  выражаются в виде разложений по плоским волнам:

$$\begin{aligned} \hat{E}^{(+)}(\vec{r}, t) &= \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \vec{e}_k \hat{a}_k e^{-i\omega_k t + i(\vec{k}\vec{r})}, \\ \hat{E}^{(-)}(\vec{r}, t) &= \sum_{(k)} \sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \vec{e}_k^* \hat{a}_k^\dagger e^{i\omega_k t - i(\vec{k}\vec{r})}. \end{aligned} \quad (5.37)$$

Общий член произведения сумм (5.37) будет содержать произведения операторов вида

$$\hat{a}_{kI}^\dagger \hat{a}_{kII}^\dagger \hat{a}_{kIII} \hat{a}_{kIV}. \quad (5.38)$$

Усреднение этого члена при помощи статистического оператора (5.36) приводит к выражению

$$Sp \left( \hat{\rho} \hat{a}_{kI}^\dagger \hat{a}_{kII}^\dagger \hat{a}_{kIII} \hat{a}_{kIV} \right) = \sum_{\{n_k\}} P_{\{n_k\}} \langle \{n_k\} | \hat{a}_{kI}^\dagger \hat{a}_{kII}^\dagger \hat{a}_{kIII} \hat{a}_{kIV} | \{n_k\} \rangle.$$

Легко увидеть, что члены, в которых все моды разные:

$$k^I \neq k^{II} \neq k^{III} \neq k^{IV},$$

будут равны нулю. Отличными от нуля будут только те члены, для которых выполняются условия:

$$k^I = k^{III} = k_1, \quad k^{II} = k^{IV} = k_2$$

или

$$k^I = k^{IV} = k_1, \quad k^{II} = k^{III} = k_2$$

или

$$k^I = k^{II} = k^{III} = k^{IV} = k.$$

Имеем: в первом случае -

$$\sum_{n_{k_1}} \sum_{n_{k_2}} P_{n_{k_1}} P_{n_{k_2}} n_{k_1} n_{k_2} = \bar{n}_{k_1} \bar{n}_{k_2}, \quad (5.39)$$

во втором -

$$\sum_{n_{k_1}} \sum_{n_{k_2}} P_{n_{k_1}} P_{n_{k_2}} n_{k_1} n_{k_2} = \bar{n}_{k_1} \bar{n}_{k_2}. \quad (5.40)$$

Последний случай был нами рассмотрен выше (5.33), что дает

$$\sum_{n_k} P_{n_k} \langle n_k | \hat{a}_k^\dagger \hat{a}_k^\dagger \hat{a}_k \hat{a}_k | n_k \rangle = 2 (\bar{n}_k)^2. \quad (5.41)$$

Все изложенное выше позволяет написать выражение для функции когерентности в виде

$$\begin{aligned} G_{12}^{(2)} = & \frac{\sum_{k_1} \sum_{k_2 \neq k_1} \bar{n}_{k_1} \bar{n}_{k_2} \omega_{k_1} \omega_{k_2} e^{i\omega_{k_1} \tau} e^{-i\omega_{k_2} \tau}}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} + \\ & + \frac{2 \sum_k \bar{n}_k^2 \omega_k^2}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} + \\ & + \frac{\sum_{k_1} \sum_{k_2 \neq k_1} \bar{n}_{k_1} \bar{n}_{k_2} \omega_{k_1} \omega_{k_2}}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} \end{aligned} \quad (5.42)$$

где обозначено

$$\omega \tau = \omega (t_2 - t_1) - \left( \vec{k}, \vec{r}_2 - \vec{r}_1 \right) = \omega \left[ (t_2 - t_1) - \frac{1}{c} \left( \vec{k}_0, \vec{r}_2 - \vec{r}_1 \right) \right],$$

если мы имеем узкий световой пучок, в котором все моды распространяются примерно в одном направлении.

Половину средней суммы  $2 \sum_k \bar{n}_k^2 \omega_k^2$  можно объединить с левой суммой, а

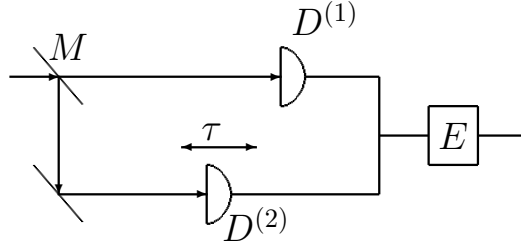


Рис. 5.5: Эксперимент по наблюдению когерентности второго порядка. При помощи 50% зеркала  $M$  световой пучок направляется на два фотоприемника  $D^{(1)}$  и  $D^{(2)}$ . Регулируемая задержка  $\tau$  осуществляется перемещением фотодетектора  $D^{(2)}$ .

вторую половину - с правой. Получим:

$$\begin{aligned}
 G_{12}^{(2)} &= \frac{\sum_{k_1} \sum_{k_2} \bar{n}_{k_1} \bar{n}_{k_2} \omega_{k_1} \omega_{k_2} e^{i\omega_{k_1} \tau} e^{-i\omega_{k_2} \tau}}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} + \\
 &\quad + \frac{\sum_{k_1} \sum_{k_2} \bar{n}_{k_1} \bar{n}_{k_2} \omega_{k_1} \omega_{k_2}}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} = \\
 &= \frac{\sum_{k_1} \bar{n}_{k_1} \omega_{k_1} e^{i\omega_{k_1} \tau} \sum_{k_2} \bar{n}_{k_2} \omega_{k_2} e^{-i\omega_{k_2} \tau} + \left( \sum_{(k)} \bar{n}_k \omega_k \right)^2}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} = \\
 &= \frac{\left| \sum_{(k)} \bar{n}_k \omega_k e^{i\omega_k \tau} \right|^2 + \left( \sum_{(k)} \bar{n}_k \omega_k \right)^2}{\left( \sum_{(k)} \bar{n}_k \omega_k \right)^2} = \left( G_{12}^{(1)} \right)^2 + 1, \quad (5.43)
 \end{aligned}$$

где  $G_{12}^{(1)}$  - функция когерентности первого порядка.

Получен важный результат: когерентность второго порядка для хаотического света выражается через когерентность первого порядка. На этом факте основана так называемая интерферометрия интенсивности. Впервые такое наблюдалось в опытах Хенбери Брауна и Твисса, схема которых изображена на [рис. 5.5](#).

Как видно из [рис. 5.5](#), при помощи 50% зеркала световой пучок направляется на два фотоприемника. Задержка осуществляется перемещением одного из фотодетекторов. Схема совпадений фиксирует регистрацию двух фотонов с заданной задержкой во времени.

На [рис. 5.6](#) изображена зависимость числа совпадений от задержки. В классическом случае схема эксперимента остается прежней, только схема совпадений заменяется коррелятором. Результат эксперимента и в этом случае имеет вид рисунка [5.6](#).



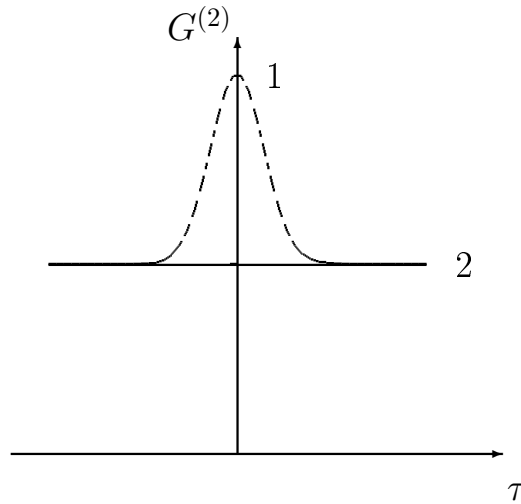


Рис. 5.6: Зависимость когерентности второго порядка  $G^{(2)}$  от задержки  $\tau$ . График 1 описывает случай хаотического света. График 2 описывает когерентное состояние (идеальный лазер).

В этих экспериментах измерялась корреляция интенсивностей, то есть функция когерентности второго порядка. Используя связь между функциями корреляций разного порядка, можно вычислить функцию первого порядка, а затем, используя связь между корреляционной функцией и энергетическим спектром (теорема Хинчина-Винера), определить спектр излучения. Таким образом, “считая фотоны”, можно косвенно производить спектральные измерения. Этим сейчас широко пользуются. Как будет видно из дальнейшего, такая процедура позволяет производить измерение спектров хаотического света с высоким разрешением, дополняя традиционные методы спектральных измерений (при помощи спектральных приборов типа дифракционных решеток, призм и т.п.).

Выражение (5.43) можно также получить, используя представление когерентных состояний. В этом случае

$$\hat{\rho} = \int \cdots \int P(\{\alpha_k\}) |\{\alpha_k\}\rangle \langle \{\alpha_k\}| d^2 \{\alpha_k\},$$

где

$$P(\{\alpha_k\}) = \prod_k \frac{1}{\pi \bar{n}_k} e^{-\frac{|\alpha_k|^2}{\bar{n}_k}} = \prod_k P_k(\alpha_k).$$

Усреднению подлежит произведение операторов

$$\hat{a}_{kI}^\dagger \hat{a}_{kII}^\dagger \hat{a}_{kIII} \hat{a}_{kIV}.$$

Это приводит к интегралу

$$\begin{aligned} & Sp \left\{ \hat{\rho} \hat{a}_{k^I}^\dagger \hat{a}_{k^{II}}^\dagger \hat{a}_{k^{III}} \hat{a}_{k^{IV}} \right\} = \\ & = \int \cdots \int d^2 \{ \alpha_k \}, P(\{ \alpha_k \}) (\alpha_{k^I}^* \alpha_{k^{II}}^* \alpha_{k^{III}} \alpha_{k^{IV}}). \end{aligned}$$

По-прежнему отличными от нуля будут члены с парными произведениями, удовлетворяющими условиям

$$k^I = k^{III} = k_1, \quad k^{II} = k^{IV} = k_2$$

или

$$k^I = k^{IV} = k_1, \quad k^{II} = k^{III} = k_2$$

а также

$$k^I = k^{II} = k^{III} = k^{IV} = k.$$

Как легко показать, интегрируя в полярных координатах  $\alpha = r e^{i\theta}$ , не равные нулю интегралы будут иметь вид:

$$\int d^2 \alpha_{k_1} P(\alpha_{k_1}) \alpha_{k_1}^* \alpha_{k_1} \int d^2 \alpha_{k_2} P(\alpha_{k_2}) \alpha_{k_2}^* \alpha_{k_2} = \bar{n}_{k_1} \bar{n}_{k_2}.$$

В третьем случае с учетом

$$P(\alpha_k) = \frac{1}{\pi \bar{n}_k} e^{-\frac{r^2}{\bar{n}_k}}$$

имеем

$$\begin{aligned} \int d^2 \alpha_k P(\alpha_k) (\alpha_k^* \alpha_k)^2 &= \int_0^\infty r dr \int_0^{2\pi} P(\alpha_k) r^4 d\theta = \\ &= \frac{2\pi}{\pi \bar{n}_k} \int_0^\infty r^4 r dr e^{-\frac{r^2}{\bar{n}_k}} = \bar{n}_k^2 \int_0^\infty x^2 dx e^{-x} = 2 \bar{n}_k^2. \end{aligned}$$

Здесь сделана замена  $x = \frac{r^2}{\bar{n}_k}$ ,  $dx = \frac{2r dr}{\bar{n}_k}$ . Таким образом у нас получились те же результаты, которые были получены ранее. Поэтому окончательный результат (5.43) не изменится.

## 5.4 Когерентность высших порядков

Функции когерентности первого и второго порядков являются частными, хотя и важнейшими случаями функций когерентности. Функцию когерент-

ности  $n$ -ого порядка в квантовом случае определяют следующим образом

$$G^{(n)}(x_1, x_2, \dots, x_n) = \frac{\langle \hat{E}^{(-)}(x_1) \hat{E}^{(-)}(x_2) \dots \hat{E}^{(-)}(x_n) \hat{E}^{(+)}(x_n) \hat{E}^{(+)}(x_{n-1}) \dots \hat{E}^{(+)}(x_1) \rangle}{\langle \hat{E}^{(-)}(x_1) \hat{E}^{(+)}(x_1) \rangle \dots \langle \hat{E}^{(-)}(x_n) \hat{E}^{(+)}(x_n) \rangle}. \quad (5.44)$$

Угловые скобки означают квантово-механическое усреднение при помощи статистического оператора (матрицы плотности),  $x$  - означает совокупность переменных  $t, \vec{r}$ . Степень когерентности  $n$ -ого порядка определяет скорость счета в эксперименте, где каким-либо образом регистрируется  $n$  фотонов.

## 5.5 Счет и статистика фотонов

Мы убедились, что квантование оптического поля и существование квантов света (фотонов) сохраняет общую картину интерференционных явлений, если наблюдение проводится достаточно долго, для того чтобы проявилась усредненная картина. В наших формулах это соответствует усреднению при помощи матрицы плотности. Однако существование фотонов дает возможность проведения экспериментов нового типа, основанных на счете фотонов, и исследования их статистических закономерностей. Эти методы называются методами счета фотонов. Суть их в следующем: исследуемый свет подается на фотодетектор, соединенный со счетчиком, считающим число фотоэлектронов, зафиксированных за определенное время. Затвор перед фотодетектором (или блокировка схемы) контролирует продолжительность счета. При счетчике, установленном на нуль, затвор открывается на время  $T$ , и регистрируется число фотоэлектронов. Через время, большее, чем время корреляции  $\tau_c$ , все повторяется снова много раз. По результатам измерений можно определить  $P_m(T)$  - вероятность зарегистрировать  $m$  отсчетов фотоэлектронов за время  $T$ :

$$P_m(T) = \frac{N_m}{N}, \quad (5.45)$$

где  $N_m$  - число измерений, в которых зафиксировано  $m$  фотоэлектронов,  $N$  - полное число измерений, которое должно быть велико. Очевидно, предполагается, что световой поток стационарен. Полученное распределение содержит информацию о спектральных свойствах световых пучков. Первой здесь является задача, как по статистике фотоотсчетов, которую мы можем измерить, найти статистику фотонов, нужную нам для получения сведений о свойствах световых пучков.

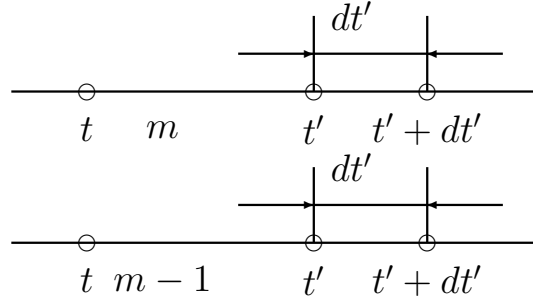


Рис. 5.7: К выводу  $P_m(t, t' + dt')$ . Существуют две возможности получения  $m$  отсчетов в интервале времени  $t, t' + dt'$ : в интервале  $t, t'$  произведено  $m$  отсчетов, а в интервале  $dt$  - ни одного; в интервале  $t, t'$  произведено  $m - 1$  отсчетов, а в интервале  $dt'$  - один.

## 5.6 Связь статистики фотонов со статистикой фотоотсчетов

Начнем с полуклассического рассмотрения, а затем обобщим результаты на полностью квантовое рассмотрение. Мы видели, что скорость фотоэмиссии пропорциональна интенсивности светового потока, которая определяется средним значением оператора  $\langle \hat{E}^{(-)} \hat{E}^{(+)} \rangle$ . Поскольку квантово-механическая интенсивность аналогична в классическом случае усредненной за период интенсивности  $I(t)$ , скорость эмиссии электронов можно в полуклассическом приближении считать пропорциональной  $I(t)$ . Обозначим  $P(t) dt$  - вероятность появления фотоэлектрона в промежутке времени  $t, t + dt$ .  $P(t) dt = \xi I(t) dt$ , где  $\xi$  характеризует эффективность фотокатода. Обозначим вероятность зафиксировать  $m$  фотоотсчетов в интервале времени  $t, t' + dt'$  через  $P_m(t, t' + dt')$ . Существуют две возможности получения  $m$  отсчетов в заданном интервале времени, изображенные на рис. 5.7:

1. в интервале  $t, t'$  произведено  $m$  отсчетов, а в интервале  $dt$  - ни одного
2. в интервале  $t, t'$  произведено  $m - 1$  отсчетов, а в интервале  $dt'$  - один.

Заметим: интервал настолько мал, что вероятности двух и более отсчетов пренебрежимо малы. Для этих двух случаев можем написать

$$\begin{aligned} P_m^{(1)}(t, t' + dt') &= P_m(t, t') (1 - P(t') dt'), \\ P_m^{(2)}(t, t' + dt') &= P_{m-1}(t, t') P(t') dt', \end{aligned} \quad (5.46)$$

где  $P(t) dt = \xi I(t) dt$ . Полная вероятность будет суммой вероятностей этих двух событий:

$$\begin{aligned} P_m(t, t' + dt') &= P_m(t, t') (1 - P(t') dt') + \\ &+ P_{m-1}(t, t') P(t') dt'. \end{aligned} \quad (5.47)$$

Отсюда получаем рекуррентную цепочку дифференциальных уравнений

$$\frac{dP_m}{dt'} = \xi I(t') \{P_{m-1}(t') - P_m(t')\}, \quad (5.48)$$

которую можно решить, интегрируя последовательно, начиная с  $m = 0$ . Начальное уравнение имеет вид:

$$\frac{dP_0}{dt'} = -\xi I(t') P_0(t'), \quad (5.49)$$

при очевидных начальных условиях  $P_0(t') = 1$  при  $t' = t$ . Решение уравнения при этих начальных условиях равно

$$P_0(t, T) = e^{-\xi \int_t^{t+T} I(t') dt'}, \quad (5.50)$$

где  $T$  - время счета. Если ввести среднюю за время счета интенсивность

$$\bar{I}(t, T) = \frac{1}{T} \int_t^{t+T} I(t') dt',$$

равенство (5.50) можно переписать следующим образом:

$$P_0(t, T) = e^{-\xi \bar{I} T} \quad (5.51)$$

Остальные вероятности можно последовательно выразить через  $P_0(t, T)$ . Методом индукции легко показать, что

$$P_m(t, T) = \frac{(\xi \bar{I} T)^m}{m!} e^{-\xi \bar{I} T} \quad (5.52)$$

В справедливости этого решения можно убедиться, подставив его в исходное уравнение (5.48). Вообще же интенсивность  $\bar{I}(t, T)$  флуктуирует от одного периода счета к другому. Для того чтобы это учесть, нужно произвести усреднение по ансамблю измерений. Результатом будет формула Манделя:

$$P_m(T) = \langle P_m(t, T) \rangle = \left\langle \frac{(\xi \bar{I}(t, T) T)^m}{m!} e^{-\xi \bar{I}(t, T) T} \right\rangle. \quad (5.53)$$

Иначе эту формулу можно представить в следующем виде:

$$P_m(T) = \langle P_m(t, T) \rangle = \int_0^\infty P(\bar{I}) \frac{(\xi \bar{I} T)^m}{m!} e^{-\xi \bar{I} T} d\bar{I}. \quad (5.54)$$

где  $P(\bar{I})$  плотность вероятности для  $\bar{I}$ .

## 5.7 Распределение фотоотсчетов для когерентного и хаотического света

Для того чтобы получить представление, как связаны между собой статистика фотоотсчетов и статистика падающего на фотодетектор света, применим формулу (5.54) к двум предельным случаям: постоянного по амплитуде (интенсивности) света и хаотического света с флуктуирующей интенсивностью. Начнем с наиболее простого случая, когда интенсивность падающего света постоянна. В этом случае  $\bar{I}(t, T)$  не зависит от  $t$  и  $T$ ,  $\bar{I}(t, T) = I_0 = \text{const}$ , поэтому второе усреднение не нужно. То же самое получим, если в (5.54) будем считать  $P(\bar{I}) = \delta(\bar{I} - I_0)$ . Окончательное выражение для случая постоянного по интенсивности света имеет вид:

$$P_m = \frac{\bar{m}^m}{m!} e^{-\bar{m}}. \quad (5.55)$$

где  $\bar{m} = \xi I_0 T$  - среднее число фотоотсчетов, регистрируемых фотодетектором за время  $T$ . Таким образом, для постоянной интенсивности распределение фотоотсчетов является распределением Пуассона. Заметим, что при достаточно большом  $T$  (значительно большем времени корреляции  $\tau_c$ ),  $\bar{I}(t, T)$  в любом случае<sup>1</sup> будет стремиться к постоянной величине, а распределение фотоотсчетов - к распределению Пуассона.

В другом предельном случае, когда  $T \ll \tau_c$ , можно считать  $\bar{I}(t, T) = I(t)$  - мгновенной интенсивности. В случае хаотического света  $P(I) = \frac{1}{I} e^{-\frac{1}{I}}$  [57]. По формуле Манделя имеем:

$$\begin{aligned} P_m(T) &= \frac{1}{\bar{I}} \int_0^\infty e^{-\frac{I}{\bar{I}}} \frac{(\xi I T)^m}{m!} e^{-\xi I T} dI = \\ &= \int_0^\infty \frac{y^m (\bar{I} \xi T)^m}{m! (1 + \bar{m})^{m+1}} e^{-y} dy. \end{aligned} \quad (5.56)$$

Здесь сделана замена переменных:

$$y = I \left( \frac{1}{\bar{I}} + \xi T \right),$$

$$I = \frac{y \bar{I}}{1 + \xi \bar{I} T},$$

$$\bar{m} = \xi \bar{I} T.$$

---

<sup>1</sup> в том числе для хаотического света

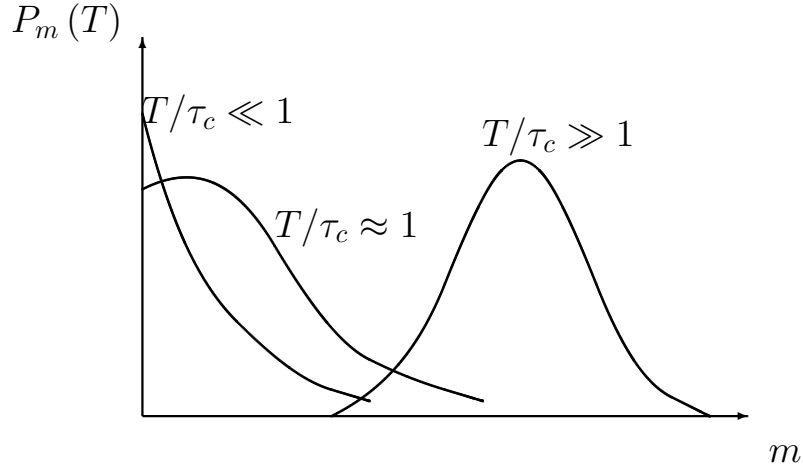


Рис. 5.8: Качественный вид распределения фотоотсчетов  $P_m(T)$  для трех значений  $T/\tau_c$ .

Окончательно получаем

$$P_m(T) = \frac{\bar{m}^m}{(1 + \bar{m})^{m+1} m!} \int_0^\infty y^m e^{-y} dy = \frac{\bar{m}^m}{(1 + \bar{m})^{m+1}} \quad (5.57)$$

так как

$$\int_0^\infty y^m e^{-y} dy = m!.$$

Мы получили, что распределение фотоотсчетов повторяет распределение фотонов для хаотического поля, но с измененным масштабом. Значительно сложнее определить распределение фотоотсчетов для времени счета  $T$ , соответствующего промежуточному случаю  $T \approx \tau_c$ . Здесь возможны только численные расчеты. Результаты таких расчетов приведены на [рис. 5.8](#) [57]. Они позволяют судить о характере изменения распределения фотоотсчетов при увеличении отношения  $T/\tau_c$ . Из графиков видно, что характер распределения меняется вблизи  $T = \tau_c$ . Это позволяет, проводя измерения при различных  $T$ , оценить  $\tau_c$  и ширину спектра падающего света  $\sim 1/\tau_c$ .

## 5.8 Определение статистики фотонов через распределение фотоотсчетов

Обычно основной интерес представляет статистика фотонов, которая характеризует световой пучок. Чтобы ее определить по измеренным  $P_m(T)$ , следует обратиться (5.54), выразив  $P(\bar{I})$  через  $P_m(T)$ .

Существует несколько способов нахождения  $P(\bar{I})$ . (О способах обраще-

ния см. [42].) Остановимся на одном из них. Рассмотрим выражение (5.54)

$$P_m(T) = \int_0^\infty P(\bar{I}) \frac{(\xi \bar{I} T)^m}{m!} e^{-\xi \bar{I} T} d\bar{I}.$$

Из этого равенства по измеренным  $P_m(T)$  нужно определить плотность вероятности  $P(\bar{I})$ , характеризующую статистику падающего света.

Перейдем к новой переменной  $u = \xi \bar{I} T$  и определим новую плотность вероятности

$$P(u) = \frac{1}{\xi T} P(\bar{I}).$$

Имеем:

$$P_T(u) du = \frac{1}{\xi T} P(\bar{I}) \xi T d\bar{I} = P(\bar{I}) d\bar{I}.$$

Отсюда:

$$\int_0^\infty P_T(u) du = \int_0^\infty P(\bar{I}) d\bar{I} = 1,$$

как и должно быть. Запишем уравнение (5.54) в этих переменных

$$P_m(T) = \int_0^\infty P_T(u) \frac{u^m}{m!} e^{-u} du. \quad (5.58)$$

Далее используем ортогональные полиномы Лагерра

$$L_n(y) = \sum_{k=0}^n \binom{n}{k} \frac{(-y)^k}{k!},$$

$$\binom{n}{k} = C_k^n = \frac{n!}{k!(n-k)!} \quad (5.59)$$

удовлетворяющие условиям ортогональности

$$\int_0^\infty L_p(y) L_q(y) e^{-y} dy = \delta_{pq}, \quad (5.60)$$

которым заменой переменных  $y \rightarrow 2y$  можно придать вид

$$2 \int_0^\infty L_p(2y) L_q(2y) e^{-2y} dy = \delta_{pq}. \quad (5.61)$$

Разложим теперь  $P_T(u)$  в ряд по полиномам Лагерра:

$$P_T(u) = \sum_{n=0}^{\infty} A_n L_n(2u) e^{-u} \quad (5.62)$$



Используя условия ортогональности (5.61), получим для коэффициентов разложения  $A_n$  выражение

$$A_n = 2 \int_0^\infty L_n(2u) P_T(u) e^{-u} du. \quad (5.63)$$

Подставим в (5.63)  $L_n(2u)$  в виде ряда (5.59). Получим:

$$\begin{aligned} A_n &= 2 \sum_{k=0}^{k=n} \binom{n}{k} (-2)^k \int_0^\infty P_T(y) \frac{y^k}{k!} e^{-y} dy = \\ &= 2 \sum_{k=0}^{k=n} \binom{n}{k} (-2)^k P_k(T), \end{aligned} \quad (5.64)$$

где использовано выражение

$$\int_0^\infty P(y) \frac{y^k}{k!} e^{-y} dy = P_k(T).$$

Будем считать, что из измерений нам известно достаточное число значений  $P_k(T)$ . Это позволит вычислить достаточное количество коэффициентов разложения  $A_n$  по формуле (5.64). Подставляя их в ряд (5.62) для  $P_T(u)$  и переходя к исходным переменным, получим

$$P(\bar{I}) = \xi T \sum_{k=0}^{\infty} A_n L_n(2\xi T \bar{I}) e^{-\xi T \bar{I}}. \quad (5.65)$$

При помощи этого выражения в принципе можно обратить формулу Манделя. Трудность здесь связана с тем, что нам известно только конечное число  $P_n(T)$  с ограниченной точностью.

## 5.9 Квантовое выражение для распределения фотоотсчетов

Полученное выше выражение для распределения фотоотсчетов основано на полуклассическом подходе. Полностью квантовое выражение имеет вид [57]:

$$P_m(T) = Sp \left\{ \hat{\rho}^{\hat{N}} \left[ \frac{(\beta \hat{I}(t) T)^m}{m!} e^{-\beta \hat{I}(t) T} \right] \right\} \quad (5.66)$$

где

$$\begin{aligned}\hat{I}(t) &= \frac{1}{T} \int_t^{t+T} 2\varepsilon_0 c \hat{E}^{(-)}(t') \hat{E}^{(+)}(t') dt' = \\ &= \frac{2}{T} \int_t^{t+T} \sqrt{\frac{\varepsilon_0}{\mu_0}} \hat{E}^{(-)}(t') \hat{E}^{(+)}(t') dt'\end{aligned}$$

соответствует усредненному за период счета оператору потока энергии,  $\beta$  - квантовая эффективность фотоприемника. Формула (5.66) по виду очень похожа на формулу Манделя. Отличие в том, что на месте классических полей стоят их операторы, усреднение проводится квантово-механически при помощи статистического оператора, и присутствует оператор нормального упорядочения  $\hat{N}$ . Действие этого оператора сводится к тому, что в операторе, на который он действует, следует расположить операторы поглощения справа от операторов рождения. При разложении оператора, входящего в (5.66), в степенной ряд появятся члены вида  $\left(\hat{E}^{(-)}\hat{E}^{(+)}\right)^n$ . Действие на них оператора  $\hat{N}$  определяется выражением

$$\hat{N} \left(\hat{E}^{(-)}\hat{E}^{(+)}\right)^n = \left(\hat{E}^{(-)}\right)^n \left(\hat{E}^{(+)}\right)^n$$

Подобные члены соответствуют когерентности высших порядков, то есть распределение фотоотсчетов зависит от когерентностей всех степеней. Формула (5.66) может быть обоснована следующим образом: положим, что поле находится в когерентном состоянии  $|\{\alpha_k\}\rangle$ . Тогда вероятность эмиссии электрона в интервале времени  $dt$  равна

$$Pdt = \sigma \langle \{\alpha_k\} | \hat{E}^{(-)}\hat{E}^{(+)} | \{\alpha_k\} \rangle dt = \sigma (E^* E) dt,$$

где  $\sigma$  характеризует эффективность фотокатода, а  $E$  - классическое поле, соответствующее состоянию  $|\{\alpha_k\}\rangle$

$$\begin{aligned}\hat{E}^{(+)} |\{\alpha_k\}\rangle &= E |\{\alpha_k\}\rangle, \\ \langle \{\alpha_k\} | \hat{E}^{(-)} &= E^* \langle \{\alpha_k\} |.\end{aligned}$$

Далее рассмотрение ведется таким же образом, как и при полуклассическом подходе. Получается аналогичная формула:

$$P_m(T | \{\alpha_k\}) = \frac{(\sigma \overline{E^* E} T)^m}{m!} e^{-\sigma T \overline{E^* E}} \quad (5.67)$$

где

$$\overline{E^* E} = \frac{1}{T} \int_t^{t+T} E^*(t') E(t') dt'.$$

Это выражение можно представить в операторном виде:

$$P_m(T|\{\alpha_k\}) = \langle \{\alpha_k\} | \hat{N} \left\{ \frac{(\sigma \overline{\hat{E}^{(-)}} \hat{E}^{(+)} T)^m}{m!} e^{-\sigma T \overline{\hat{E}^{(-)}} \hat{E}^{(+)}} \right\} | \{\alpha_k\} \rangle, \quad (5.68)$$

где  $P_m(T|\{\alpha_k\})$  - вероятность счета  $m$  фотоэлектронов за время  $T$ , если поле находится в состоянии  $|\{\alpha_k\}\rangle$ . Оператор, стоящий в фигурных скобках, можно рассматривать как оператор счета  $m$  фотоэлектронов за время  $T$ . Если поле находится в статистически смешанном состоянии со статистическим оператором, определяемым в диагональном представлении функцией  $P_m(T|\{\alpha_k\})$

$$\hat{\rho} = \int_{\{\alpha_k\}} P(\{\alpha_k\}) |\{\alpha_k\}\rangle \langle \{\alpha_k\}| \prod_k d^2 \alpha_k,$$

среднее значение оператора, входящего в выражение (5.68), согласно (1.122), будет равно

$$P_m(T) = \int_{\{\alpha_k\}} P(\{\alpha_k\}) \langle \{\alpha_k\} | \cdot \hat{N} \left\{ \frac{(\sigma \overline{\hat{E}^{(-)}} \hat{E}^{(+)} T)^m}{m!} e^{-\sigma T \overline{\hat{E}^{(-)}} \hat{E}^{(+)}} | \{\alpha_k\} \rangle \right\} \prod_k d^2 \alpha_k \quad (5.69)$$

Полученную формулу можно записать в произвольном представлении, так как операция  $Sp$  не зависит от представления. Имеем

$$P_m = Sp \left( \hat{\rho} \hat{N} \left\{ \frac{(\sigma \overline{\hat{E}^{(-)}} \hat{E}^{(+)} T)^m}{m!} e^{-\sigma T \overline{\hat{E}^{(-)}} \hat{E}^{(+)}} \right\} \right), \quad (5.70)$$

где

$$\overline{\hat{E}^{(-)}} \hat{E}^{(+)} = \frac{1}{T} \int_t^{t+T} \hat{E}^{(-)}(t') \hat{E}^{(+)}(t') dt'.$$

Формула (5.70) полностью соответствует формуле (5.66), взятой из [57]. Расчеты по формуле (5.70) несколько сложнее, чем по формуле Манделя. Для примера рассмотрим несколько простейших случаев. Сперва рассмотрим одномодовые состояния. Тогда (5.70) можно представить в следующем виде

$$P_m = Sp \left( \hat{\rho} \hat{N} \left\{ \frac{(\gamma \overline{\hat{a}^\dagger} \hat{a} T)^m}{m!} e^{-\gamma T \overline{\hat{a}^\dagger} \hat{a}} \right\} \right)$$

где  $\gamma$  - коэффициент, характеризующий в этой записи эффективность фото-  
катада. Оператор

$$\hat{N} \left\{ \frac{(\gamma \hat{a}^\dagger \hat{a} T)^m}{m!} e^{-\gamma T \hat{a}^\dagger \hat{a}} \right\}$$

имеет в представлении чисел заполнения (чисел фотонов) только диагональ-  
ные члены. Тогда  $Sp(\dots)$  будет определяться только диагональными элемен-  
тами матрицы плотности, которые обозначим  $P_n = \langle n | \hat{\rho} | n \rangle$ .

Тогда (5.70) можно представить в виде:

$$\begin{aligned} P_m &= \sum_n P_n \langle n | \hat{N} \frac{(\gamma \hat{a}^\dagger \hat{a} T)^m}{m!} e^{-\gamma T \hat{a}^\dagger \hat{a}} | n \rangle = \\ &= \sum_n P_n \frac{(\gamma T)^m}{m!} \langle n | \sum_l (-1)^l \frac{(\gamma T)^l}{l!} (\hat{a}^\dagger)^{l+m} (\hat{a})^{l+m} | n \rangle = \\ &= \sum_{n=m} P_n \frac{(\gamma T)^m}{m!} \sum_{l=0}^{n-m} (-1)^l \frac{(\gamma T)^l}{l!} \frac{n!}{(n-m-l)!}, \end{aligned} \quad (5.71)$$

что следует из соотношения:

$$\begin{aligned} \langle n | (\hat{a}^\dagger)^{l+m} (\hat{a})^{l+m} | n \rangle &= \\ &= \{n(n-1)(n-2)\dots(n-m-l+1)\} = \frac{n!}{(n-m-l)!}. \end{aligned}$$

Выражение (5.71) можно подвергнуть дальнейшим преобразованиям. Извест-  
но разложение (бином Ньютона):

$$(1 - \gamma T)^{n-m} = \sum_{l=0}^{n-m} (-1)^l (\gamma T)^l \frac{(n-m)!}{l! (n-m-l)!}.$$

Отсюда имеем:

$$P_m(T) = \sum_{n=m}^{\infty} P_n \frac{n!}{m! (n-m)!} (\gamma T)^m (1 - \gamma T)^{n-m}. \quad (5.72)$$

Заметим, что, как известно из теории вероятности (см. распределение Бер-  
нулли), общий член суммы определяет вероятность того, что из  $n$  фотонов  
 $m$  будет зарегистрировано, а  $n-m$  останутся незарегистрированными. При-  
меним общую формулу (5.71) к случаю хаотического света. Тогда

$$P_n = \frac{\bar{n}^n}{(\bar{n} + 1)^{n+1}},$$

и из (5.71) получим

$$\begin{aligned} P_m(T) &= \sum_{n=m}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} (\gamma T)^m (1-\gamma T)^{n-m} \frac{n!}{m!(n-m)!} = \\ &= (\gamma T)^m \sum_{l=0}^{\infty} \frac{\bar{n}^{l+m}}{(\bar{n}+1)^{l+m+1}} (1-\gamma T)^l \frac{(l+m)!}{m!l!}. \end{aligned} \quad (5.73)$$

При преобразовании сделана замена индексов суммирования:  $l = n - m$ ,  $n = l + m$ .

Известно разложение [42]:

$$(1-x)^{-(m+l)} = \sum_{l=0}^{\infty} \frac{x^l (m+l)!}{m!l!}.$$

Используя его, получим:

$$\begin{aligned} P_m(T) &= \frac{(\gamma T \bar{n})^m}{(1+\bar{n})^{m+1}} \left(1 - \frac{\bar{n}}{1+\bar{n}} (1-\gamma T)\right)^{-(m+1)} = \\ &= \frac{(\gamma T \bar{n})^m}{(1+\bar{n})^{m+1}} \left\{ \frac{1-\gamma T \bar{n}}{1+\bar{n}} \right\}^{-(m+1)} = \frac{(\gamma T \bar{n})^m}{(1+\gamma T \bar{n})^{m+1}} = \frac{\bar{m}^m}{(\bar{m}+1)^{m+1}}, \end{aligned} \quad (5.74)$$

где  $\bar{m} = \gamma T \bar{n}$ . Мы получили такой же результат, как и при полуклассическом рассмотрении. Распределение  $P_m(T)$  повторяет  $P_n$ , но в другом масштабе. Вместо  $\bar{n}$  стоит  $\bar{m} = \gamma T \bar{n}$ . Рассмотрим теперь другой предельный случай: поле находится в когерентном состоянии. Его удобно рассматривать в представлении когерентных состояний. Имеем

$$\begin{aligned} P_m(T) &= \langle \alpha | \hat{N} \frac{(\gamma \hat{a}^\dagger \hat{a} T)^m}{m!} e^{-\gamma T \hat{a}^\dagger \hat{a}} | \alpha \rangle = \\ &= \frac{(\gamma |\alpha|^2 T)^m}{m!} e^{-\gamma |\alpha|^2 T} = \frac{\bar{m}^m}{m!} e^{-\bar{m}}, \end{aligned} \quad (5.75)$$

где  $\bar{m} = \gamma |\alpha|^2 T = \gamma \bar{n} T$ .

Распределение фотонов для когерентного состояния, как известно (1.95), равно

$$P_n = \frac{\bar{n}^n e^{-\bar{n}}}{n!}.$$

Таким образом, и в этом случае распределение фотоотсчетов повторяет распределение фотонов, но в другом масштабе. Вместо  $\bar{n}$  стоит  $\bar{m}$ . В общем

случае такой простой связи не будет. Из проведенного нами вывода квантовой формулы фотоотсчетов следует, что пока  $P(\{\alpha_k\})$  в выражении для статистического оператора можно интерпретировать как распределение вероятности, расхождения результатов полуклассического рассмотрения (формулы Манделя), и полностью квантового рассмотрения не будет. Если же  $P(\{\alpha_k\})$  в некоторых областях может быть отрицательно, результаты будут различаться.

## 5.10 Эксперименты по счету фотонов. Применение техники счета фотонов для спектральных измерений

Мы видели, что распределение фотоотсчетов зависит от времени счета  $T$ . Когда время счета сравнивается со временем корреляции, характер распределения меняется, на кривой появляется максимум. При дальнейшем увеличении времени счета характер кривой сохраняется, и при больших временах счета распределение будет стремиться к распределению Пуассона. Следовательно, измеряя  $P_m(T)$  при различных  $T$ , можно оценить  $\tau_c$  и ширину спектра светового пучка  $\sim 1/\tau_c$ . Подобные методы, когда из экспериментов по счету фотонов определяют спектральные параметры света, называют спектроскопией флуктуаций интенсивности. Минимальное время отсчета определяется разрешением фотодетектора, которое порядка  $10^{-8} - 10^{-9}$  сек, что соответствует частоте  $10^8 \nabla \cdot 10^9$  Гц. Эта верхняя граница частотных изменений метода. Нижняя граница определяется максимальным временем счета, которое обычно равно 1 сек, что соответствует разрешению 1 Гц.

Таким образом, методом счета фотонов можно исследовать интервал частот от 1 Гц до  $10^8$  Гц. Следовательно, этот метод дополняет обычную спектроскопию, которая работает в интервале частот от  $10^7$  Гц до  $10^{15}$  Гц. Более удобно использовать эксперименты по счету фотонов другого типа. В них измеряется корреляция между числами фотонов  $m_1$  и  $m_2$ , то есть  $\langle m_1 m_2 \rangle$ , зарегистрированных в двух коротких интервалах времени  $\Delta t_1 = \Delta t_2 = \Delta t$ , задержанных один относительно другого на время  $\tau$ . Оба интервала имеют одинаковую длительность  $\Delta t$ , меньшую, чем  $\tau$ , и время корреляции  $\tau_c$ . В этом случае измеряется когерентность второго порядка, определяемая по формуле

$$G_{12}^{(2)} = \frac{\langle m_1 m_2 \rangle}{(\bar{m})^2} = 1 + \left( G_{12}^{(1)} \right)^2$$

где  $\bar{m}$  - среднее число отсчетов за время  $\Delta t$ .

Зная  $G_{12}^{(2)}$  для хаотического света, можно вычислить функцию когерентности первого порядка

$$G_{12}^{(1)} = \sqrt{G_{12}^{(2)} - 1}$$

и связанную с ней преобразованием Фурье форму и ширину спектральной линии светового пучка. Для хаотического света с лоренцевской спектральной линией имеем:

$$\langle m_1 m_2 \rangle = \bar{m}^2 \left( e^{-2\gamma|\tau|} + 1 \right), \quad (5.76)$$

а для доплеровской линии -

$$\langle m_1 m_2 \rangle = \bar{m}^2 \left( e^{-\delta^2 \tau^2} + 1 \right). \quad (5.77)$$

Здесь  $\delta$  и  $\gamma$  определяют ширину линий в этих случаях. Измерив эти параметры в эксперименте, можно определить спектральную ширину линий.

## 5.11 Упражнения

1. Показать, что формула (5.52) действительно дает решение задачи.
2. Получить из формулы (5.56) выражение (5.57).
3. Получить формулу (5.74), используя представление когерентных состояний.
4. Доказать условия ортогональности для полиномов Лагерра (5.60) и (5.61).
5. Разложить  $P_T(u)$  в ряд по полиномам Лагерра: (5.62)-(5.63)





## Глава 6

# Квантовое описание оптических интерференционных экспериментов

### 6.1 Общие соображения

В квантовой оптике, как и в классической оптике, одним из основных приборов, применяемых для исследования оптических полей (света), является интерферометр.

В квантовой физике прибор описывается, исходя из представлений классической физики, а квантовый объект, взаимодействующий с прибором, описывают квантовыми уравнениями.

Граница между прибором и квантовым объектом несколько условна и может быть выбрана в зависимости от задачи, которую предстоит решить.

В квантовой оптике сам интерферометр описывается классическими уравнениями, так же как в классической оптике. Световое поле описывается квантовыми уравнениями для операторов поля, при этом обычно используют представление Гейзенберга.

Важнейшим элементом любого интерферометра является зеркало. В соответствии со сказанным выше, мы рассматриваем зеркало как часть прибора и описываем его классически, введя в рассмотрение коэффициенты отражения  $r$ ,  $r'$  и коэффициенты прохождения  $t$ ,  $t'$  см. [рис. 6.1](#). На рисунке показаны коэффициенты  $r$ ,  $t$  и  $r'$ ,  $t'$  относящиеся к разным сторонам зеркала. Показаны также операторы уничтожения двух входных мод поля  $\hat{a}_0$  и  $\hat{a}_1$  и два оператора выходных мод  $\hat{a}_2$  и  $\hat{a}_3$

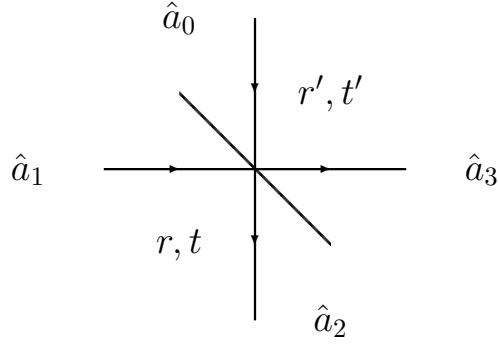


Рис. 6.1: Модель зеркала,  $\hat{a}_0, \hat{a}_1$  - операторы уничтожения входных мод поля,  $\hat{a}_2, \hat{a}_3$  - операторы уничтожения выходных мод поля,  $r, r', t$  и  $t'$  - коэффициенты отражения и прохождения с разных сторон зеркала.

Если зеркало без потерь, то “матрица рассеяния” унитарная, как и в классическом случае:

$$\hat{S} = \begin{bmatrix} t' & r \\ r' & t \end{bmatrix},$$

где  $r, t$  и  $r', t'$  - коэффициенты прохождения и отражения с разных сторон зеркала.

Условие унитарности записывается в следующем виде

$$\begin{aligned} \hat{S}^{-1} &= \hat{S}^\dagger = \begin{bmatrix} t'^* & r'^* \\ r^* & t^* \end{bmatrix}, \\ \hat{S}\hat{S}^\dagger &= \begin{bmatrix} t' & r \\ r' & t \end{bmatrix} \begin{bmatrix} t'^* & r'^* \\ r^* & t^* \end{bmatrix} = \\ &= \begin{bmatrix} |t'|^2 + |r|^2 & t'r'^* + rt^* \\ r't'^* + tr^* & |r'|^2 + |t|^2 \end{bmatrix} = \hat{I}, \\ \hat{S}^\dagger\hat{S} &= \begin{bmatrix} t'^* & r'^* \\ r^* & t^* \end{bmatrix} \begin{bmatrix} t' & r \\ r' & t \end{bmatrix} = \\ &= \begin{bmatrix} |t'|^2 + |r'|^2 & t'^*r + r'^*t \\ r^*t' + t^*r' & |r|^2 + |t|^2 \end{bmatrix} = \hat{I} \end{aligned} \quad (6.1)$$

Для того чтобы выполнялось условие унитарности (6.1), необходимо выполнение закона сохранения энергии и теоремы взаимности. Это приводит к некоторым условиям, которым должны удовлетворять коэффициенты  $r, r', t$  и  $t'$ :

$$\begin{aligned} |r| &= |r'|, \quad |t| = |t'|, \\ |r|^2 + |t|^2 &= 1, \\ r't'^* + tr^* &= 0, \\ t'r^* + r't'^* &= 0. \end{aligned} \quad (6.2)$$

Стоит отметить, что последнее выражение не является независимым, действительно, полагая  $t \neq 0$  (в противном случае можно рассмотреть соотношение для коэффициентов отражения) из соотношения  $|t| = |t'|$  можно получить  $tt^* = t't'^*$  откуда

$$t^* = \frac{t't'^*}{t}.$$

Следовательно, привлекая  $r't'^* + tr^* = 0$ , имеем

$$\begin{aligned} t'r^* + r't^* &= t'r^* + r'\frac{t't'^*}{t} = \\ &= \frac{t'}{t}(tr^* + r't'^*) = 0. \end{aligned}$$

Плоскость отсчета фазы можно в небольших пределах смещать относительно плоскости зеркала, тем более что реальное зеркало не является бесконечно тонким. Плоскость отсчета в ряде случаев можно перемещать на расстояние порядка длины волны. Выбором плоскости отсчета можно перевести матрицу рассеяния к более простому виду, при этом условия (6.2) автоматически выполняются. Предполагая  $t = t' = Te^{i\theta}$  и  $r = r' = Re^{i\phi}$  из (6.2) получим

$$tr^* + r't^* = TRe^{i\theta}e^{-i\phi} + TRe^{i\phi}e^{-i\theta} = e^{i(\phi-\theta)}TR(e^{-2i(\phi-\theta)} + 1) = 0,$$

т.е.  $\phi - \theta = \frac{\pi}{2}$ . Полагая  $\theta = 0$  и переназначая  $t = T, r = R$  имеем

$$\hat{S} = \begin{pmatrix} t & ir \\ ir & t \end{pmatrix}. \quad (6.3)$$

Если принять  $t, t', r, r' \in \mathbb{R}$ , то очевидно, что необходимые условия также будут выполнены при  $t' = t$  и  $r' = -r$ :

$$\hat{S} = \begin{pmatrix} t & r \\ -r & t \end{pmatrix}. \quad (6.4)$$

В уравнениях (6.3) и (6.4) коэффициенты  $r$  и  $t$  вещественны и положительны.

В выражении (6.3) фаза коэффициента отражения сдвинута на  $\frac{\pi}{2}$  относительно фазы коэффициента прохождения. Во втором варианте (6.4) все коэффициенты вещественны, но коэффициенты отражения с разных сторон имеют разные знаки. Поскольку выбором плоскости отсчета можно общий случай привести либо к (6.3) либо к (6.4), то мы в дальнейшем будем пользоваться одним из этих выражений.

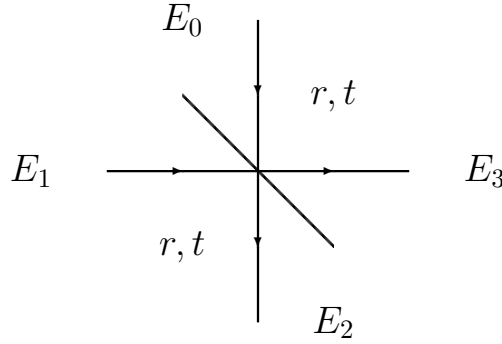


Рис. 6.2: Симметричный делитель. Классический случай.  $E_0, E_1$  - два входных пучка света,  $E_2, E_3$  - поля на выходе, операторы уничтожения выходных мод поля,  $r$  и  $t$  - коэффициенты отражения и прохождения.

**Пример 6.1.1** (Симметричный делитель. Классический случай). *Допустим, что наш делитель симметричный, т. е.  $r = r'$  и  $t = t'$  (см. рис. 6.2) Очевидно, что должен выполняться закон сохранения энергии:*

$$|E_0|^2 + |E_1|^2 = |E_2|^2 + |E_3|^2,$$

или же

$$\begin{aligned} |E_0|^2 + |E_1|^2 &= |tE_0 + rE_1|^2 + |rE_0 + tE_1|^2 = \\ &= \left(|t|^2 + |r|^2\right) \left(|E_0|^2 + |E_1|^2\right) + \\ &+ E_0 E_1^* (tr^* + rt^*) + E_1 E_0^* (tr^* + rt^*) \end{aligned}$$

Т. е.

$$\begin{aligned} |t|^2 + |r|^2 &= 1, \\ tr^* + rt^* &= 0 \end{aligned} \tag{6.5}$$

Последнее равенство будет справедливо если фаза  $t$  и  $r$  различается на  $\frac{\pi}{2}$ , в частности если принять  $t = |t|$ ,  $r = i|r|$ , что соответствует выражению (6.3).

Кроме того выражения (6.5) соответствуют (6.1), действительно

$$\begin{aligned} \hat{S}\hat{S}^\dagger &= \begin{pmatrix} t & r \\ r & t \end{pmatrix} \begin{pmatrix} t^* & r^* \\ r^* & t^* \end{pmatrix} = \\ &= \begin{pmatrix} |t|^2 + |r|^2 & tr^* + rt^* \\ t^*r + r^*t & |t|^2 + |r|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \hat{I}. \end{aligned}$$

Таким образом условие унитарности (6.1) представляет собой закон сохранения энергии.

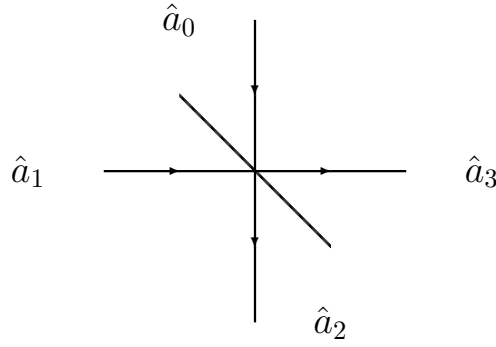


Рис. 6.3: Модель зеркала. Операторы  $\hat{a}_0$  и  $\hat{a}_1$  - операторы падающего поля, относящиеся к двум разным модам (нулевой и первой). Операторы прошедшего поля  $\hat{a}_2$  и  $\hat{a}_3$  (вторая и третья моды).

## 6.2 Операторные соотношения

Будем рассматривать падающее и прошедшее поля как двухмерные см. [рис. 6.3](#). Операторы  $\hat{a}_0$  и  $\hat{a}_1$  - операторы падающего поля, относящиеся к двум разным модам (нулевой и первой). Операторы прошедшего поля  $\hat{a}_2$  и  $\hat{a}_3$  (вторая и третья моды). Естественно, что операторы должны удовлетворять коммутационным соотношениям:

$$\begin{aligned} [\hat{a}_0, \hat{a}_0^\dagger] &= [\hat{a}_1, \hat{a}_1^\dagger] = [\hat{a}_2, \hat{a}_2^\dagger] = [\hat{a}_3, \hat{a}_3^\dagger] = 1, \\ [\hat{a}_0, \hat{a}_1^\dagger] &= [\hat{a}_2, \hat{a}_3^\dagger] = 0. \end{aligned} \quad (6.6)$$

Связь между модами возникает при отражении от зеркала и прохождении через него. Она описывается следующими уравнениями:

$$\begin{aligned} \hat{a}_2 &= t' \hat{a}_0 + r \hat{a}_1, \\ \hat{a}_3 &= r' \hat{a}_0 + t \hat{a}_1. \end{aligned} \quad (6.7)$$

Падающее и прошедшее поля должны удовлетворять коммутационным соотношениям (6.6), откуда имеем с учетом (6.2)

$$\begin{aligned} [\hat{a}_2, \hat{a}_2^\dagger] &= [t' \hat{a}_0 + r \hat{a}_1, t'^* \hat{a}_0^\dagger + r^* \hat{a}_1^\dagger] = \\ &= |r|^2 + |t|^2 = 1. \end{aligned} \quad (6.8)$$

Аналогично получаем

$$[\hat{a}_3, \hat{a}_3^\dagger] = 1 \quad (6.9)$$

и далее

$$[\hat{a}_2, \hat{a}_3^\dagger] = [t' \hat{a}_0 + r \hat{a}_1, r'^* \hat{a}_0^\dagger + t^* \hat{a}_1^\dagger] = t' r'^* + r t^* = 0. \quad (6.10)$$

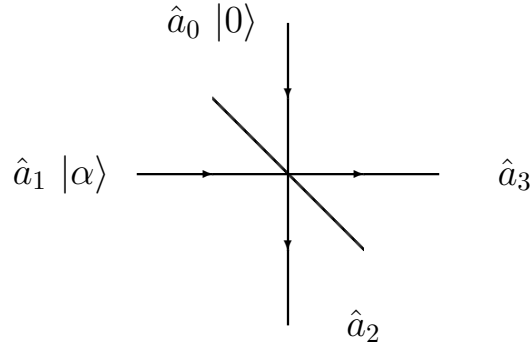


Рис. 6.4: Модель зеркала. На вход 1 (первая мода) подается когерентное состояние  $|\alpha\rangle$ , а на нулевой вход (нулевая мода) - вакуумное состояние  $|0\rangle$

Таким образом мы получили что выполнение всех требуемых коммутационных соотношений. Заметим что если возбуждена только мода 1 (вход 1), то поле нулевой моды (вход 0) нельзя отменить как это делается в классическом случае. В квантовом случае мода находится в вакуумном состоянии, и ее поле не равно нулю. Если это не учитывать, то коммутационные соотношения (6.6) будут нарушены.

Положим, что на зеркало (делитель световых пучков), изображенное на рис. 6.4, подается на вход 1 (первая мода) - когерентное состояние  $|\alpha\rangle$ , а на нулевой вход (нулевая мода) вакуумное состояние  $|0\rangle$ , т. е.

$$\begin{aligned}\hat{a}_0 |0\rangle &= 0, \\ \hat{a}_1 |\alpha\rangle &= \alpha |\alpha\rangle.\end{aligned}$$

Таким образом на входе мы имеем двухмодовое состояние

$$|\psi\rangle = |0\rangle_0 |\alpha\rangle_1.$$

Из (6.7) следует

$$\hat{a}_3 |\psi\rangle = (r'\hat{a}_0 + t\hat{a}_1) |0\rangle_0 |\alpha\rangle_1 = t\alpha |\psi\rangle,$$

откуда видно, что состояние на выходе 3 является когерентным состоянием с ослабленной амплитудой  $\alpha_3 = t\alpha$ . Аналогичным образом получим

$$\hat{a}_2 |\psi\rangle = r\alpha |\psi\rangle, \quad \alpha_2 = r\alpha. \quad (6.11)$$

Таким образом изменение амплитуды  $\alpha$  получается таким же как в классическом случае, а состояние остается когерентным.

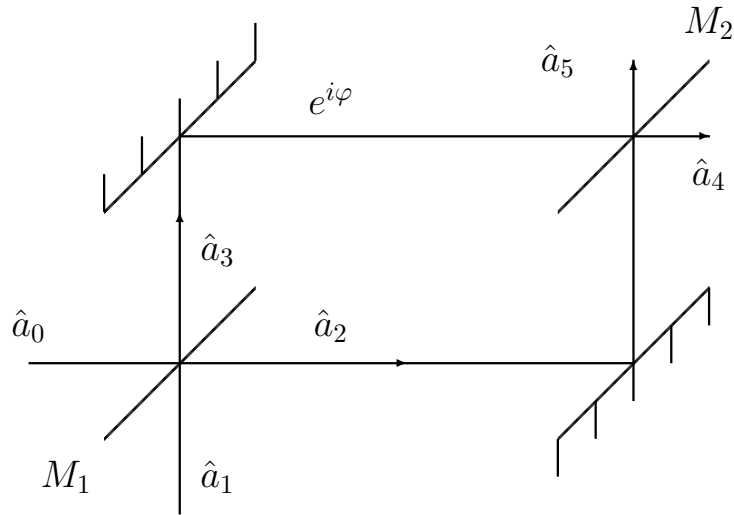


Рис. 6.5: Интерферометр Маха-Цендера. Считаем, что входное  $M_1$  и выходное  $M_2$  зеркала полупрозрачные (50:50), а два других зеркала - глухие.

## 6.3 Интерферометр Маха-Цендера. Погрешность фазовых измерений.

### 6.3.1 Уравнение интерферометра

Рассмотрим теперь более подробно работу интерферометра Маха-Цендера, схема которого изображена на [рис. 6.5](#).

Считаем, что входное  $M_1$  и выходное  $M_2$  зеркала полупрозрачные (50:50), т. е.

$$t = r = \frac{1}{\sqrt{2}},$$

а два других зеркала - глухие

$$t = 0, r = 1.$$

“Матрица рассеяния” полужеркал имеет вид

$$\hat{S} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

Мы здесь воспользовались записью (6.3). Уравнение интерферометра имеет вид:

$$\begin{aligned} \hat{a}_2 &= \frac{1}{\sqrt{2}} (\hat{a}_0 + i\hat{a}_1), \quad \hat{a}_3 = \frac{1}{\sqrt{2}} (i\hat{a}_0 + \hat{a}_1), \\ \hat{a}_4 &= \frac{1}{\sqrt{2}} (i\hat{a}_2 + e^{i\varphi}\hat{a}_3) = \frac{1}{2} [i(1 + e^{i\varphi})\hat{a}_0 - (1 - e^{i\varphi})\hat{a}_1], \\ \hat{a}_5 &= \frac{1}{\sqrt{2}} (\hat{a}_2 + ie^{i\varphi}\hat{a}_3) = \frac{1}{2} [(1 - e^{i\varphi})\hat{a}_0 + i(1 + e^{i\varphi})\hat{a}_1], \end{aligned} \quad (6.12)$$

где  $\varphi$  - разность оптических длин плеч интерферометра (разность набега фаз в плечах).

Формулы (6.12) связывают входящие поля с выходящими. Положим, что входное поле нулевого входа находится в вакуумном состоянии  $|0\rangle$ , а входное поле первого входа - в когерентном состоянии  $|\alpha\rangle$ . Таким образом входное поле находится в двухмодовом состоянии  $|\psi\rangle = |0\rangle_0 |\alpha\rangle_1$ . Далее можно найти среднее число фотонов на выходах 4 и 5 в зависимости от  $\varphi$ . Результат получится неотличимый от классического. Действительно

$$\begin{aligned}\hat{a}_5^\dagger \hat{a}_5 &= \frac{1}{4} \left[ (1 - e^{-i\varphi}) \hat{a}_0^\dagger - i(1 + e^{-i\varphi}) \hat{a}_1^\dagger \right] \\ &\quad \left[ (1 - e^{i\varphi}) \hat{a}_0 + i(1 + e^{i\varphi}) \hat{a}_1 \right] = \\ &= \frac{1}{2} \left[ (1 - \cos \phi) \hat{a}_0^\dagger \hat{a}_0 + (1 + \cos \phi) \hat{a}_1^\dagger \hat{a}_1 \right] - \frac{\sin \phi}{2} \left[ \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right]\end{aligned}\quad (6.13)$$

Таким образом для состояния  $|\psi\rangle = |0\rangle_0 |\alpha\rangle_1$  получим на фотодетекторе 5 следующий сигнал

$$\langle \psi | \hat{a}_5^\dagger \hat{a}_5 | \psi \rangle = \frac{1}{2} (1 + \cos \phi) |\alpha|^2.$$

Для фотодетектора 4 аналогичным образом получаем

$$\begin{aligned}\hat{a}_4^\dagger \hat{a}_4 &= \frac{1}{4} \left[ -i(1 + e^{-i\varphi}) \hat{a}_0^\dagger - (1 - e^{-i\varphi}) \hat{a}_1^\dagger \right] \\ &\quad \left[ i(1 + e^{i\varphi}) \hat{a}_0 - (1 - e^{i\varphi}) \hat{a}_1 \right] = \\ &= \frac{1}{2} \left[ (1 + \cos \phi) \hat{a}_0^\dagger \hat{a}_0 + (1 - \cos \phi) \hat{a}_1^\dagger \hat{a}_1 \right] + \frac{\sin \phi}{2} \left[ \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right]\end{aligned}\quad (6.14)$$

На фотодетекторе 4 имеем следующий сигнал

$$\langle \psi | \hat{a}_4^\dagger \hat{a}_4 | \psi \rangle = \frac{1}{2} (1 - \cos \phi) |\alpha|^2.$$

Мы рассмотрим более сложную схему балансного детектирования, изображенную на рис. 6.6. Каждый канал детектируется своим фотоприемником. Сигналы, идущие с фотоприемников, вычитаются и фиксируются. Такой способ регистрации по сути является синхронным детектором (гомодинным детектором), где гомодином служит поле когерентного состояния, а сигналом - вакуумные колебания.

Воспользовавшись (6.14, 6.13) можно вычислить сигнал на входе балансного детектора, который определяется средним значением оператора

$$\hat{R} = \hat{a}_5^\dagger \hat{a}_5 - \hat{a}_4^\dagger \hat{a}_4 = \left( \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_0^\dagger \hat{a}_0 \right) \cos \varphi - \left( \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right) \sin \varphi. \quad (6.15)$$



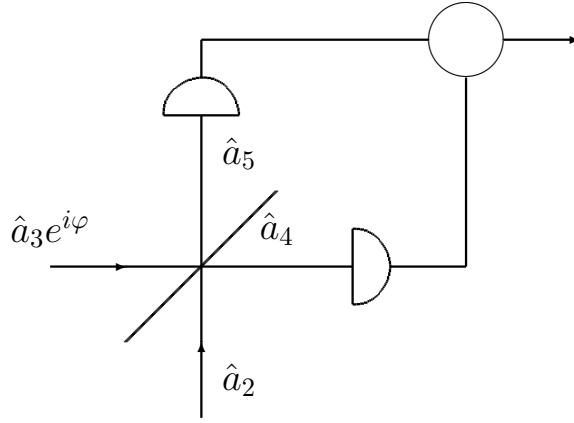


Рис. 6.6: Балансный детектор

При выводе (6.15) были использованы соотношения (6.12).

Если мода гомодина (вход 1, мода  $\hat{a}_1$ ) находится в когерентном состоянии с большой амплитудой  $\alpha$ , а сигнальная мода (вход 0, мода  $\hat{a}_0$ ) в вакуумном состоянии, то выходной сигнал равен

$$\begin{aligned} \langle \hat{R} \rangle &= \langle \psi | \hat{R} | \psi \rangle = \langle 0 |_0 \langle \alpha |_1 \left( \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_0^\dagger \hat{a}_0 \right) | 0 \rangle_0 | \alpha \rangle_1 \cos \varphi - \\ &\quad - \langle 0 |_0 \langle \alpha |_1 \left( \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right) | 0 \rangle_0 | \alpha \rangle_1 \sin \varphi = \\ &= |\alpha|^2 \cos \varphi. \end{aligned} \quad (6.16)$$

При выводе (6.16) учитывалось, что операторы первой и нулевой моды действуют только на состояние своей моды. Поэтому имеем

$$\hat{a}_0 | 0 \rangle = 0, \quad \langle 0 | \hat{a}_0^\dagger = 0,$$

следовательно

$$\langle 0 |_0 \langle \alpha |_1 \left( \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right) | 0 \rangle_0 | \alpha \rangle_1 = 0,$$

а

$$\begin{aligned} \langle \psi | \hat{R} | \psi \rangle &= \langle 0 |_0 \langle \alpha |_1 \left( \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_0^\dagger \hat{a}_0 \right) | 0 \rangle_0 | \alpha \rangle_1 = \\ &= \langle 0 |_0 \langle \alpha |_1 \left( \hat{a}_1^\dagger \hat{a}_1 \right) | 0 \rangle_0 | \alpha \rangle_1 = |\alpha|^2 = \langle \hat{n} \rangle \end{aligned}$$

среднему числу фотонов в моде гомодина.

Если  $\varphi = \frac{\pi}{2}$ , то  $\langle \hat{R} \rangle = 0$  и выходной сигнал отсутствует. При этом оператор  $\hat{R} \neq 0$ :

$$\hat{R} = - \left( \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right).$$

Хотя среднее этого оператора равно нулю, среднее его квадрата будет отличаться от нуля и будет описывать шумы, которые ограничивают точность измерения  $\varphi$ , которая в свою очередь описывает различие оптических длин плеч интерферометра.

### 6.3.2 Точность измерения интерферометром

Для начала найдем среднее квадрата шумового члена:

$$\begin{aligned} \langle \psi | \hat{R} \hat{R}^\dagger | \psi \rangle &= \langle \psi | \left( \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 \right) \left( \hat{a}_0 \hat{a}_1^\dagger + \hat{a}_1 \hat{a}_0^\dagger \right) | \psi \rangle = \\ &= \langle \psi | \left( \hat{a}_0^\dagger \hat{a}_1 \hat{a}_0 \hat{a}_1^\dagger + \hat{a}_0^\dagger \hat{a}_1 \hat{a}_1 \hat{a}_0^\dagger + \hat{a}_1^\dagger \hat{a}_0 \hat{a}_0 \hat{a}_1^\dagger + \hat{a}_1^\dagger \hat{a}_0 \hat{a}_1 \hat{a}_0^\dagger \right) | \psi \rangle. \end{aligned} \quad (6.17)$$

Из четырех членов, входящих в (6.17) три первых обращаются при усреднении в 0, а последний будет отличен от нуля. Например, для первого члена имеем

$$\begin{aligned} \langle \psi | \hat{a}_0^\dagger \hat{a}_1 \hat{a}_0 \hat{a}_1^\dagger | \psi \rangle &= \langle 0 |_0 \langle \alpha |_1 \hat{a}_0^\dagger \hat{a}_1 \hat{a}_0 \hat{a}_1^\dagger | 0 \rangle_0 | \alpha \rangle_1 = \\ &= \langle 0 |_0 \langle \alpha |_1 \hat{a}_0^\dagger \hat{a}_0 \hat{a}_1 \hat{a}_1^\dagger | 0 \rangle_0 | \alpha \rangle_1 = \langle 0 |_0 \hat{a}_0^\dagger \hat{a}_0 | 0 \rangle_0 \langle \alpha |_1 \hat{a}_1 \hat{a}_1^\dagger | \alpha \rangle_1 = 0. \end{aligned}$$

Последний член равен

$$\begin{aligned} \langle \psi | \hat{a}_1^\dagger \hat{a}_0 \hat{a}_1 \hat{a}_0^\dagger | \psi \rangle &= \langle 0 |_0 \langle \alpha |_1 \hat{a}_1^\dagger \hat{a}_0 \hat{a}_1 \hat{a}_0^\dagger | 0 \rangle_0 | \alpha \rangle_1 = \\ &= \langle 0 |_0 \langle \alpha |_1 \hat{a}_1^\dagger \hat{a}_1 \hat{a}_0 \hat{a}_0^\dagger | 0 \rangle_0 | \alpha \rangle_1 = \langle \alpha |_1 \hat{a}_1^\dagger \hat{a}_1 | \alpha \rangle_1 \langle 0 |_0 \hat{a}_0 \hat{a}_0^\dagger | 0 \rangle_0 = \\ &= \langle \alpha |_1 \hat{a}_1^\dagger \hat{a}_1 | \alpha \rangle_1 \langle 1 | 1 \rangle_0 = \langle \alpha |_1 \hat{a}_1^\dagger \hat{a}_1 | \alpha \rangle_1 = |\alpha|^2. \end{aligned} \quad (6.18)$$

Таким образом мы получили, что среднеквадратичная величина шумов равна среднему числу фотонов в моде, находящейся в когерентном состоянии:

$$|\bar{R}|^2 = \langle \hat{R} \hat{R}^\dagger \rangle = |\alpha|^2 = \bar{n}.$$

Дисперсия равна

$$\sqrt{|\bar{R}|^2} = \sqrt{\bar{n}}.$$

Сигнал возникает из-за изменения

$$\varphi = \frac{\pi}{2} + \Delta\varphi.$$

Величина его равна

$$\bar{R} = \bar{n} \cos \left( \frac{\pi}{2} + \Delta\varphi \right) \approx -\bar{n} \Delta\varphi.$$

Максимально различимым сигналом, т. е. пороговым сигналом, будем считать сигнал, равный дисперсии шумов:

$$|\bar{n}\Delta\varphi| \geq \sqrt{|\bar{R}|^2} = \sqrt{\bar{n}},$$

откуда имеем

$$\Delta\varphi \geq \frac{1}{\sqrt{\bar{n}}}.$$

Равенству соответствует пороговое значение  $\Delta\varphi$ .

Как мы увидим в дальнейшем (см. гл. 9), точность измерения можно заметно увеличить, если в сигнальное плечо интерферометра подать “сжатый вакуум”.

## 6.4 Упражнения

1. Проверить справедливость коммутационных соотношений (6.8), (6.9) и (6.10).
2. Доказать справедливость (6.11).
3. Вывести уравнение интерферометра (6.12).



## Глава 7

# Квантовое описание поляризационных свойств света

### 7.1 Классическое описание поляризационных свойств света

Поле произвольной монохроматической плоской волны можно представить в следующем виде:

$$\vec{E} = \vec{E}_0 e^{-i(\omega t - \vec{k}\vec{r})},$$

где вектор

$$\vec{E}_0 = E_x \vec{e}_x + E_y \vec{e}_y$$

определяет интенсивность и поляризационные свойства электромагнитного излучения. Для описания поляризационных свойств используется комплексный вектор поляризации - вектор Джонса:

$$\vec{e} = \alpha \vec{e}_x + \beta \vec{e}_y. \quad (7.1)$$

Компоненты этого вектора,  $\alpha$  и  $\beta$  могут быть представлены как точки на некоторой сфере называемой сферой Пуанкаре. Координаты этих точек определяются двумя углами  $\theta$  и  $\varphi$

$$\alpha = \frac{E_x}{|E_x|^2 + |E_y|^2} = \cos \frac{\theta}{2},$$

$$\beta = \frac{E_y}{|E_x|^2 + |E_y|^2} = e^{i\varphi} \sin \frac{\theta}{2}.$$

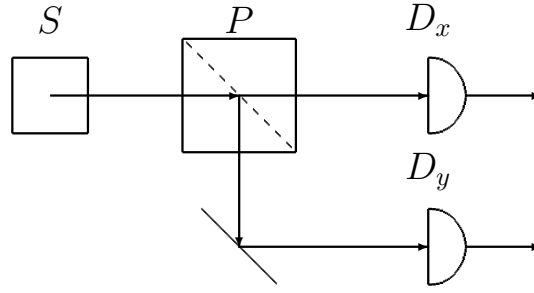


Рис. 7.1: Схема измерения параметров вектора Джонса.  $S$  - источник света,  $P$  - призма Николя,  $D_x$  и  $D_y$  - фотодетекторы.

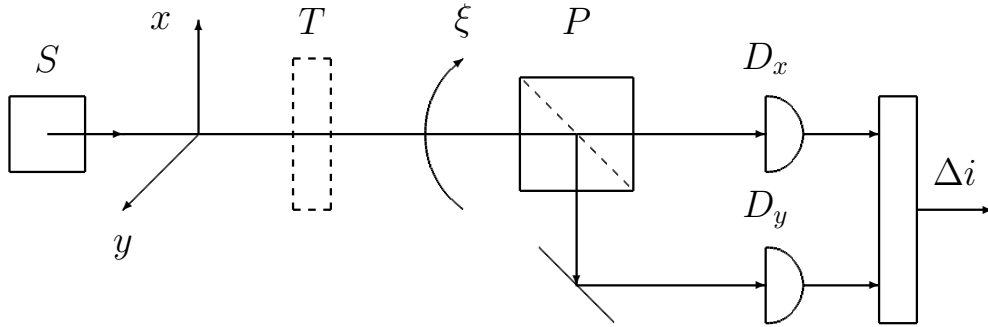


Рис. 7.2: Схема измерения параметров Стокса.  $S$  - источник света,  $P$  - призма Николя,  $\xi$  - угол ее ориентации относительно оси  $x$ , равный 0 при измерении  $S_0$  и  $S_1$ ,  $\frac{\pi}{4}$  - при измерении  $S_2$ ,  $T$  - дополнительная фазовая пластина  $\frac{\lambda}{4}$  для измерения  $S_3$ ,  $D_x$  и  $D_y$  - фотодетекторы,  $\Delta i$  - разность токов детекторов.

Для измерения компонентов вектора Джонса  $\alpha$  и  $\beta$  может быть использована схема, представленная на рис. 7.1. Здесь пучок поляризованного света направляется на призму Николя  $P$ , разделяющую  $x$  и  $y$  компоненты этого пучка, которые подаются на два фотодетектора  $D_x$  и  $D_y$ .

Кроме вектора Джонса, для описания поляризационных свойств часто используют вектор Стокса, четыре компонента которого имеют размерность интенсивности и могут быть легко измерены экспериментально. Вектор Стокса может быть определен следующим образом:

$$\begin{aligned} S_0 &= |E_x|^2 + |E_y|^2, \\ S_1 &= |E_x|^2 - |E_y|^2, \\ S_2 &= E_x^* E_y + E_x E_y^* = 2\text{Re}(E_x^* E_y), \\ S_3 &= \frac{E_x^* E_y - E_x E_y^*}{i} = 2\text{Im}(E_x^* E_y), \end{aligned} \quad (7.2)$$

где значения амплитуд  $E_{x,y}$  взяты в некоторый момент времени  $t$ . Параметр  $S_0$  в (7.2) определяет интенсивность волны в момент времени  $t$ , а остальные три параметра  $S_1$ ,  $S_2$  и  $S_3$  - поляризационные свойства.

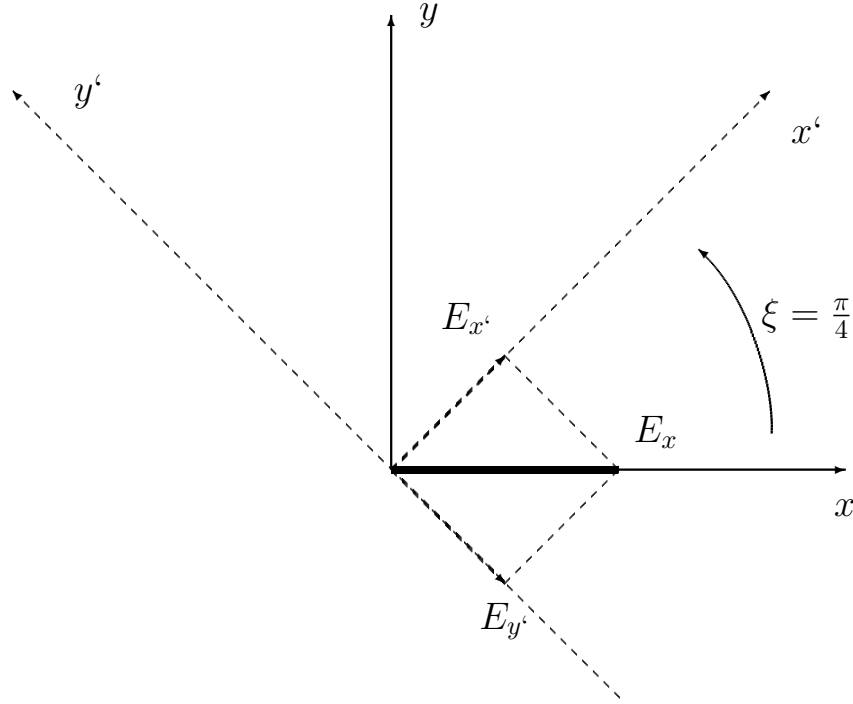


Рис. 7.3: Поляризация в повернутой системе координат.  $E_{x'} = \frac{E_y + E_x}{\sqrt{2}}$ ,  $E_{y'} = \frac{E_y - E_x}{\sqrt{2}}$ , т. о.  $|E_{x'}|^2 - |E_{y'}|^2 = E_{x'} E_{x'}^* - E_{y'} E_{y'}^*$  или же  $|E_{x'}|^2 - |E_{y'}|^2 = \frac{|E_x|^2 + |E_y|^2 + E_x E_y^* + E_x^* E_y}{2} - \frac{|E_x|^2 + |E_y|^2 - E_x E_y^* - E_x^* E_y}{2}$ , т. е.  $|E_{x'}|^2 - |E_{y'}|^2 = E_x^* E_y + E_x E_y^* = 2\text{Re}(E_x^* E_y) = S_2$

Для измерения параметров Стокса может быть использована схема, представленная на [рис. 7.2](#) [44]. Для измерения  $S_1$ ,  $S_2$  и  $S_3$  необходимо разделить исходный пучок на три части, каждая из которых подается на детектор, изображенный на [рис. 7.2](#).

Для измерения  $S_1$  используется призма Николя  $P$ , которая разделяет  $x$  и  $y$  поляризованные компоненты пучка, так что разность токов двух фотодетекторов пропорциональна  $S_1$ , при этом сумма токов будет пропорциональна  $S_0$ . Для измерения  $S_2$  призма поворачивается на угол  $\xi = \frac{\pi}{4}$ , так что разность токов будет пропорциональна  $S_2$  (см. [рис. 7.3](#)). Для измерения  $S_3$  перед призмой ставится фазовая пластина  $\frac{\lambda}{4}$  с ориентацией  $\frac{\pi}{4}$ , в результате разность токов фотодетекторов будет пропорциональна  $S_3$ .

Результаты показаний детекторов усредняются по времени. Таким образом можно говорить о том, что измеряются усредненные параметры Стокса -  $\langle S_k \rangle$ , которые могут быть также использованы для описания частично поляризованного света. Для количественной характеристики такого излучения

используется величина, называемая степенью поляризации:

$$P = \frac{\sqrt{\langle S_1 \rangle^2 + \langle S_2 \rangle^2 + \langle S_3 \rangle^2}}{\langle S_0 \rangle}.$$

Степень поляризации полностью поляризованного света  $P = 1$ . Для полностью не поляризованного света  $P = 0$ .

## 7.2 Квантовое описание поляризационных свойств света

При описании поляризационных свойств однофотонного состояния удобно использовать вектор Джонса, при этом волновая функция будет иметь вид:

$$|\psi\rangle = \alpha |x\rangle + \beta |y\rangle, \quad (7.3)$$

где  $|\alpha|^2 + |\beta|^2 = 1$ , а  $|x\rangle = |1\rangle_x \otimes |0\rangle_y$  обозначает однофотонное состояние, поляризованное по  $x$ . Аналогично  $|y\rangle = |0\rangle_x \otimes |1\rangle_y$  - однофотонное состояние, поляризованное по  $y$ .

Измеряемыми величинами у нас будут параметры Стокса, так что переменные (7.2) должны быть заменены на операторы. Для этого мы заменим операторы электрического поля  $E_{x,y}$  на операторы уничтожения  $\hat{a}_{x,y}$ , в результате получим

$$\begin{aligned} \hat{S}_0 &= \hat{a}_x^\dagger \hat{a}_x + \hat{a}_y^\dagger \hat{a}_y, \\ \hat{S}_1 &= \hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y, \\ \hat{S}_2 &= \hat{a}_x^\dagger \hat{a}_y + \hat{a}_x \hat{a}_y^\dagger, \\ \hat{S}_3 &= \frac{\hat{a}_x^\dagger \hat{a}_y - \hat{a}_x \hat{a}_y^\dagger}{i}. \end{aligned} \quad (7.4)$$

В дальнейшем нас будут интересовать прежде всего два оператора  $\hat{S}_1$  и  $\hat{S}_2$ , для которых мы найдем коммутатор, собственные числа и вектора.



Для коммутатора  $[\hat{S}_1 \hat{S}_2]$  имеем:

$$\begin{aligned}
[\hat{S}_1 \hat{S}_2] &= \hat{S}_1 \hat{S}_2 - \hat{S}_2 \hat{S}_1 = \\
&= \hat{a}_x^\dagger \hat{a}_x \hat{a}_x^\dagger \hat{a}_y - \hat{a}_y^\dagger \hat{a}_y \hat{a}_y^\dagger \hat{a}_x + \\
&\quad + \hat{a}_x^\dagger \hat{a}_x \hat{a}_x \hat{a}_y^\dagger - \hat{a}_y^\dagger \hat{a}_y \hat{a}_y^\dagger \hat{a}_x - \\
&\quad - \hat{a}_x^\dagger \hat{a}_x^\dagger \hat{a}_x \hat{a}_y + \hat{a}_y \hat{a}_y^\dagger \hat{a}_y \hat{a}_x^\dagger - \\
&\quad - \hat{a}_x \hat{a}_x^\dagger \hat{a}_x \hat{a}_y^\dagger + \hat{a}_y^\dagger \hat{a}_y^\dagger \hat{a}_y \hat{a}_x = \\
&= \hat{a}_x^\dagger [\hat{a}_x \hat{a}_x^\dagger] \hat{a}_y - [\hat{a}_x \hat{a}_x^\dagger] \hat{a}_x \hat{a}_y^\dagger + \\
&\quad + [\hat{a}_y \hat{a}_y^\dagger] \hat{a}_y \hat{a}_x^\dagger - \hat{a}_y^\dagger [\hat{a}_y \hat{a}_y^\dagger] \hat{a}_x = \\
&= \hat{a}_x^\dagger \hat{a}_y + \hat{a}_y \hat{a}_x^\dagger - \hat{a}_x \hat{a}_y^\dagger - \hat{a}_y^\dagger \hat{a}_x = \\
&= 2 (\hat{a}_x^\dagger \hat{a}_y - \hat{a}_x \hat{a}_y^\dagger) = 2i\hat{S}_3 \neq 0.
\end{aligned} \tag{7.5}$$

При выводе (7.5) мы воспользовались коммутационными соотношениями для операторов рождения и уничтожения:

$$[\hat{a}_x \hat{a}_x^\dagger] = [\hat{a}_y \hat{a}_y^\dagger] = 1,$$

а также тем фактом, что операторы действующие на разные компоненты поляризации  $x$  и  $y$ , коммутируют между собой.

Для получения собственных чисел и векторов операторов  $\hat{S}_1$  и  $\hat{S}_2$  удобно представить их в матричной форме. Для этого будем использовать базис, образованный векторами  $|x\rangle$  и  $|y\rangle$ :

$$\begin{aligned}
|x\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \\
|y\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix},
\end{aligned}$$

Для оператора  $\hat{S}_1$  имеем:

$$\begin{aligned}
\hat{S}_1 |x\rangle &= \hat{a}_x^\dagger \hat{a}_x |1\rangle_x \otimes |0\rangle_y - \hat{a}_y^\dagger \hat{a}_y |1\rangle_x \otimes |0\rangle_y = \\
&= \hat{a}_x^\dagger \hat{a}_x |1\rangle_x \otimes |0\rangle_y = |1\rangle_x \otimes |0\rangle_y = |x\rangle, \\
\hat{S}_1 |y\rangle &= \hat{a}_x^\dagger \hat{a}_x |0\rangle_x \otimes |1\rangle_y - \hat{a}_y^\dagger \hat{a}_y |0\rangle_x \otimes |1\rangle_y = \\
&= -\hat{a}_y^\dagger \hat{a}_y |0\rangle_x \otimes |1\rangle_y = -|0\rangle_x \otimes |1\rangle_y = -|y\rangle,
\end{aligned} \tag{7.6}$$

откуда получаем следующее матричное представление

$$\hat{S}_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{7.7}$$

Из (7.7) можно написать уравнение для собственных чисел:

$$(1 - s)(1 + s) = 0,$$

из которого можно найти два собственных значения  $s_1 = 1$  и  $s_2 = -1$ . Как нетрудно проверить, собственным вектором для  $s_1 = 1$  будет  $|s_1\rangle = |x\rangle$ . Действительно, из (7.6) имеем:

$$\hat{S}_1 |s_1\rangle = \hat{S}_1 |x\rangle = 1 \cdot |s_1\rangle. \quad (7.8)$$

Для второго собственного числа - собственным вектором будет  $|s_2\rangle = |y\rangle$ :

$$\hat{S}_1 |s_2\rangle = -|y\rangle = -1 \cdot |s_2\rangle. \quad (7.9)$$

Для оператора  $\hat{S}_2$  имеем:

$$\begin{aligned} \hat{S}_2 |x\rangle &= \hat{a}_x^\dagger \hat{a}_y |1\rangle_x \otimes |0\rangle_y + \hat{a}_y^\dagger \hat{a}_x |1\rangle_x \otimes |0\rangle_y = \\ &= \hat{a}_y^\dagger \hat{a}_x |1\rangle_x \otimes |0\rangle_y = |0\rangle_x \otimes |1\rangle_y = |y\rangle, \\ \hat{S}_2 |y\rangle &= \hat{a}_x^\dagger \hat{a}_y |0\rangle_x \otimes |1\rangle_y + \hat{a}_y^\dagger \hat{a}_x |0\rangle_x \otimes |1\rangle_y = \\ &= \hat{a}_x^\dagger \hat{a}_y |0\rangle_x \otimes |1\rangle_y = |1\rangle_x \otimes |0\rangle_y = |x\rangle. \end{aligned} \quad (7.10)$$

Из (7.10) имеем следующее матричное представление оператора  $\hat{S}_2$ :

$$\hat{S}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (7.11)$$

По аналогии с оператором  $\hat{S}_1$  из (7.10) и (7.11) можно получить два собственных числа  $s_1 = 1$  и  $s_2 = -1$ . Для первого числа собственным вектором будет

$$|s_1\rangle = \frac{1}{\sqrt{2}} (|x\rangle + |y\rangle), \quad (7.12)$$

а для второго

$$|s_2\rangle = \frac{1}{\sqrt{2}} (|x\rangle - |y\rangle). \quad (7.13)$$

Для оператора  $\hat{S}_3$  имеем:

$$\begin{aligned} \hat{S}_3 |x\rangle &= \frac{1}{i} \left( \hat{a}_x^\dagger \hat{a}_y |1\rangle_x \otimes |0\rangle_y - \hat{a}_y^\dagger \hat{a}_x |1\rangle_x \otimes |0\rangle_y \right) = \\ &= -\frac{1}{i} \hat{a}_y^\dagger \hat{a}_x |1\rangle_x \otimes |0\rangle_y = -\frac{1}{i} |0\rangle_x \otimes |1\rangle_y = -\frac{|y\rangle}{i} = i |y\rangle, \\ \hat{S}_3 |y\rangle &= \frac{1}{i} \left( \hat{a}_x^\dagger \hat{a}_y |0\rangle_x \otimes |1\rangle_y + \hat{a}_y^\dagger \hat{a}_x |0\rangle_x \otimes |1\rangle_y \right) = \\ &= \frac{1}{i} \hat{a}_x^\dagger \hat{a}_y |0\rangle_x \otimes |1\rangle_y = \frac{1}{i} |1\rangle_x \otimes |0\rangle_y = -i |x\rangle. \end{aligned} \quad (7.14)$$

Таким образом из (7.14) получаем следующее матричное представление оператора  $\hat{S}_3$ :

$$\hat{S}_3 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}. \quad (7.15)$$

Из (7.15) можно получить что собственными числами являются все те же  $s_1 = 1$  и  $s_2 = -1$ . При этом собственными состояниями оператора  $\hat{S}_3$  являются состояния с левой и правой круговыми поляризациями:

$$\begin{aligned} |s_1\rangle &= |-\rangle = \frac{1}{\sqrt{2}} (|x\rangle - i|y\rangle), \\ |s_2\rangle &= |+\rangle = \frac{1}{\sqrt{2}} (|x\rangle + i|y\rangle). \end{aligned} \quad (7.16)$$

TBD: Добавить про связь с Матрицами Паули

## 7.3 Упражнения

1. TBD



## Часть 3

# Неклассический свет



## Глава 8

# Неклассический свет

Квантовые состояния света можно разбить на две группы: состояния, которые при росте интенсивности света асимптотически стремятся к классическому состоянию (классическому свету) и состояния, которые не обладают таким свойством. Например, из рассмотренных нами ранее состояний когерентное состояние имеет классический предел, а энергетическое (фоковское) состояние его не имеет.

Ранее мы определили понятие функции когерентности второго порядка  $G^{(2)}$ . Для одномодового света (5.33)

$$\begin{aligned} G^{(2)} &= \frac{\langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rangle}{\langle \hat{a}^\dagger \hat{a} \rangle^2} = \\ &= \frac{\langle \hat{a}^\dagger \hat{a} (\hat{a}^\dagger \hat{a} - 1) \rangle}{\langle \hat{a}^\dagger \hat{a} \rangle^2} = \frac{\langle n^2 \rangle - \langle n \rangle}{\langle n \rangle^2}, \end{aligned} \quad (8.1)$$

где использованы коммутационные соотношения  $[\hat{a}\hat{a}^\dagger] = 1$ ,  $\hat{n} = \hat{a}^\dagger \hat{a}$  - оператор числа частиц.

В классическом случае  $\langle \hat{a}^\dagger \hat{a} \rangle = |\alpha|^2$ , где  $|\alpha|^2 = I$  интенсивность поля (модуль квадрата амплитуды поля). Поскольку классические величины коммутируют, формулу (8.1) в классическом случае можно заменить

$$G_{\text{кл.}}^{(2)} = \frac{\langle |\alpha|^4 \rangle}{\langle |\alpha|^2 \rangle^2} = \frac{\langle I^2 \rangle}{\langle I \rangle^2}, \quad (8.2)$$

где усреднение осуществляется при помощи положительно определенной классической функции распределения  $P(\alpha)$

$$\langle |\alpha|^{2n} \rangle = \int_0^\infty P(|\alpha|^2) |\alpha|^{2n} d^2\alpha, \quad n = 1, 2.$$

Рассмотрим разность  $G_{\text{кл.}}^{(2)} - G_{\text{кл.}}^{(1)} = G_{\text{кл.}}^{(2)} - 1$ , т. к. для одномодового поля, как мы знаем,  $G_{\text{кл.}}^{(1)} = 1$  всегда. Из (8.2) следует

$$\begin{aligned}
 G_{\text{кл.}}^{(2)} - G_{\text{кл.}}^{(1)} &= G_{\text{кл.}}^{(2)} - 1 = \\
 &= \frac{\langle |\alpha|^4 \rangle}{\langle |\alpha|^2 \rangle^2} - 1 = \frac{\langle |\alpha|^4 \rangle - \langle |\alpha|^2 \rangle^2}{\langle |\alpha|^2 \rangle^2} = \\
 &= \frac{\int_0^\infty P |\alpha|^4 d^2\alpha - 2 \langle |\alpha|^2 \rangle^2 + \langle |\alpha|^2 \rangle^2}{\langle |\alpha|^2 \rangle^2} = \\
 &= \frac{\int_0^\infty P \left( |\alpha|^4 - 2 |\alpha|^2 \langle |\alpha|^2 \rangle + \langle |\alpha|^2 \rangle^2 \right) d^2\alpha}{\langle |\alpha|^2 \rangle^2} = \\
 &= \frac{\int_0^\infty P \left( |\alpha|^2 - \langle |\alpha|^2 \rangle \right)^2 d^2\alpha}{\langle |\alpha|^2 \rangle^2} \geq 0.
 \end{aligned} \tag{8.3}$$

Из неравенства (8.3) следует, что

$$G_{\text{кл.}}^{(2)} \geq 1.$$

В квантовом случае из-за некоммутативности операторов ситуация будет иная. Формулу (8.1) перепишем в следующем виде

$$\begin{aligned}
 G^{(2)} &= \frac{\langle \hat{n}^2 \rangle - \langle \hat{n} \rangle}{\langle \hat{n} \rangle^2} = \\
 &= 1 + \frac{(\langle \hat{n}^2 \rangle - \langle \hat{n} \rangle^2) - \langle \hat{n} \rangle}{\langle \hat{n} \rangle^2} = 1 + \frac{\sigma^2 - \langle \hat{n} \rangle}{\langle \hat{n} \rangle^2},
 \end{aligned} \tag{8.4}$$

где  $\sigma^2$  - среднеквадратичное отклонение от среднего, т. е.  $\sigma$  - дисперсия.

Из (8.4) следует, что  $G^{(2)}$  может быть как больше, так и меньше 1, смотря что больше:  $\sigma^2$  или  $\langle \hat{n} \rangle$ . В классическом случае  $G^{(2)} \geq 1$ , поэтому критерием неклассичности можно принять

$$G^{(2)} < 1 \tag{8.5}$$

Из (8.4, 8.5) следует, что условием неклассичности будет  $\sigma^2 - \langle \bar{n} \rangle < 0$ , т. е. квадрат дисперсии должен быть меньше среднего числа фотонов. Известно, что поток фотонов, для которого  $\sigma^2 - \langle \bar{n} \rangle = 0$ , имеет пуассоновскую





Рис. 8.1: Примеры реализаций фотоотсчетов, соответствующие различным статистическим свойствам света: а) группировка и свехпуассоновская статистика, б) пуассоновская статистика, в) антигруппировка и субпуассоновская статистика (по данным работы [45]).

статистику (примером служит когерентное состояние). Случай  $\sigma^2 - \langle \bar{n} \rangle < 0$  соответствует более регулярному потоку, который называется субпуассоновским. Это случай антигруппировки фотонов. Примером состояния, для которого это справедливо, является например состояние, возникающее в результате параметрического рассеяния, которое мы рассмотрим позднее. Случай  $\sigma^2 - \langle \bar{n} \rangle > 0$  соответствует менее регулярному процессу, когда фотоны группируются (примером является тепловое возбуждение света). Такое состояние называется суперпуассоновским. Все три случая изображены на рис. 8.1, где показано расположение фотоотсчетов во времени.

Мы приходим к заключению, что неклассическим состояниям соответствует субпуассоновский порог. Число  $G^{(2)}$  просто связано с другими параметрами, характеризующими флуктуации числа фотонов: с дисперсией и фактором Фоко, которые часто встречаются в литературе.

$$\Phi = \frac{\sigma^2}{\langle \bar{n} \rangle},$$

$$G^{(2)} - 1 = \frac{\Phi - 1}{\langle \bar{n} \rangle}$$

Экспериментальный характер статистики можно установить из эксперимента, в котором определяется корреляционная функция второго порядка (эксперимент Брауна - Твисса). Схема эксперимента изображена на рис. 8.2

Регулируемая задержка  $\tau$  осуществляется изменением длины одного из плеч.

На рис. 8.3 изображены три кривые, которые получаются в результате эксперимента. Кривая (б) соответствует когерентному состоянию. Кривая (а)

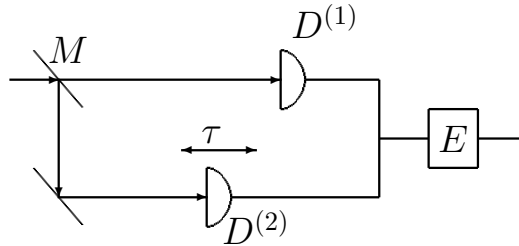


Рис. 8.2: Схема эксперимента Брауна-Твисса. При помощи 50% зеркала  $M$  световой пучок направляется на два фотоприемника  $D^{(1)}$  и  $D^{(2)}$ . Регулируемая задержка  $\tau$  осуществляется перемещением фотодетектора  $D^{(2)}$ . Результат с фотодетекторов подается на схему совпадений  $E$ .

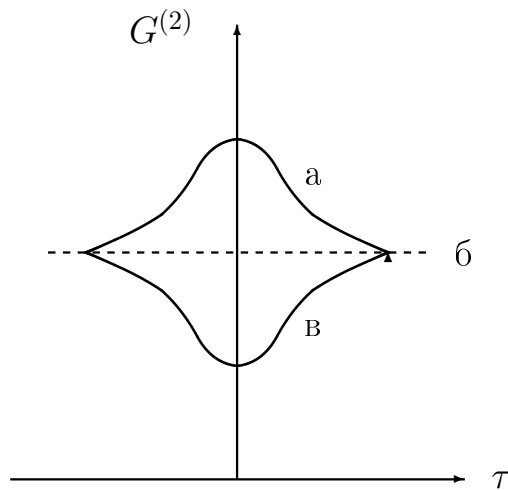


Рис. 8.3: Качественный вид зависимости корреляционной функции  $G^{(2)}$  от задержки  $\tau$  для 3 различных случаев: а) группировка и свехпуассоновская статистика, б) пуассоновская статистика, в) антигруппировка и субпуассоновская статистика.

соответствует группировке фотонов и сверхпуассоновской статистике. Кривая (в) соответствует антигруппировке и субпуассоновской статистике. Такая кривая характерна для неклассического света. Объяснение поведения кривых просто. Если  $\tau$  велико, фотоотсчеты фотоприемников случайны и не зависят друг от друга. Поэтому поведение всех трех кривых определяется случайными совпадениями и для всех трех будет одинаково. При малых  $\tau$  поведение кривых различно. В случае группировки фотонов мы будем иметь максимум при  $\tau = 0$ , а при антигруппировке - минимум.

Еще одним критерием неклассичности является отсутствие положительной определенности квазивероятности  $P(\alpha)$ , если используется представление когерентных состояний.

В классическом случае функция  $P(\alpha)$  должна быть всюду положительно определена, т. е.  $P(\alpha) \geq 0$  при всех значения  $\alpha$ . Рассмотрим этот вопрос подробнее. Условие неклассичности  $G^{(2)} < 1$ , с помощью (8.1) это условие можно представить в виде

$$\langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rangle - \langle \hat{a}^\dagger \hat{a} \rangle^2 < 0. \quad (8.6)$$

Рассмотрим выражение

$$\int P(\alpha) \left( |\alpha|^2 - \langle \hat{n} \rangle \right)^2 d^2\alpha < 0 \quad (8.7)$$

$$\begin{aligned} \int P(\alpha) \left( |\alpha|^2 - \langle \hat{n} \rangle \right)^2 d^2\alpha &= \int P(\alpha) \left( |\alpha|^4 - 2|\alpha|^2 \langle \hat{n} \rangle + \langle \hat{n} \rangle^2 \right) d^2\alpha = \\ &= \langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rangle - \langle \hat{a}^\dagger \hat{a} \rangle^2 < 0, \end{aligned}$$

т. е. выражения (8.6) и (8.7) эквивалентны. Это следует из следующих соотношений

$$\begin{aligned} \langle \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rangle &= Sp(\hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \rho) = \\ &= \sum_n \langle n | \left( \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} \int P(\alpha) |\alpha\rangle \langle \alpha| d^2\alpha \right) | n \rangle = \\ &= \int P(\alpha) \langle \alpha | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} | \alpha \rangle d^2\alpha = \int P(\alpha) |\alpha|^4 d^2\alpha, \\ &\int P(\alpha) |\alpha|^2 d^2\alpha = \langle \hat{a}^\dagger \hat{a} \rangle = \langle \hat{n} \rangle. \end{aligned}$$

Мы получили, что выражение (8.7) должно быть отрицательным. Поскольку  $\left( |\alpha|^2 - \langle \hat{n} \rangle \right)^2$  всегда положительно, то отрицательный результат будет получен, если  $P(\alpha)$  по крайней мере в части области  $(\alpha)$  будет отрицательно.

Таким образом, для неклассического света квазивероятность  $P(\alpha)$  не является положительно определенной функцией.

## Глава 9

# Сжатые состояния

В сжатых состояниях реализуется возможность, допускаемая соотношением неопределенности Гайзенберга, уменьшить неопределенность одной из сопряженных наблюдаемых за счет увеличения неопределенности другой. Такие состояния могут оказаться полезными в квантовой оптике для практических нужд. Например, для повышения точности интерференционных экспериментов.

Далее рассматривается теория сжатых состояний в параметрических процессах и применения сжатых состояний в интерференционных экспериментах.

### 9.1 Соотношение неопределенности Гайзенберга

В квантовой механике двум сопряженным наблюдаемым  $A$  и  $B$  соответствуют некоммутирующие операторы  $\hat{A}$  и  $\hat{B}$ , удовлетворяющие коммутационному соотношению

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} = i\hat{C},$$

где  $\hat{C}$  некоторый эрмитов оператор. В этом случае наблюдаемые  $A$  и  $B$  могут быть измерены только с некоторой неопределенностью, выражаемой соотношением неопределенности Гайзенберга (более подробно см. [разд. 14.3.1](#))

$$(\Delta A \Delta B) \geq \frac{1}{2} |\langle \hat{C} \rangle|, \quad (9.1)$$

где

$$(\Delta A)^2 = \langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2$$

и

$$(\Delta B)^2 = \langle \hat{B}^2 \rangle - \langle \hat{B} \rangle^2$$

средний квадрат отклонения от среднего значения. Среднее  $\langle \dots \rangle$  соответствует квантовому состоянию, в котором находится квантовый объект.

Соотношение (9.1) ограничивает только произведение неопределенностей, допуская состояния, для которых неопределенность одной из наблюдаемых существенно меньше неопределенности другой. Если

$$(\Delta A)^2 < \frac{1}{2} |\langle \hat{C} \rangle|,$$

то такое состояние называется сжатым состоянием для наблюдаемой  $A$ . Если при этом наблюдается условие минимальной неопределенности

$$(\Delta A \Delta B) = \frac{1}{2} |\langle \hat{C} \rangle|,$$

то такое состояние называют идеально сжатым.

## 9.2 Операторы квадратурных составляющих электромагнитного поля

Рассмотрим оператор одномодового электромагнитного поля

$$\hat{\vec{E}} = E_1 \vec{e} [\hat{a} e^{-i\omega t} + \hat{a}^\dagger e^{i\omega t}]$$

и введем два новых оператора, связанных с ним

$$\begin{aligned} \hat{X}_1 &= \frac{1}{2} (\hat{a} + \hat{a}^\dagger), \\ \hat{X}_2 &= \frac{1}{2i} (\hat{a} - \hat{a}^\dagger), \end{aligned}$$

которые пропорциональны операторам  $\hat{q}$  и  $\hat{p}$  (координата, импульс) с которыми мы познакомились раньше.

Операторы  $\hat{X}_1$  и  $\hat{X}_2$  являются эрмитовыми операторами. Коммутационные соотношения для них имеют вид.

$$\begin{aligned} [\hat{X}_1, \hat{X}_2] &= (\hat{X}_1 \hat{X}_2 - \hat{X}_2 \hat{X}_1) = \\ &= \frac{1}{4i} \{ (\hat{a} + \hat{a}^\dagger) (\hat{a} - \hat{a}^\dagger) - (\hat{a} - \hat{a}^\dagger) (\hat{a} + \hat{a}^\dagger) \} = \\ &= \frac{1}{4i} \{ \hat{a}^\dagger \hat{a} - \hat{a} \hat{a}^\dagger - \hat{a} \hat{a}^\dagger + \hat{a}^\dagger \hat{a} \} = \frac{1}{2i} \{ \hat{a}^\dagger \hat{a} - \hat{a} \hat{a}^\dagger \} = \\ &= \frac{1}{2i} [\hat{a}^\dagger, \hat{a}] = \frac{i}{2} \end{aligned}$$

При помощи операторов  $\hat{X}_1$  и  $\hat{X}_2$  оператор электрического поля можно представить в виде

$$E = 2E_1 \vec{e} \left( \hat{X}_1 \cos \omega t + \hat{X}_2 \sin \omega t, \right)$$

т. е. эти операторы можно рассматривать, как операторы квадратурных компонент электромагнитного поля. Из соотношения неопределенности (9.1) имеем

$$(\Delta X_1 \Delta X_2) \geq \frac{1}{4}.$$

Условием сжатого состояния будет

$$(\Delta X_i) < \frac{1}{4}, \quad i = 1, 2.$$

Если при этом выполняется соотношение минимальной неопределенности

$$(\Delta X_1 \Delta X_2) = \frac{1}{4},$$

то сжатие будет идеальным.

Для примера рассмотрим неопределенность  $\hat{X}_1$ ,  $\hat{X}_2$  в случае, когда поле находится в когерентном состоянии:

$$\begin{aligned} (\Delta X_1)^2 &= \langle \alpha | \hat{X}_1^2 | \alpha \rangle - \langle \alpha | \hat{X}_1 | \alpha \rangle^2 = \\ &= \frac{1}{4} \left\{ \langle \alpha | (\hat{a} + \hat{a}^\dagger)^2 | \alpha \rangle - \langle \alpha | (\hat{a} + \hat{a}^\dagger) | \alpha \rangle^2 \right\} = \\ &= \frac{1}{4} \left\{ \alpha^{*2} + \alpha^2 + 2|\alpha|^2 + 1 - (\alpha^{*2} + \alpha^2 + 2|\alpha|^2) \right\} = \frac{1}{4}. \end{aligned}$$

Аналогично можно получить

$$(\Delta X_2)^2 = \frac{1}{4} \tag{9.2}$$

и

$$(\Delta X_1 \Delta X_2) = \frac{1}{4}. \tag{9.3}$$

Таким образом мы получили, что рассматриваемый случай является состоянием с минимальной неопределенностью, но сжатия нет.

Рассмотрим теперь, что дает энергетическое состояние  $|n\rangle$ . Имеем

$$\begin{aligned} (\Delta X_1)^2 &= \frac{1}{4} \left\{ \langle n | (\hat{a} + \hat{a}^\dagger)^2 | n \rangle - \langle n | (\hat{a} + \hat{a}^\dagger) | n \rangle^2 \right\} = \\ &= \frac{1}{4} \langle n | (\hat{a} + \hat{a}^\dagger)^2 | n \rangle = \frac{1}{4} \langle n | (\hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}) | n \rangle = \\ &= \frac{1}{4} \langle n | (1 + 2\hat{a}^\dagger\hat{a}) | n \rangle = \frac{1}{4} (2n + 1). \end{aligned}$$

Аналогично

$$(\Delta X_2)^2 = \frac{1}{4} (2n + 1) \quad (9.4)$$

и

$$(\Delta X_1 \Delta X_2) = \frac{1}{4} (2n + 1). \quad (9.5)$$

Следовательно, энергетическое состояние не является состоянием с минимальной неопределенностью и сжатым состоянием для наблюдаемых  $X_1$  или  $X_2$ .

### 9.3 Сжатие квадратурного состояния

Сначала рассмотрим теоретическую возможность создания сжатых квадратурных состояний. Рассмотрим построение сжатого состояния из когерентного состояния, в котором будет сжата одна из квадратурных составляющих. Преобразование состояний производится при помощи некоторого унитарного преобразования.

Рассмотрим унитарный оператор, который называют оператором сжатия (причина такого названия станет ясна из дальнейшего)

$$\hat{S}(z) = e^{\frac{1}{2}z^* \hat{a}^2 - \frac{1}{2}z \hat{a}^{+2}},$$

где  $z = re^{i\theta}$  - произвольное комплексное число. Сопряженный оператор имеет вид

$$\hat{S}^\dagger(z) = e^{\frac{1}{2}z \hat{a}^{+2} - \frac{1}{2}z^* \hat{a}^2},$$

откуда видно, что

$$\hat{S}\hat{S}^\dagger = \hat{S}^\dagger\hat{S} = \hat{I},$$

где  $\hat{I}$  является единичным оператором. Таким образом,  $\hat{S}^\dagger = \hat{S}^{-1}$  действительно является унитарным оператором.

Рассмотрим действие оператора  $\hat{S}(z)$  на операторы  $\hat{a}$  и  $\hat{a}^\dagger$  и на когерентное состояние. Для этой цели применим теорему об операторном разложении (подробный вывод см. теорему об операторном тождестве (Теорема 17.1.1)):

$$e^{\hat{A}}\hat{B}e^{-\hat{A}} = \hat{B} + [\hat{A}, \hat{B}] + \frac{1}{2!} [\hat{A}, [\hat{A}, \hat{B}]] + \dots \quad (9.6)$$

При помощи (9.6) легко показать, если принять

$$e^{\hat{A}} = \hat{S}(z), \quad \hat{B} = \hat{a},$$



что

$$\begin{aligned}\hat{A} &= \hat{S}(z) \hat{a} \hat{S}^\dagger(z) = \hat{a} + z \hat{a}^\dagger + \frac{|z|^2 \hat{a}}{2!} + \frac{z |z|^2 \hat{a}^\dagger}{3!} + \dots = \\ &= \hat{a} \cosh r + \hat{a}^\dagger e^{i\theta} \sinh r = \mu \hat{a} + \nu \hat{a}^\dagger,\end{aligned}\quad (9.7)$$

где  $\mu = \cosh r$ ,  $\nu = e^{i\theta} \sinh r$ ,  $|\mu|^2 - |\nu|^2 = 1$ . Таким же образом можно показать, что при обратном порядке действия операторов  $\hat{S}^\dagger \dots \hat{S}$  получается формула, которая отличается от (9.7) только знаком между слагаемыми:

$$\begin{aligned}\hat{S}^\dagger(z) \hat{a} \hat{S}(z) &= \hat{a} \cosh r - \hat{a}^\dagger e^{i\theta} \sinh r, \\ \hat{S}^\dagger(z) \hat{a}^\dagger \hat{S}(z) &= \hat{a}^\dagger \cosh r - \hat{a} e^{-i\theta} \sinh r.\end{aligned}\quad (9.8)$$

Подействуем оператором  $\hat{S}$  на вектор когерентного состояния. При этом мы получим новое состояние:

$$|\alpha, z\rangle = \hat{S}(z) |\alpha\rangle. \quad (9.9)$$

Покажем теперь, что состояние  $|\alpha, z\rangle$  является собственным состоянием оператора  $\hat{A}$ :

$$\begin{aligned}\hat{A} |\alpha, z\rangle &= \hat{S}(z) \hat{a} \hat{S}^\dagger(z) \hat{S}(z) |\alpha\rangle = \hat{S}(z) \hat{a} |\alpha\rangle = \\ &= \alpha \hat{S}(z) |\alpha\rangle = \alpha |\alpha, z\rangle.\end{aligned}\quad (9.10)$$

Здесь использовано определение  $\hat{A}$  и  $\hat{S} \hat{S}^\dagger = \hat{I}$ . Из (9.10) следует, что состояние  $|\alpha, z\rangle$  является собственным состоянием оператора  $\hat{A}$ , а собственное число совпадает с собственным числом когерентного состояния, из которого получено состояние  $|\alpha, z\rangle$ . Сопряженное равенство имеет вид

$$\langle \alpha, z | \hat{A}^\dagger = \alpha^* \langle \alpha, z | \quad (9.11)$$

Исходя из соотношений (9.10) и (9.11), по аналогии с операторами  $\hat{a}$  и  $\hat{a}^\dagger$ ,  $\hat{A}$  и  $\hat{A}^\dagger$  называют операторами квазирождения и квазиуничтожения.

Остается выяснить, является ли состояние  $|\alpha, z\rangle$  сжатым состоянием? Для этого надо написать соотношение неопределенности для  $\Delta X_1$  и  $\Delta X_2$ . Имеем

$$(\Delta X_{1,2})^2 = \langle \alpha, z | \hat{X}_{1,2}^2 | \alpha, z \rangle - \langle \alpha, z | \hat{X}_{1,2} | \alpha, z \rangle^2.$$

Это выражение, используя (9.9), можно представить в виде

$$(\Delta X_{1,2})^2 = \langle \alpha | \hat{S}^\dagger(z) \hat{X}_{1,2}^2 \hat{S}(z) | \alpha \rangle - \langle \alpha | \hat{S}^\dagger(z) \hat{X}_{1,2} \hat{S}(z) | \alpha \rangle^2. \quad (9.12)$$

Операторы  $\hat{X}_{1,2}$  выражаются через  $\hat{a}$  и  $\hat{a}^\dagger$ :

$$\begin{aligned}\hat{X}_1 &= \frac{1}{2} (\hat{a} + \hat{a}^\dagger), \\ \hat{X}_2 &= \frac{1}{2i} (\hat{a} - \hat{a}^\dagger).\end{aligned}$$

Подставляя это в (9.12), преобразуя операторы  $\hat{a}$  и  $\hat{a}^\dagger$  при помощи (9.8), получим окончательное выражение для  $\Delta X_1$  и  $\Delta X_2$ : (при условии  $z = r$ , т.е.  $\theta = 0$ )

$$\begin{aligned}(\Delta X_1)^2 &= \frac{1}{4} e^{-2r}, \\ (\Delta X_2)^2 &= \frac{1}{4} e^{2r}, \\ (\Delta X_1 \Delta X_2) &= \frac{1}{4},\end{aligned}\tag{9.13}$$

где  $r = |z|$  является параметром сжатия. Из (9.13) следует, что состояние  $|\alpha, z\rangle$  действительно является сжатым состоянием для одной из квадратурных компонент. Поскольку состояние неопределенности имеет минимальное значение, состояние является идеально сжатым состоянием. Мы будем называть это состояние идеально сжатым квадратурным состоянием.

Если воздействовать оператором  $\hat{S}(z)$  на вакуумное состояние ( $\alpha = 0$ ), получим сжатое вакуумное состояние (сжатый вакуум)

$$\hat{S}(z) |0\rangle = |z, 0\rangle.$$

Среднее число фотонов в квадратурно сжатом когерентном состоянии определяется выражением:

$$\begin{aligned}\langle \alpha, z | \hat{a}^\dagger \hat{a} | \alpha, z \rangle &= \langle \alpha | \hat{S}^\dagger \hat{a}^\dagger \hat{a} \hat{S} | \alpha \rangle = \\ &= \langle \alpha | \hat{S}^\dagger \hat{a}^\dagger \hat{S} \hat{S}^\dagger \hat{a} \hat{S} | \alpha \rangle = \\ &= \langle \alpha | (\hat{a}^\dagger ch r - \hat{a} e^{-i\theta} sh r) (\hat{a} ch r - \hat{a}^\dagger e^{i\theta} sh r) | \alpha \rangle = \\ &= \left( |\alpha|^2 (ch^2 r + sh^2 r) - (\alpha^*)^2 e^{i\theta} sh r ch r - \alpha^2 sh r ch r e^{-i\theta} + sh^2 r \right).\end{aligned}\tag{9.14}$$

При выводе (9.14) мы использовали соотношение (9.8).

Сжatomу вакуумному состоянию соответствует  $\alpha = 0$ . Тогда среднее число фотонов в этом состоянии

$$\langle 0, z | \hat{a}^\dagger \hat{a} | 0, z \rangle = sh^2 r \neq 0,\tag{9.15}$$

где  $r$  - параметр сжатия.

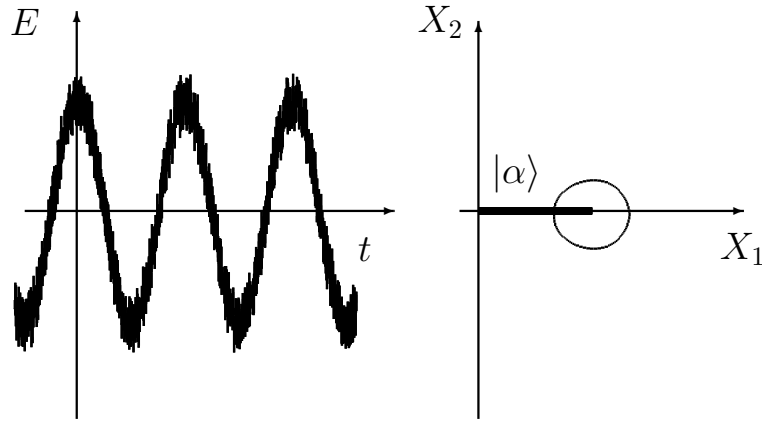


Рис. 9.1: Область неопределенности и соответствующее им зависимость электрического поля от времени для когерентного состояния. Комплексное число  $\alpha$ , соответствующее рассматриваемому состоянию  $|\alpha\rangle$  на комплексной плоскости, задаваемой  $X_1$  и  $X_2$  лежит вдоль оси  $X_1$ . В этом случае, число  $\alpha$  - вещественное, среднее значение  $\langle\alpha|\hat{X}_1|\alpha\rangle = \frac{\alpha+\alpha^*}{2} = \text{Re}\alpha = \alpha$ . Таким образом неопределенность  $\Delta X_1$  может трактоваться как неопределенность амплитуды, а  $\Delta X_2$  как неопределенность фазы. В предложенном на рис. случае когерентного (не сжатого) состояния, неопределенность по фазе и амплитуде одинаковая.

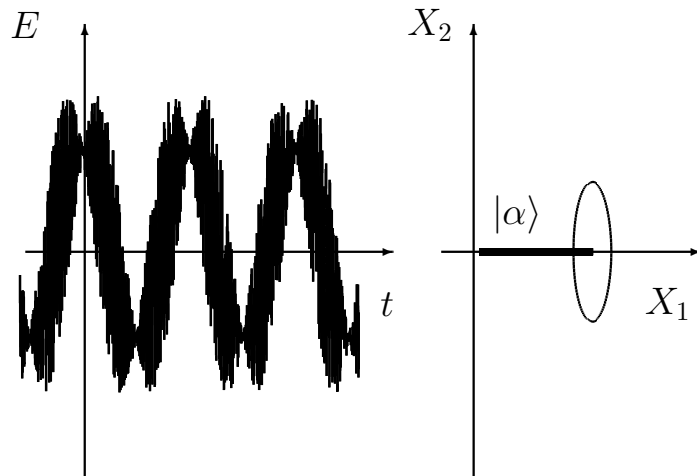


Рис. 9.2: Область неопределенности и соответствующее им зависимость электрического поля от времени для когерентного состояния сжатого по  $X_1$ . Неопределенность по амплитуде минимальна, что позволяет с высокой точностью измерять пики напряженности электрического поля.

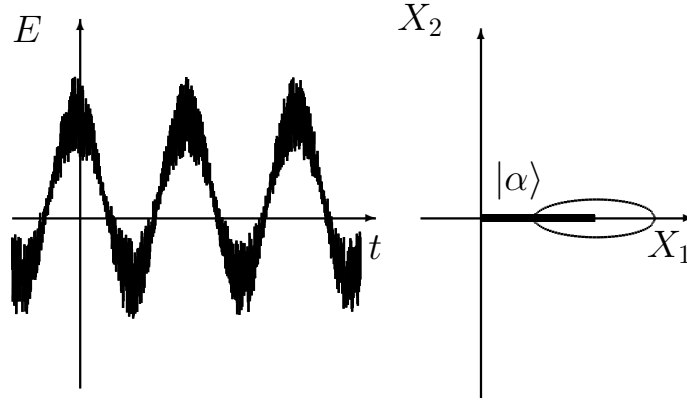


Рис. 9.3: Область неопределенности и соответствующее им зависимость электрического поля от времени для когерентного состояния сжатого по  $X_2$ . Неопределенность по фазе минимальна, что позволяет с большой точностью измерять период колебаний: значения времени в которые напряженность электрического поля равна 0.

Очевидно, что состояние сжатого вакуума не является настоящим вакуумным состоянием, т. к. может быть обнаружено фотоприемником, использующим фотоэффект, что для истинного вакуумного состояния невозможно.

Наглядно квадратурно сжатые состояния представлены на рисунках 9.1-9.3, где представлены начальные состояния и развитие колебаний во времени для различных сжатых состояний. На правых графиках изображены области неопределенности, которые имеют форму эллипса. Такую картину можно было бы увидеть, если бы мы имели что-то вроде оптического стробоскопического осциллографа, которого в действительности нет.

Рассмотрим полученные состояния более подробно. Формулу (9.9) можно написать несколько иначе, если воспользоваться представлением когерентного состояния через вакуумное в форме (1.100):

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} |0\rangle = \hat{D} |0\rangle,$$

где  $\hat{D} = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$  называют оператором смещения.  $\hat{D}$  является унитарным оператором, т. к.

$$\hat{D}^\dagger = e^{-(\alpha\hat{a}^\dagger - \alpha^*\hat{a})}$$

откуда

$$\hat{D}^\dagger \hat{D} = \hat{D} \hat{D}^\dagger = \hat{I},$$

т. е.  $\hat{D}^\dagger = \hat{D}^{-1}$ .

Название оператора связано с тем, что действие  $\hat{D}(\alpha)$  на операторы  $\hat{a}$  и

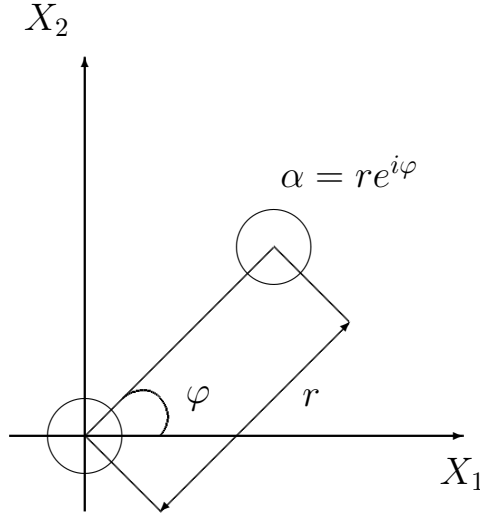


Рис. 9.4: Когерентное состояние как смещенное вакуумное состояние. Неопределенности наблюдаемых  $\hat{X}_1$  и  $\hat{X}_2$  равны:  $\Delta X_1 = \Delta X_2 = \frac{1}{2}$ .

$\hat{a}^\dagger$  приводит к их смещению на величину  $\alpha$  ( $\alpha^*$ ):

$$\begin{aligned}\hat{D}^\dagger(\alpha) \hat{a} \hat{D}(\alpha) &= \hat{a} + \alpha, \\ \hat{D}^\dagger(\alpha) \hat{a}^\dagger \hat{D}(\alpha) &= \hat{a}^\dagger + \alpha^*,\end{aligned}\tag{9.16}$$

Этот результат следует из теоремы об операторном разложении (9.6), если принять  $\hat{A} = -\alpha \hat{a}^\dagger + \alpha^* \hat{a}$ ,  $\hat{B} = \hat{a}, \hat{a}^\dagger$ .

Таким образом, когерентное состояние  $|\alpha\rangle$  является смещенным на  $\alpha$  вакуумным состоянием (см. рис. 9.4). Исходя из сказанного, можно представить сжатое состояние как результат двух действий: смещение вакуумного состояния и последующего его сжатия, как это показано на рис. 9.5.

Рассмотренная нами процедура сжатия не является единственной. Можно применить другую последовательность действий - сперва сжать вакуумное состояние, а затем сместить его, получив новое сжатое состояние (см. рис. 9.6). В операторном виде эту операцию можно представить так:

$$|\alpha, z\rangle = \hat{D}(\alpha) \hat{S}(z) |0\rangle.\tag{9.17}$$

Для различия состояний последовательность параметров здесь описана обратная по сравнению с

$$|z, \alpha\rangle = \hat{S}(z) \hat{D}(\alpha) |0\rangle.$$

Состояние (9.17) также относится к квадратурно сжатому состоянию, но между собой они не вполне совпадают. Подробно рассматривать этот случай мы здесь не будем.

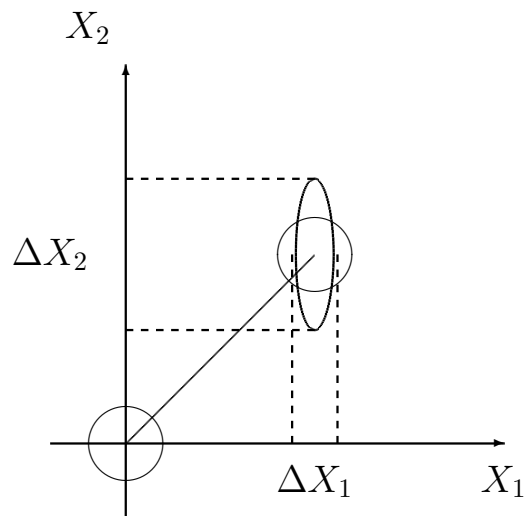


Рис. 9.5: Состояние сжатое по  $X_1$  как результат двух действий: смещение вакуумного состояния с последующим его сжатием.

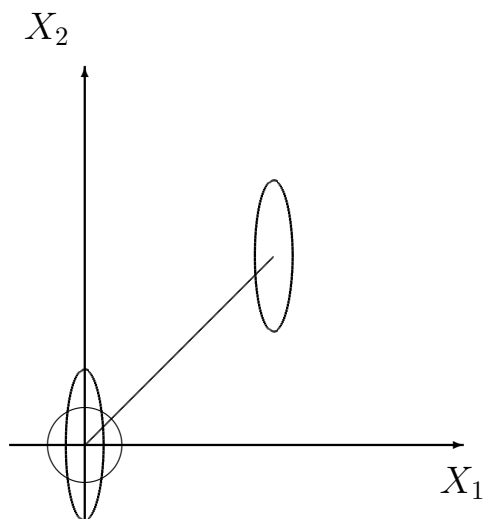


Рис. 9.6: Сжатое состояние как результат сжатия вакуумного состояния с последующим его смещением.

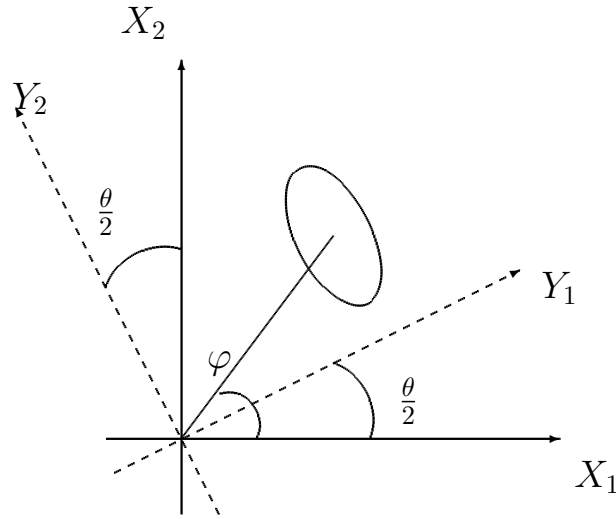


Рис. 9.7: Сжатое когерентное состояние. Ось сжатия повернута на угол  $\frac{\theta}{2}$  относительно осей  $X_1, X_2$ , а положение центра области неопределенности повернуто на угол  $\varphi$  относительно  $X_1$ .

Приведенные выше результаты и иллюстрации, изображенные на [рис. 9.1-9.3](#) получены для случая, когда параметры  $z = re^{i\theta}$  и  $\alpha = |\alpha|e^{i\varphi}$  вещественны ( $\varphi = \theta = 0$ ). Если параметры комплексные, то картинка несколько изменится (см. [рис. 9.7](#)): ось сжатия повернута на угол  $\frac{\theta}{2}$  относительно осей  $X_1, X_2$ , а положение центра области неопределенности повернуто на угол  $\varphi$  относительно  $X_1$ . Изменяя в процессе генерации и регистрации фазы действующих там световых пучков, мы можем перейти к новым квадратурам  $Y_1, Y_2$ , как это изображено на [рис. 9.7](#). Если еще компенсировать сдвиг фазы  $\varphi$ , мы перейдем к ситуации, которая изображена на рисунках [9.1-9.3](#). Из [рис. 9.7](#) видно, что измерением углов  $\theta$  и  $\varphi$  можно, например, состояние, сжатое по  $X_1$ , превратить в состояние, сжатое по  $X_2$ , и наоборот.

## 9.4 Генерация квадратурно сжатых состояний

До сих пор рассматривалась теоретическая возможность существования и генерации сжатых состояний. Возникает вопрос - в каких реальных процессах можно получить свет в сжатом состоянии? Здесь рассмотрим возможность получения квадратурно сжатого состояния при параметрическом взаимодействии, возникающем при прохождении сильного поля накачки через среду с квадратичной нелинейностью. При таком взаимодействии возникают две волны, связанные с частотой накачки соотношениями:

$$\omega_p = \omega_s + \omega_i,$$

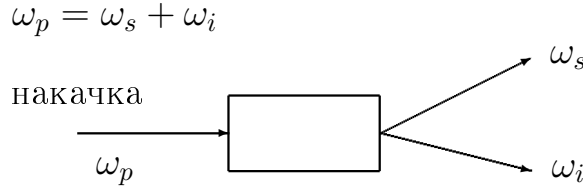


Рис. 9.8: Генерация сжатого состояния при параметрическом взаимодействии

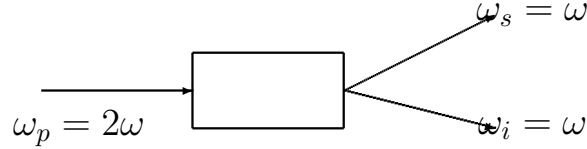


Рис. 9.9: Генерация сжатого состояния при вырожденном параметрическом взаимодействии

где  $\omega_p$  - частота накачки,  $\omega_s$  - сигнальная частота,  $\omega_i$  - холостая частота. Условно это изображено на [рис. 9.8](#).

Гамильтониан взаимодействия между накачкой, сигнальной и холостой волнами в представлении взаимодействия имеет вид:

$$\hat{V} = \hbar\kappa \left( \hat{a}_s^\dagger \hat{a}_i^\dagger \hat{b} + \hat{a}_s \hat{a}_i \hat{b}^\dagger \right), \quad (9.18)$$

где  $\hat{a}_s^\dagger$ ,  $\hat{a}_i^\dagger$ ,  $\hat{a}_s$  и  $\hat{a}_i$  - операторы рождения и уничтожения для сигнальной и холостой волны,  $\kappa$  - постоянная взаимодействия.

В вырожденном режиме сигнальная и холостая волна имеют одну и ту же частоту накачки (см. [рис. 9.9](#)):

$$\omega_s = \omega_i = \frac{\omega_p}{2} = \omega.$$

Для вырожденного параметрического процесса гамильтониан взаимодействия (9.18) упрощается:

$$\hat{V} = \hbar\kappa \left( (\hat{a}^\dagger)^2 \hat{b} + \hat{a}^2 \hat{b}^\dagger \right).$$

Если поле накачки находится в когерентном состоянии с большой амплитудой  $\alpha_p = A_p e^{i\varphi}$ ,  $|\alpha_p| \gg 1$ , накачку можно заменить классическим полем. При этом гамильтониан взаимодействия еще больше упрощается

$$\hat{V} = \hbar\kappa A_p \left( (\hat{a}^\dagger)^2 e^{-i\varphi} + \hat{a}^2 e^{i\varphi} \right),$$



где  $A_p$  и  $\varphi$  - действительная амплитуда и фаза накачки. Очевидно, что в этом приближении мы пренебрегаем истощением накачки. Это будет справедливо, пока амплитуда сигнальной (холостой) волны будет мала по сравнению с амплитудой поля накачки. Уравнение Гейзенберга для оператора  $\hat{a}$  будет иметь вид:

$$\begin{aligned}
 \frac{d\hat{a}}{dt} &= \frac{i}{\hbar} [\hat{V}, \hat{a}] = i\kappa A_p \left[ (\hat{a}^\dagger)^2 e^{-i\varphi} + \hat{a}^2 e^{i\varphi}, \hat{a} \right] = \\
 &= i\kappa A_p e^{-i\varphi} \left( (\hat{a}^\dagger)^2 \hat{a} - \hat{a} (\hat{a}^\dagger)^2 \right) = \\
 &= i\kappa A_p e^{-i\varphi} \left( (\hat{a}^\dagger)^2 \hat{a} - (\hat{a}^\dagger \hat{a} + 1) \hat{a}^\dagger \right) = \\
 &= i\kappa A_p e^{-i\varphi} (\hat{a}^\dagger \hat{a}^\dagger \hat{a} - \hat{a}^\dagger \hat{a} \hat{a}^\dagger - \hat{a}^\dagger) = \\
 &= i\kappa A_p e^{-i\varphi} \hat{a}^\dagger (\hat{a}^\dagger \hat{a} - \hat{a} \hat{a}^\dagger - 1) = i\kappa A_p e^{-i\varphi} \hat{a}^\dagger ((-1) - 1) = \\
 &= -2i\kappa A_p e^{-i\varphi} \hat{a}^\dagger.
 \end{aligned}$$

Таким образом имеем

$$\frac{d\hat{a}}{dt} = -i\Omega_p e^{-i\varphi} \hat{a}^\dagger, \quad (9.19)$$

где

$$\Omega_p = 2\kappa A_p$$

эквивалент частоты Рабби (энергия, выраженная через частоту). Аналогично

$$\frac{d\hat{a}^\dagger}{dt} = i\Omega_p e^{i\varphi} \hat{a}. \quad (9.20)$$

Исключая из системы уравнений (9.19) и (9.20)  $\hat{a}^\dagger$ , получим

$$\frac{d^2 \hat{a}(t)}{dt^2} = -i\Omega_p e^{-i\varphi} \frac{d\hat{a}^\dagger(t)}{dt} = \Omega_p^2 \hat{a}(t). \quad (9.21)$$

Начальные условия для этого уравнения имеют вид

$$\begin{aligned}
 \hat{a}(0) &= \hat{a}_0, \\
 \hat{a}^\dagger(0) &= \hat{a}_0^\dagger,
 \end{aligned}$$

откуда

$$\begin{aligned}
 \hat{a}|_{t=0} &= \hat{a}_0, \\
 \left. \frac{d\hat{a}}{dt} \right|_{t=0} &= -i\Omega_p e^{-i\varphi} \hat{a}_0^\dagger,
 \end{aligned} \quad (9.22)$$

где  $\hat{a}_0$  и  $\hat{a}_0^\dagger$  начальные значения операторов при  $t = 0$ . Решение уравнения (9.21) с учетом начальных условий (9.22) имеет вид:

$$\hat{a}(t) = \hat{a}_0 \operatorname{ch}(\Omega_p t) - i \hat{a}_0^\dagger \operatorname{sh}(\Omega_p t) e^{-i\varphi}. \quad (9.23)$$

Аналогично

$$\hat{a}^\dagger(t) = \hat{a}_0^\dagger \operatorname{ch}(\Omega_p t) + i \hat{a}_0 \operatorname{sh}(\Omega_p t) e^{i\varphi}. \quad (9.24)$$

Заметим, что при  $\varphi = \frac{\pi}{2}$  выражения (9.23) и (9.24) приводят к соотношениям (9.8):

$$\begin{aligned} \hat{a}(t) &= \hat{a}_0 \operatorname{ch}(\Omega_p t) - \hat{a}_0^\dagger \operatorname{sh}(\Omega_p t), \\ \hat{a}^\dagger(t) &= \hat{a}_0^\dagger \operatorname{ch}(\Omega_p t) - \hat{a}_0 \operatorname{sh}(\Omega_p t). \end{aligned}$$

Как мы видим, оператор  $\hat{a}(t)$  получается унитарным преобразованием (9.8) которое в нашем случае имеет вид:

$$\hat{a}(t) = \hat{S}^\dagger(t) \hat{a}(0) \hat{S}(t) = \hat{a}_0 \operatorname{ch}(\Omega_p t) - \hat{a}_0^\dagger \operatorname{sh}(\Omega_p t). \quad (9.25)$$

Таким образом, переходя от представления Гейзенберга (14.36) к представлению Шредингера (14.34), можно заключить что исходное когерентное состояние подвергается тому же унитарному преобразованию что и оператор уничтожения (9.25):

$$\hat{S}(t) |\alpha\rangle = |t, \alpha\rangle,$$

т. е. параметрическое взаимодействие эквивалентно действию оператора сжатия. В этом случае для квадратурных компонент

$$\hat{X}_1 = \frac{\hat{a} + \hat{a}^\dagger}{2}$$

и

$$\hat{X}_2 = \frac{\hat{a} - \hat{a}^\dagger}{2i}$$

будет осуществлено сжатое состояние с неопределенностями

$$\begin{aligned} (\Delta X_1)^2 &= \frac{1}{4} e^{-2\Omega_p t}, \\ (\Delta X_2)^2 &= \frac{1}{4} e^{2\Omega_p t}, \\ (\Delta X_1 \Delta X_2) &= \frac{1}{4}. \end{aligned}$$

Параметр сжатия  $r = \Omega_p t$  неограниченно растет во времени и, следовательно, степень сжатия неограниченно увеличивается. В действительности этого не

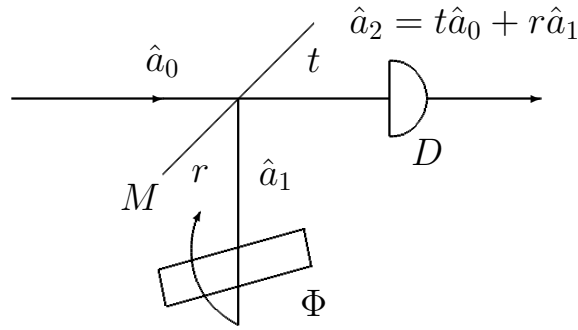


Рис. 9.10: Схема гомодинного детектора.  $M$  - зеркало с коэффициентом отражения  $r$  и коэффициентом пропускания  $t$ .  $D$  - детектор.  $\Phi$  - фазовращатель.

происходит. Неограниченное сжатие есть следствие излишней идеализации задачи: не учитывалось истощение накачки, отличие реальной накачки от монохроматического классического света и ряд других факторов. Все это приводит к ограничению степени сжатия. Чем ближе реальные условия к идеальным, тем большую степень сжатия можно получить.

Рассмотренный выше случай получения сжатого состояния за счет параметрического процесса относится к получению сжатого вакуума, т. к. генерация сжатого состояния возникает от всегда присутствующей затравки вакуумного поля. Ее иногда называют параметрическим рассеянием поля накачки. Как мы выяснили, “сжатый вакуум” не является в полном смысле вакуумным полем. Среднее число фотонов в этом поле не равно 0, а зависит от степени сжатия по формуле (9.15) и может быть при высокой степени сжатия достаточно велико.

## 9.5 Наблюдение сжатого состояния. Измерение степени сжатия

При квадратурном сжатии света флуктуации одной из квадратурных компонент могут быть существенно меньше другой. Если выделить эту компоненту и использовать ее в измерительных целях, можно ожидать сильного уменьшения шумов, ограничивающих точность измерений.

Выделение можно осуществить, используя гомодинный (синхронный) детектор. Простейшая схема гомодинного детектора изображена на рис. 9.10. Делительное зеркало имеет следующие параметры: коэффициент пропускания близок к 1 ( $t \approx 1$ ) и, следовательно,  $r \ll 1$ , т. к.  $|t|^2 + |r|^2 = 1$ . Это необходимо для того чтобы сигнал  $\hat{a}_0$  не сильно ослаблялся. При этом амплитуда гомодина, поле которого находится в когерентном состоянии  $|\alpha_H\rangle$  так велика, чтобы поле гомодина по интенсивности существенно превышало бы поле сигнала. Для работы гомодинного детектора необходимо, чтобы поле

гомодина и сигнала имели бы одинаковую частоту. Это достигается тем, что поле сигнала и поле гомодина формируются от одного заданного лазера. Например если  $\hat{a}_0$  соответствует сжатому вакууму, накачка параметрического генератора осуществляется второй гармоникой задающего лазера  $2\omega_p$ . При вырожденном параметрическом взаимодействии генерируется сигнал с частотой  $\omega_p$ , что совпадает с частотой гомодина  $\omega_p$ . Таким образом условие равенства частот соблюдается.

Оператор поля, поступающего на фотодетектор  $\hat{a}_2$ , можно выразить через операторы  $\hat{a}_0$  и  $\hat{a}_1$  - операторы поля сигнала и поля гомодина

$$\hat{a}_2 = t\hat{a}_0 + r\hat{a}_1.$$

Тогда оператор числа фотонов равен

$$\begin{aligned}\hat{a}_2^\dagger \hat{a}_2 &= (t\hat{a}_0^\dagger + r\hat{a}_1^\dagger)(t\hat{a}_0 + r\hat{a}_1) = \\ &= t^2 \hat{a}_0^\dagger \hat{a}_0 + rt(\hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0) + r^2 \hat{a}_1^\dagger \hat{a}_1.\end{aligned}$$

Положим, что гомодин находится в когерентном состоянии, а сигнал в состоянии сжатого вакуума. Тогда входное состояние будет двухмодовым

$$|\psi\rangle = |\alpha_p\rangle |r, 0\rangle.$$

Среднее значение оператора числа фотонов  $\hat{n}_2 = \hat{a}_2^\dagger \hat{a}_2$  в таком случае будет равно:

$$\begin{aligned}\langle \hat{n}_2 \rangle &= \langle \psi | \hat{a}_2^\dagger \hat{a}_2 | \psi \rangle = \\ &= t^2 \langle r, 0 | \hat{a}_0^\dagger \hat{a}_0 | r, 0 \rangle + r^2 |\alpha_p|^2 + 2tr |\alpha_p| \langle r, 0 | \hat{X}(\varphi) | r, 0 \rangle,\end{aligned}\quad (9.26)$$

где

$$\begin{aligned}\hat{X}(\varphi) &= \frac{1}{2} (\hat{a}_0 e^{-i\varphi} + \hat{a}_0^\dagger e^{i\varphi}), \\ \alpha_p &= |\alpha_p| e^{i\varphi}.\end{aligned}$$

Здесь  $\varphi$  - фаза гомодина. Тогда при  $\varphi = 0$  и при  $\varphi = \frac{\pi}{2}$  имеем

$$\begin{aligned}\hat{X}(0) &= \frac{1}{2} (\hat{a}_0 + \hat{a}_0^\dagger) = \hat{X}_1, \\ \hat{X}\left(\frac{\pi}{2}\right) &= \frac{1}{2i} (\hat{a}_0 - \hat{a}_0^\dagger) = \hat{X}_2,\end{aligned}$$

т. е. меняя фазовращателем фазу гомодина, можно выделить ту или иную квадратурную составляющие.

Равенство (9.26) содержит три члена, содержащие  $\langle \hat{a}_0^\dagger \hat{a}_0 \rangle$  - среднее число фотонов в моде сигнала,  $r^2 |\alpha_p|^2$  - среднее число фотонов в моде гомодина и интерференционный член  $\langle r, 0 | \hat{X}(\varphi) | r, 0 \rangle$ , который выделяет ту или иную квадратурные составляющие. Положим, что интенсивность гомодина настолько велика, что

$$r^2 |\alpha_p|^2 \gg \langle \hat{a}_0^\dagger \hat{a}_0 \rangle$$

тогда первым членом в (9.26) можно пренебречь. В этом случае среднее число фотонов, поступающих на фотодетектор, равно

$$\langle \hat{n}_2 \rangle = r^2 |\alpha_p|^2 + 2tr |\alpha_p| \langle r, 0 | \hat{X}(\varphi) | r, 0 \rangle,$$

где первый член является известным числом и его можно вычесть. Остается только член, содержащий квадратуру сигнала. Далее можно определить флуктуации числа фотонов (неопределенность числа фотонов), воспользовавшись формулой

$$(\Delta n_2)^2 = \langle \hat{n}_2^2 \rangle - \langle \hat{n}_2 \rangle^2.$$

Вычисления приводят к формуле

$$(\Delta n_2)^2 = r^2 |\alpha_p|^2 \left\{ r^2 + 4t^2 (\Delta X(\varphi))^2 \right\}. \quad (9.27)$$

Из (9.27) следует, что шумы содержат две составляющих, одна из которых  $r^2 |\alpha_p|^2 r^2$  - выражает шумы гомодина, вторая  $r^2 |\alpha_p|^2 4t^2 (\Delta X(\varphi))^2$  - связана с шумами сигнала. Если сигналом является вакуумное колебание

$$(\Delta X(\varphi))^2 = \frac{1}{4},$$

то условием сжатия является

$$(\Delta X_1)^2 < \frac{1}{4}$$

для сжатой компоненты.

Обнаружить эффект сжатия можно при помощи гомодинного детектора в следующем эксперименте. Сперва на входе присутствует только вакуумное состояние, при этом измеряется уровень шумов. Затем на вход подается исследуемое колебание и измеряется уровень шумов в зависимости от  $\varphi$ . Если на вход подано сжатое состояние, при некотором значении  $\varphi = \varphi^{(1)}$  шумы будут минимальными (меньшими, чем в случае вакуумных колебаний на входе). При другом значении  $\varphi = \varphi^{(2)}$ , отличающемся на  $\pi$  шумы будут максимальными (больше, чем в случае вакуумных колебаний). Подобные эксперименты проводились неоднократно. При этом обнаруживался эффект сжатия и измерялась его степень (см. например [28]).

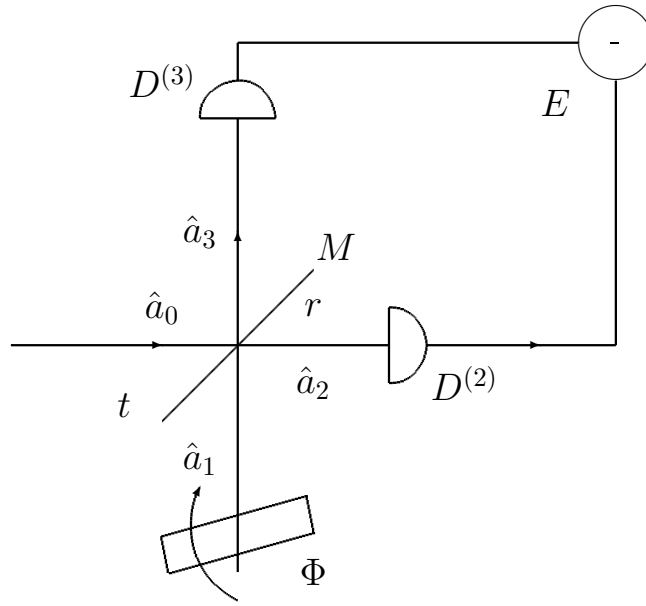


Рис. 9.11: Балансная схема гомодинного детектора. Исследуемый сигнал ( $\hat{a}_0$ ) и сигнал моды гомодина ( $\hat{a}_1$ ) подаются на зеркало  $M$  с коэффициентом отражения  $r = \frac{1}{\sqrt{2}}$  и преломления  $t = \frac{1}{\sqrt{2}}$ . Сигналы после прохождения зеркала регистрируются двумя фотодетекторами  $D^{(2)}$  и  $D^{(3)}$  выход с которых подается на вычитатель  $E$ .

### 9.5.1 Балансная схема гомодинного детектора

Более сложной схемой гомодинного приемника является балансная схема, изображенная на рис. 9.11. Она позволяет существенно уменьшить шумы гомодина. От уже рассмотренной схемы она отличается наличием двух фотоприемников, по одному для каждого выходного пучка. Сигналы, идущие с каждого фотоприемника, вычитаются, и разность фиксируется. Делительное зеркало полупрозрачное  $t = r = \frac{1}{\sqrt{2}}$  (на этот раз мы приняли, что  $t$  и  $r$  вещественны, но коэффициент отражения по разные стороны зеркала отличается знаком).

На схеме  $\hat{a}_0$  - оператор сигнала, а  $\hat{a}_1$  - оператор моды гомодина. Предполагается, что гомодин находится в когерентном состоянии с большой амплитудой. Поля мод 2 и 3 (операторы  $\hat{a}_2$  и  $\hat{a}_3$ ) детектируются отдельными фотодетекторами  $D^{(2)}$  и  $D^{(3)}$ , и сигналы, идущие с каждого фотоэлемента, вычитаются. Таким образом, на выходе сигнал определяется средним значением оператора

$$\hat{n}_{23} = \hat{a}_2^\dagger \hat{a}_2 - \hat{a}_3^\dagger \hat{a}_3.$$

Операторы  $\hat{a}_2$  и  $\hat{a}_3$  связаны делительным зеркалом с операторами входных

полей  $\hat{a}_0$  и  $\hat{a}_1$  следующими соотношениями:

$$\begin{aligned}\hat{a}_2 &= \frac{1}{\sqrt{2}} (\hat{a}_0 + \hat{a}_1), \\ \hat{a}_3 &= \frac{1}{\sqrt{2}} (-\hat{a}_0 + \hat{a}_1),\end{aligned}$$

таким образом

$$\begin{aligned}\hat{n}_{23} &= \frac{1}{2} \left( (\hat{a}_0^\dagger + \hat{a}_1^\dagger) (\hat{a}_0 + \hat{a}_1) - (-\hat{a}_0^\dagger + \hat{a}_1^\dagger) (-\hat{a}_0 + \hat{a}_1) \right) = \\ &= \frac{1}{2} \left( \hat{a}_0^\dagger \hat{a}_0 + \hat{a}_1^\dagger \hat{a}_0 + \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_1 - \left( \hat{a}_0^\dagger \hat{a}_0 - \hat{a}_1^\dagger \hat{a}_0 - \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_1 \right) \right) = \\ &= \hat{a}_0^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_0 = \left( \hat{a}_0^\dagger e^{i\varphi} + \hat{a}_0 e^{-i\varphi} \right) |\alpha_H|,\end{aligned}$$

где использовано то обстоятельство, что гомодин находится в когерентном состоянии с большой амплитудой

$$\alpha_H = |\alpha_H| e^{i\varphi},$$

и  $\hat{a}_1$  заменено на классическое поле  $|\alpha_H| e^{i\varphi}$  ( $|\alpha_H| \gg 1$ ).

Найдем среднее значение оператора  $\hat{n}_{23}$  в случае сигнала в сжатом вакуумном состоянии  $|z, 0\rangle$ , где для простоты положим  $z = r$  - вещественным ( $r = |z|$ ). Также для простоты положим  $\varphi = 0$ . В этом случае

$$\hat{n}_{23} = \left( \hat{a}_0 + \hat{a}_0^\dagger \right) |\alpha_H| = 2\hat{X}_1 |\alpha_H|.$$

Это означает, что мы рассматриваем случай сжатия квадратурной компоненты  $\hat{X}_1$ . Среднее значение оператора  $\hat{n}_{23}$  записывается в следующем виде

$$\begin{aligned}\langle \hat{n}_{23} \rangle &= 2 |\alpha_H| \langle \hat{X}_1 \rangle = |\alpha_H| \langle r, 0 | \hat{a}_0 + \hat{a}_0^\dagger | r, 0 \rangle = \\ &= |\alpha_H| \langle 0 | \hat{S}^\dagger(r) \left( \hat{a}_0 + \hat{a}_0^\dagger \right) \hat{S}(r) | 0 \rangle = \\ &= |\alpha_H| \left( \langle 0 | \hat{a}_0 c h r - \hat{a}_0^\dagger s h r | 0 \rangle + \langle 0 | \hat{a}_0^\dagger c h r - \hat{a}_0 s h r | 0 \rangle \right) = 0,\end{aligned}$$

т. к.  $\hat{a}_0 | 0 \rangle = 0$ ,  $\langle 0 | \hat{a}_0^\dagger = 0$ . Таким образом, среднее значение  $\langle \hat{n}_{23} \rangle = 0$ . Однако средний квадрат не равен 0. Он выражает шумы, ограничивающие точность измерений.

Вычислим неопределенность  $(\Delta X_{1,2})^2$ , которая определяет уровень шумов рассматриваемой балансной схемы:

$$\begin{aligned}(\Delta X_{1,2})^2 &= \langle r, 0 | \frac{1}{4} \left( \hat{a}_0 \pm \hat{a}_0^\dagger \right)^2 | r, 0 \rangle - \\ &- \langle r, 0 | \frac{1}{2} \left( \hat{a}_0 \pm \hat{a}_0^\dagger \right) | r, 0 \rangle^2.\end{aligned}\tag{9.28}$$

Поскольку мы показали, что последний член в (9.28) равен нулю, получаем:

$$\begin{aligned} (\Delta X_{1,2})^2 &= \langle 0 | \hat{S}^\dagger(r, 0) \frac{1}{4} (\hat{a}_0 \pm \hat{a}_0^\dagger)^2 \hat{S}(r, 0) | 0 \rangle = \\ &= \langle 0 | \hat{S}^\dagger(r, 0) \frac{1}{4} (\hat{a}_0 \pm \hat{a}_0^\dagger) \hat{S}^\dagger(r, 0) \hat{S}(r, 0) (\hat{a}_0 \pm \hat{a}_0^\dagger) \hat{S}(r, 0) | 0 \rangle. \end{aligned} \quad (9.29)$$

Чтобы найти  $(\Delta X_{1,2})^2$ , нужно вычислить средние:

$$\begin{aligned} \langle \hat{a}_0 \rangle &= \langle 0 | \hat{S}^\dagger(r, 0) \hat{a}_0 \hat{S}(r, 0) | 0 \rangle = \langle 0 | \hat{a}_0 \cosh r - \hat{a}_0^\dagger \sinh r | 0 \rangle = 0, \\ \langle \hat{a}_0^\dagger \rangle &= \langle 0 | \hat{a}_0^\dagger \cosh r - \hat{a}_0 \sinh r | 0 \rangle = 0, \end{aligned} \quad (9.30)$$

т. к.  $\hat{a}_0 | 0 \rangle = 0$ ,  $\langle 0 | \hat{a}_0^\dagger = 0$ .

Таким же образом можно показать

$$\begin{aligned} \langle \hat{a}_0^\dagger \hat{a}_0 \rangle &= \sinh^2 r, \\ \langle \hat{a}_0 \hat{a}_0^\dagger \rangle &= 1 + \langle \hat{a}_0^\dagger \hat{a}_0 \rangle = 1 + \sinh^2 r = \cosh^2 r, \\ \langle \hat{a}_0 \hat{a}_0 \rangle &= \langle \hat{a}_0^\dagger \hat{a}_0^\dagger \rangle^* = -\cosh r \sinh r. \end{aligned} \quad (9.31)$$

Преобразуя (9.29) при помощи (9.30) и (9.31), получим следующее выражение

$$(\Delta X_{1,2})^2 = \cosh 2r \mp \sinh 2r = e^{\mp 2r},$$

откуда

$$(\Delta n_{2,3})^2 = n_H e^{-2r}$$

для компоненты  $X_1$ . Дисперсия равна

$$\Delta n_{2,3} = \sqrt{n_H} e^{-r},$$

где  $n_H = |\alpha_H|^2$  - число фотонов в поле гомодина. При помощи балансной схемы можно измерять степень сжатия таким же образом, как и при помощи простейшей схемы гомодина. Преимущество здесь в том, что шумы самого гомодина в этом случае компенсируются и точность измерения возрастет.

## 9.6 Интерференционные измерения с применением сжатого света

Рассмотрим схему интерферометра Маха-Цендера, изображенную на рис. 9.12. Такая схема уже рассматривалась нами ранее, при исследовании погрешности интерференционных измерений. Различие в том, что на нулевой вход подается не вакуумное излучение, а излучение сжатого вакуума. Попрежнему



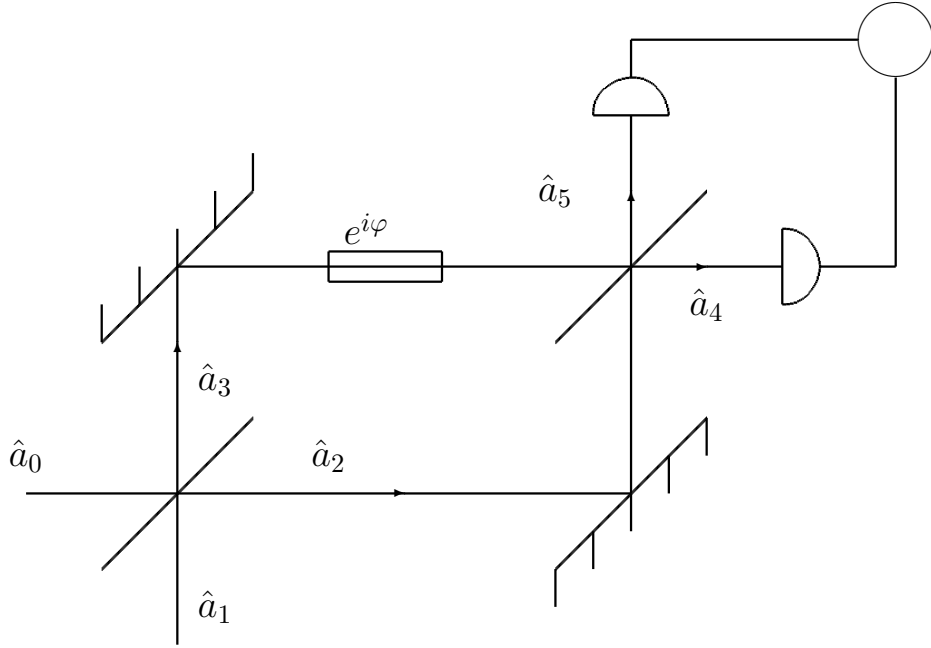


Рис. 9.12: Интерферометр Маха-Цендера

считаем, что входное и выходное зеркала полупрозрачные ( $t = r = \frac{1}{\sqrt{2}}$ ), а угловые зеркала - глухие ( $r = 1, t = 0$ ). Матрица рассеяния зеркал -

$$\hat{S} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

Интерферометр рассматриваем как датчик какой-либо физической величины, воздействующей на оптическую длину одного из плечей. На схеме включенный в верхнее плечо фазовращатель может реагировать на действие этой величины.

Уравнения интерферометра имеют вид (6.12):

$$\begin{aligned} \hat{a}_2 &= \frac{1}{\sqrt{2}} (\hat{a}_0 + i\hat{a}_1), \quad \hat{a}_3 = \frac{1}{\sqrt{2}} (i\hat{a}_0 + \hat{a}_1), \\ \hat{a}_4 &= \frac{1}{\sqrt{2}} (i\hat{a}_2 + e^{i\varphi}\hat{a}_3) = \frac{1}{2} [i(1 + e^{i\varphi})\hat{a}_0 - (1 - e^{i\varphi})\hat{a}_1], \\ \hat{a}_5 &= \frac{1}{\sqrt{2}} (\hat{a}_2 + ie^{i\varphi}\hat{a}_3) = \frac{1}{2} [(1 - e^{i\varphi})\hat{a}_0 + i(1 + e^{i\varphi})\hat{a}_1]. \end{aligned} \quad (9.32)$$

Положим, что входное поле сигнала (вход 0, оператор  $\hat{a}_0$ ) находится в состоянии сжатого вакуума. Второе входное поле (вход 1, оператор  $\hat{a}_1$ ) находится в когерентном состоянии с большой амплитудой. Настолько большой, что входное поле является двухмодовым

$$|\psi\rangle_{\text{BX}} = |\alpha\rangle |re^{i\theta}, 0\rangle,$$

где  $|\alpha\rangle$  - когерентное состояние,  $|re^{i\theta}, 0\rangle$  - состояние сжатого вакуума. Каналы 4 и 5 детектируются каждый своим фотодетектором. Сигналы, идущие с фотодетекторов, вычитаются и фиксируются.

Таким образом, выходной сигнал определяется средним значением оператора

$$\begin{aligned}\hat{n}_{54} &= \hat{a}_5^\dagger \hat{a}_5 - \hat{a}_4^\dagger \hat{a}_4 = \\ &= \left( \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_0^\dagger \hat{a}_0 \right) \cos \varphi - \left( \hat{a}_0^\dagger \hat{a}_1 - \hat{a}_1^\dagger \hat{a}_0 \right) \sin \varphi\end{aligned}\quad (9.33)$$

Здесь использовалось равенство (9.32).

Найдем среднее значение оператора  $\langle \psi | \hat{n}_{54} | \psi \rangle$ . При этом учтем, что каждый оператор действует только на свою моду. Имеем:

$$\begin{aligned}\langle \psi | \hat{n}_{54} | \psi \rangle &= \left( \langle \alpha | \hat{a}_1^\dagger \hat{a}_1 | \alpha \rangle - \langle re^{i\theta}, 0 | \hat{a}_0^\dagger \hat{a}_0 | re^{i\theta}, 0 \rangle \right) \cos \varphi - \\ &- \left( \langle re^{i\theta}, 0 | \hat{a}_0^\dagger | re^{i\theta}, 0 \rangle \alpha + \alpha \langle re^{i\theta}, 0 | \hat{a}_0 | re^{i\theta}, 0 \rangle \right) \sin \varphi.\end{aligned}\quad (9.34)$$

Первый член в первой скобке равен среднему числу фотонов накачки  $|\alpha|^2$ , а второй член, как мы знаем, равен числу фотонов в сжатом состоянии, равном  $sh^2r$ . Вторая скобка справа, как мы получили при рассмотрении балансного детектора, равна нулю. Таким образом получим

$$\langle \psi | \hat{n}_{54} | \psi \rangle = \left( |\alpha|^2 - sh^2r \right) \cos \varphi.$$

Если установить  $\varphi = \frac{\pi}{2}$ , то среднее значение выходного сигнала равно нулю:

$$\langle \psi | \hat{n}_{54} | \psi \rangle = 0.$$

Среднее значение второго члена в (9.34) равно нулю, но его средний квадрат нулю не равен. Это означает, что он является источником шумов, которые ограничивают точность измерений.

Найдем средний квадрат  $\hat{n}_{54}$ :

$$(\Delta n_{54})^2 = \langle \psi | \hat{n}_{54}^2 | \psi \rangle - \langle \psi | \hat{n}_{54} | \psi \rangle^2.$$

Среднее в нашем случае равно нулю, следовательно имеем

$$\begin{aligned}(\Delta n_{54})^2 &= \langle \psi | \hat{n}_{54}^2 | \psi \rangle = \\ &= |\alpha|^2 \langle re^{i\theta}, 0 | \left( \hat{a}_0^\dagger + \hat{a}_0 \right)^2 | re^{i\theta}, 0 \rangle = \\ &= |\alpha|^2 \langle re^{i\theta}, 0 | \left( \hat{a}_0^\dagger \right)^2 + (\hat{a}_0)^2 + \hat{a}_0^\dagger \hat{a}_0 + \hat{a}_0 \hat{a}_0^\dagger | re^{i\theta}, 0 \rangle.\end{aligned}$$

Ранее мы имели (9.30):

$$\begin{aligned}\langle \hat{a}_0 \rangle &= \langle 0 | \hat{S}^\dagger(r, 0) \hat{a}_0 \hat{S}(r, 0) | 0 \rangle = \langle 0 | \hat{a}_0 \cosh r - \hat{a}_0^\dagger \sinh r | 0 \rangle = 0, \\ \langle \hat{a}_0^\dagger \rangle &= \langle 0 | \hat{a}_0^\dagger \cosh r - \hat{a}_0 \sinh r | 0 \rangle = 0,\end{aligned}$$

откуда получим

$$(\Delta n_{54})^2 = \langle \psi | \hat{n}_{54}^2 | \psi \rangle = |\alpha|^2 (\cosh 2r - \sinh 2r) = |\alpha|^2 e^{-2r}.$$

Среднеквадратичная величина шумов будет

$$|\Delta n_{54}| = |\alpha| e^{-r}.$$

Примем эту величину за пороговое значение, ниже которого мы не сможем ни обнаружить, ни измерить сигнал. Следовательно, сигнал должен быть выше порога.

Если начальное значение  $\varphi = \frac{\pi}{2}$  изменится на величину  $\Delta\varphi$ , то появится сигнал равный

$$\Delta n_{54} = |\alpha|^2 \Delta\varphi.$$

Необходимо чтобы

$$|\alpha|^2 \Delta\varphi > |\alpha| e^{-r},$$

откуда получаем

$$\Delta\varphi > \frac{1}{|\alpha|} e^{-r}, \quad (9.35)$$

$|\alpha| = \sqrt{\bar{n}}$ , где  $\bar{n}$  - среднее число фотонов поля гомодина.

Выражение (9.35) дает меньшее значение, чем то, которое мы получим ранее, рассматривая точность интерференционных измерений. Применение сжатого состояния способно увеличить точность измерений.

## 9.7 Сжатый свет в нелинейных явлениях

Эффективность генерации высших гармоник может быть увеличена если в качестве ЭМП вместо когерентного состояния используется сжатый свет. В частности  $2N$  гармоника генерируется в  $(2N - 1)!!$  раз эффективнее [39, с. 72-76], где через

$$n!! = \prod_{k=1}^{\frac{n}{2}} (2k)$$

обозначен двойной факториал.

TBD

## 9.8 Неклассичность сжатого состояния

В заключение покажем, что сжатое состояние неклассично. Условием сжатого состояния является

$$(\Delta X_1)^2 < \frac{1}{4},$$

где

$$(\Delta X_1)^2 = \langle \hat{X}_1^2 \rangle - \langle \hat{X}_1 \rangle^2.$$

Оператор

$$\hat{X}_1 = \frac{\hat{a} + \hat{a}^\dagger}{2},$$

тогда

$$\begin{aligned} \hat{X}_1^2 &= \frac{\hat{a}^2 + (\hat{a}^\dagger)^2 + \hat{a}^\dagger \hat{a} + \hat{a} \hat{a}^\dagger}{4} = \\ &= \frac{\hat{a}^2 + (\hat{a}^\dagger)^2 + 2\hat{a}^\dagger \hat{a} + 1}{4}. \end{aligned}$$

В то же время

$$(\hat{N} \hat{X}_1^2) = \frac{\hat{a}^2 + (\hat{a}^\dagger)^2 + 2\hat{a}^\dagger \hat{a}}{4},$$

где  $\hat{N} \hat{X}_1^2$  - оператор, подвергнутый действию оператора  $\hat{N}$ , действие которого состоит в том, что устанавливается нормальная последовательность операторов  $\hat{a}^\dagger$  и  $\hat{a}$ , независимо от коммутационного соотношения.

Отсюда получим

$$(\Delta N X_1)^2 = (\Delta X_1)^2 - \frac{1}{4},$$

или

$$(\Delta N X_1)^2 < 0,$$

т. к.

$$(\Delta X_1)^2 < \frac{1}{4}.$$

Положим, что сжатое состояние описывается оператором плотности, который записан в представлении когерентных состояний

$$\hat{\rho} = \int P(\alpha) |\alpha\rangle \langle \alpha| d^2\alpha,$$

тогда для среднего значения

$$(\Delta N X_1)^2 = \langle \hat{N} \hat{X}_1^2 \rangle - \langle \hat{N} \hat{X}_1 \rangle^2 \quad (9.36)$$

можем написать

$$\begin{aligned}
 (\Delta N X_1)^2 &= \int P(\alpha) \langle \alpha | \hat{N} \hat{X}_1^2 | \alpha \rangle d^2 \alpha - \int P(\alpha) \langle X_1 \rangle^2 d^2 \alpha = \\
 &= \int P(\alpha) \left( \frac{\alpha^2 + \alpha^{*2} + 2\alpha\alpha^*}{4} - \langle X_1 \rangle^2 \right) d^2 \alpha = \\
 &= \int P(\alpha) (\Delta X_1)^2 d^2 \alpha \quad (9.37)
 \end{aligned}$$

где  $(\Delta X_1)^2$  получается из (9.36), если заменить все  $\hat{a}^\dagger$  на  $\alpha^*$ , а  $\hat{a}$  на  $\alpha$ . Можно показать, что

$$(\Delta X_1)^2 = (\Delta \alpha^* + \Delta \alpha)^2$$

величина очевидно неотрицательная. По условию сжатия интеграл должен быть меньше нуля:

$$(\Delta N X_1)^2 = \int P(\alpha) (\Delta X_1(\alpha^* \alpha))^2 d^2 \alpha < 0.$$

Это очевидно возможно, если хотя бы на части плоскости  $(\alpha)$   $P(\alpha) < 0$ . Это, как мы знаем, является условием неклассичности.

## 9.9 Когерентность второго порядка для сжатого вакуума

Посчитаем чему равна когерентность второго порядка для сжатого вакуума  $|z, 0\rangle$ . Из (8.1) имеем

$$G^{(2)} = \frac{\langle z, 0 | \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} | z, 0 \rangle - \langle n \rangle^2}{\langle n \rangle^2}.$$

Выражение  $\langle z, 0 | \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} | z, 0 \rangle$  можно переписать в виде

$$\begin{aligned}
 \langle z, 0 | \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} | z, 0 \rangle &= \\
 &= \langle 0 | \hat{a}^\dagger \hat{S} \hat{S}^\dagger \hat{a} \hat{S} \hat{S}^\dagger \hat{a}^\dagger \hat{S} \hat{S}^\dagger \hat{a} \hat{S} | 0 \rangle = \langle \phi | \phi \rangle,
 \end{aligned}$$

где

$$|\phi\rangle = \hat{S}^\dagger \hat{a}^\dagger \hat{S} \hat{S}^\dagger \hat{a} \hat{S} | 0 \rangle.$$

С помощью (9.8) можно получить

$$\begin{aligned}
 |\phi\rangle &= (\hat{a}^\dagger \text{ch } r - \hat{a} e^{-i\theta} \text{sh } r) (\hat{a} \text{ch } r - \hat{a}^\dagger e^{i\theta} \text{sh } r) | 0 \rangle = \\
 &= e^{i\theta} \text{sh } r (\hat{a}^\dagger \text{ch } r - \hat{a} e^{-i\theta} \text{sh } r) \hat{a}^\dagger | 0 \rangle = \text{sh}^2 r | 0 \rangle + \sqrt{2} e^{i\theta} \text{sh } r \text{ch } r | 2 \rangle.
 \end{aligned}$$

Т. о.

$$\langle \phi | \phi \rangle = sh^4 r + 2sh^2 r ch^2 r.$$

Следовательно, с учетом (9.15),

$$\begin{aligned} G^{(2)} &= \frac{sh^4 r + 2sh^2 r ch^2 r - sh^2 r}{sh^4 r} = 1 + 2 \frac{ch^2 r}{sh^2 r} - \frac{1}{sh^2 r} = \\ &= 1 + \frac{ch^2 r}{sh^2 r} + \frac{ch^2 r - 1}{sh^2 r} = 1 + \frac{ch^2 r}{sh^2 r} + \frac{sh^2 r}{sh^2 r} = 2 + \frac{ch^2 r}{sh^2 r} = \\ &= 2 + \frac{1 + sh^2 r}{sh^2 r} = 3 + \frac{1}{\langle n \rangle} \end{aligned}$$

## 9.10 Упражнения

1. Вывести соотношения для неопределенностей (9.2) и (9.3).
2. Вывести соотношения для неопределенностей (9.4) и (9.5).
3. Доказать (9.7) и (9.8).
4. Доказать соотношения неопределенностей (9.13).
5. Доказать выражения (9.16) для операторов смещения  $\hat{D}(\alpha)$ .
6. Доказать, что (9.23) и (9.24) являются решением уравнения (9.21) с учетом начальных условий (9.22).

## Глава 10

# Перепутанные состояния

С момента появления квантовой механики возник вопрос о полноте этой теории. Точность предсказаний квантовой механики очень велика, но при этом предсказываются только вероятности тех или иных событий. В частности, нет возможности измерить с произвольной точностью координату и импульс некоторой частицы. Кажется, что вероятности, присущие квантовомеханическому описанию, отражают его неполноту и, возможно существует другая теория, которая будет обладать точностью квантовой механики и при этом не будет использовать вероятностный подход.

Оказалось, что вероятности, лежащие в основе квантовой механики, имеют глубокий физический смысл и не существует теорий, в которых можно было бы от них отказаться, и в которых, например, было бы возможно измерять координату и импульс с произвольной точностью. Особую роль при этом приобретают так называемые перепутанные состояния, которые описывают системы, состоящие из нескольких частиц, при этом поведение такой составной системы описывается общей волновой функцией.

В силу того, что перепутанные состояния являются чисто квантовыми, т. е. не имеют классических аналогов, с их помощью имеется возможность наблюдать явления, которые кажутся совершенно невозможными с классической точки зрения, такие например, как квантовая телепортация. Кроме этого, в последнее время появились практические приложения перепутанных состояний, такие как квантовая плотная кодировка (см. [11.2.3](#)) и квантовая криптография (см. [12.3](#)).

Существует несколько способов получения перепутанных фотонов [\[62\]](#), т. е. имеющих отношение к квантовой оптике, среди которых следует выделить перепутанные по поляризации состояния. Связано это с тем, что существует большое количество способов управления поляризационными характеристиками, а также методов измерения поляризационных свойств света.

## 10.1 Парадокс ЭПР для параметров Стокса и перепутанные состояния

Рассмотрим однофотонное состояние (7.3). Для того чтобы объяснить физический смысл параметров  $\alpha$  и  $\beta$ , надо обратиться к схеме экспериментальной установки, изображенной на рис. 7.1. Предположим, что источник  $S$  излучает фотоны в состоянии (7.3). Тогда среднее значение тока фотодетектора  $D_x$  будет пропорционально  $|\alpha|^2$ , а фотодетектора  $D_y$  -  $|\beta|^2$ , т. е.  $P_x = |\alpha|^2$  и  $P_y = |\beta|^2$  описывают вероятности обнаружить фотон в состоянии поляризованном по  $x$  -  $|x\rangle$  или по  $y$  -  $|y\rangle$ . Возникает следующий вопрос - “что кроется за этими вероятностями?”. Возможны два варианта ответа. В первом из них предполагается, что на самом деле мы обладаем неполным знанием об источнике  $S$ , т. е. если бы мы знали об этом источнике все, то смогли бы предсказать, какой фотон, поляризованный по  $x$  или по  $y$ , создается в некоторый произвольный момент времени и, соответственно, показания фотодетекторов  $D_x$  и  $D_y$ . С этой точки зрения квантовая механика представляет собой некоторую промежуточную теорию, которая в дальнейшем может быть заменена на более точную, описывающую квантовые свойства объектов с абсолютной точностью.

Во втором варианте ответа предполагается, что невозможно опеределить все параметры, описывающие некоторую квантовую систему с произвольной точностью, поскольку результат измерения не предопределен заранее (как в нашем случае свойствами источника  $S$ ), а определяется в момент измерения по результатам взаимодействия квантовой системы и измерительного макроприбора.

Первая попытка дать ответ на этот вопрос была предпринята А. Эйнштейном, Б. Подольским и Н. Розеном в 1935 г. в статье которую часто называют ЭПР[5]. В ЭПР физическая теория предполагается полной, если каждый элемент физической реальности имеет отражение в физической теории. В качестве опеределения элемента физической реальности принималось следующее: “если мы можем достоверно (с вероятностью равной единице) предсказать значение некоторой физической величины, то существует элемент реальности соответствующий этой величине”[37]. Особый интерес при этом представляют некоммутирующие операторы. В нашем случае это могут быть операторы  $\hat{S}_1$  и  $\hat{S}_2$ . Так как эти операторы не коммутируют (7.5), то значения соответствующих величин не могут быть измерены с произвольной точностью. Исходя из этого можно сделать два предположения:

1. Квантово-механическое описание реальности не полно
2. Величины, определяемые операторами  $\hat{S}_1$  и  $\hat{S}_2$ , не могут быть одновре-



менно реальными

В качестве тестовой системы мы, следуя ЭПР, будем рассматривать сложную систему, состоящую из нескольких частиц. При этом для описания всей системы используется некоторая общая волновая функция.

Для описания поляризационных свойств сложной системы, состоящей из двух фотонов необходимо использовать волновую функцию следующего вида:

$$\begin{aligned} |\psi\rangle &= \sum_{i,j=x,y} c_{ij} |i\rangle_1 |j\rangle_2 = \\ &= c_{xx} |x\rangle_1 |x\rangle_2 + c_{xy} |x\rangle_1 |y\rangle_2 + c_{yx} |y\rangle_1 |x\rangle_2 + c_{yy} |y\rangle_1 |y\rangle_2. \end{aligned} \quad (10.1)$$

Если два и более коэффициентов  $c_{ij}$  в (10.1) отличны от нуля, то волновая функция не факторизуется, т. е.

$$|\psi\rangle \neq |\psi\rangle_1 |\psi\rangle_2.$$

Таким образом, каждому отдельному фотону не может быть приписана некоторая волновая функция. Такие состояния называются перепутанными.

**Комментарий 10.1.1.** Рассмотрим следующее чистое перепутанное состояние

$$|\psi_{12}\rangle = \frac{|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2}{\sqrt{2}},$$

матрица плотности которого имеет вид

$$\begin{aligned} \hat{\rho}_{12} &= |\psi_{12}\rangle \langle \psi_{12}| = \\ &= \frac{1}{2} (|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2) (\langle x|_1 \langle y|_2 - \langle y|_1 \langle x|_2) = \\ &= \frac{|x\rangle_1 |y\rangle_2 \langle y|_2 \langle x|_1 + |y\rangle_1 |x\rangle_2 \langle x|_2 \langle y|_1 -}{2} - \\ &\quad - \frac{|x\rangle_1 |y\rangle_2 \langle x|_2 \langle y|_1 + |y\rangle_1 |x\rangle_2 \langle y|_2 \langle x|_1}{2}. \end{aligned}$$

При этом матрица плотности второго фотона имеет вид (см. [разд. 14.5](#))

$$\begin{aligned} \hat{\rho}_2 &= Sp_1 \hat{\rho}_{12} = \langle x|_1 \hat{\rho}_{12} |x\rangle_1 + \langle y|_1 \hat{\rho}_{12} |y\rangle_1 = \\ &= \frac{|y\rangle_2 \langle y|_2 + |x\rangle_2 \langle x|_2}{2}. \end{aligned}$$

Т. о. состояние второго фотона является смешанным.

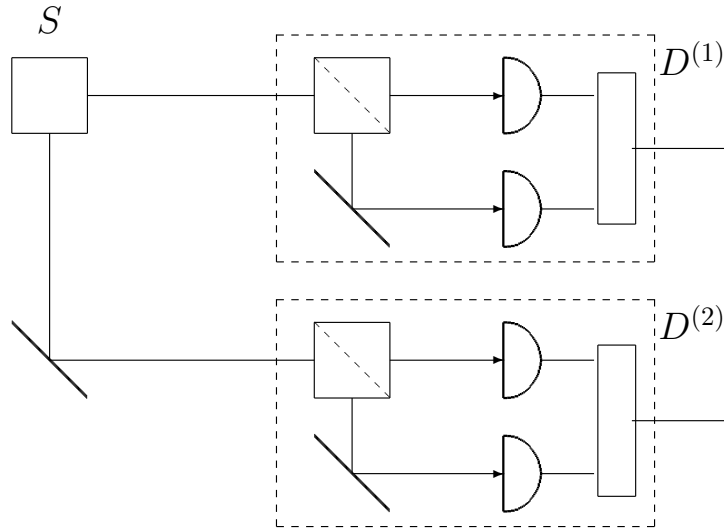


Рис. 10.1: Схема измерения параметров Стокса для перепутанного двухфотонного состояния. Источник перепутанных фотонов  $S$ . Детекторы перепутанных фотонов  $D^{(1,2)}$

Этот удивительный факт сильно отличает квантовые системы от классических: если у нас имеется чистое состояние двух частиц, то соответствующие состояния отдельных частиц не обязательно являются чистыми. В частности, если состояние Вселенной является чистым квантовым состоянием [10], то состояния отдельных частей этой Вселенной (звезды, планеты и т.п.) не обязательно являются чистыми и могут быть смешанными, т.е. классическими.

В качестве примера мы будем исследовать следующую волновую функцию:

$$|\psi\rangle = \frac{|+\rangle_1 |-\rangle_2 - |-\rangle_1 |+\rangle_2}{\sqrt{2}}, \quad (10.2)$$

т. е. все, что нам известно о фотонах - это то что они имеют разную круговую поляризацию. С вероятностью 50% первый фотон имеет левую круговую поляризацию, и в этом случае, второй фотон имеет правую круговую поляризацию. И наоборот - с вероятностью 50% первый фотон имеет правую круговую поляризацию, и в этом случае, второй фотон имеет левую круговую поляризацию.

Для измерения поляризационных свойств состояния (10.2) может быть использована схема, приведенная на рис. 10.1. В этой схеме перепутанные фотоны с источника  $S$  подаются на два детектора параметров Стокса  $D^{(1,2)}$ . Детектор  $D^{(1)}$  измеряет средние значения операторов Стокса для первого фотона -  $\hat{S}_k^{(1)}$ , а  $D^{(2)}$  - измеряет средние значения операторов Стокса  $\hat{S}_k^{(2)}$  для второго фотона. Схема каждого детектора идентична схеме, изображенной

на [рис. 7.2](#).

Так как собственные значения операторов Стокса (7.4) равны  $s = \pm 1$ , на выходе детекторов мы будем получать либо  $+1$ , либо  $-1$ . Допустим, что мы измеряем параметр Стокса  $\hat{S}_1^{(1)}$  для первого фотона. Предположим что результат измерения  $+1$ . При этом происходит редукция волновой функции (10.2). Редукция может быть описана оператором проецирования (см. [разд. 14.1.6](#)) на состояние  $|x\rangle_1$ :

$$\hat{P}_{|x\rangle_1} = |x\rangle_1 \langle x|_1,$$

при этом волновая функция (10.2) преобразуется следующим образом:

$$\begin{aligned} \hat{P}_{|x\rangle_1} |\psi\rangle &= |x\rangle_1 \langle x|_1 |\psi\rangle = \\ &= |x\rangle_1 \langle x|_1 \frac{(|x\rangle_1 + i|y\rangle_1)|-\rangle_2 - (|x\rangle_1 - i|y\rangle_1)|+\rangle_2}{2} = \\ &= |x\rangle_1 \frac{|-\rangle_2 - |+\rangle_2}{2} = -\frac{1}{2\sqrt{2}} |x\rangle_1 (2i) |y\rangle_2 = -\frac{i}{\sqrt{2}} |x\rangle_1 |y\rangle_2. \end{aligned}$$

Следовательно после измерения  $\hat{S}_1^{(1)}$  волновая функция всей системы будет записана так

$$|\psi\rangle_{red} = |x\rangle_1 |y\rangle_2.$$

Это значит, что второй фотон будет в состоянии  $|y\rangle_2$ , т. е. показание детектора  $D^{(2)}$  будет равно  $-1$ .

Аналогично, если показание первого детектора было равно  $-1$ , то волновая функция после измерения будет равна

$$\begin{aligned} P_{|y\rangle_1} |\psi\rangle &= |y\rangle_1 \langle y|_1 |\psi\rangle = \\ &= |y\rangle_1 \langle y|_1 \frac{(|x\rangle_1 + i|y\rangle_1)|-\rangle_2 - (|x\rangle_1 - i|y\rangle_1)|+\rangle_2}{2} = \\ &= |y\rangle_1 i \frac{|-\rangle_2 + |+\rangle_2}{2} = \frac{i}{2\sqrt{2}} |y\rangle_1 (2) |x\rangle_2 = \frac{i}{\sqrt{2}} |y\rangle_1 |x\rangle_2, \end{aligned}$$

т. е.

$$|\psi\rangle_{red} = |x\rangle_2 |y\rangle_1,$$

состояние второго фотона будет описываться состоянием  $|x\rangle_2$  а показание детектора  $D^{(2)}$  будет равно  $+1$ . Таким образом, при любом измерении  $\hat{S}_1^{(1)}$  мы можем достоверно (с вероятностью, равной 1) предсказать результат измерения  $\hat{S}_1^{(2)}$ , при этом прямо не воздействуя на второй фотон, т. е. величина  $\hat{S}_1^{(2)}$  должна рассматриваться как элемент физической реальности.

При этом параметры Стокса для второй частицы  $\hat{S}_1^{(2)}$  и  $\hat{S}_2^{(2)}$  имеют разные собственные вектора:  $|x\rangle_2, |y\rangle_2$  (7.8, 7.9) и  $\frac{1}{\sqrt{2}}(|x\rangle_2 \pm |y\rangle_2)$  (7.12, 7.13) соответственно. Т. о. первый и второй параметры Стокса для второй частицы не могут быть измерены одновременно, действительно в противном случае измеренному значению соответствовал бы некоторый вектор состояния, который был бы собственным для обоих операторов  $\hat{S}_1^{(2)}$  и  $\hat{S}_2^{(2)}$  (см также [разд. 14.3.3](#)).

Теперь если мы предполагаем, что результаты экспериментов предопределены заранее, т. е. не зависят от того измерения какой величины ( $S_1$  или  $S_2$ ) было выполнено, и так как измерения над первым фотоном производятся в произвольном порядке, то получается, что для второго фотона  $\hat{S}_1^{(2)}$  и  $\hat{S}_2^{(2)}$  должны быть одновременно элементами физической реальности. Это влечет за собой тезис о неполноте квантовой механики.

Мы имеем иную ситуацию, когда принимаем предположение о том, что результат некоторого измерения определяется в момент проведения этого самого эксперимента. В этом случае мы уже не можем говорить, что  $\hat{S}_1^{(2)}$  и  $\hat{S}_2^{(2)}$  должны **одновременно** рассматриваться как элементы физической реальности и соответственно нет никаких противоречий с основными принципами квантовой механики.

## 10.2 Неравенство Белла для параметров Стокса

Ответ на вопрос о полноте квантовой механики может дать следующий эксперимент [2, 62, 7].

Допустим, что рассматриваемая система состоит из двух фотонов с общей волновой функцией вида

$$|\psi\rangle = \frac{|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2}{\sqrt{2}}. \quad (10.3)$$

Пусть детектор  $D^{(1)}$  ([рис. 10.1](#)) измеряет величину

$$\hat{A} = \hat{S}_1^{(1)}, (\xi = 0)$$

или

$$\hat{A}' = \hat{S}_2^{(1)}, (\xi = \frac{\pi}{4}).$$

Как уже отмечалось ранее, собственными числами операторов  $\hat{A}$  и  $\hat{A}'$  будут  $\pm 1$ , т. е. показаниями детектора  $D^{(1)}$  могут быть только два числа:  $\pm 1$ .

Приемник  $D^{(2)}$  будет измерять следующие величины

$$\hat{B} = \frac{1}{\sqrt{2}} \left( \hat{S}_1^{(2)} + \hat{S}_2^{(2)} \right), \quad (\xi = \frac{\pi}{8})$$

или

$$\hat{B}' = \frac{1}{\sqrt{2}} \left( \hat{S}_1^{(2)} - \hat{S}_2^{(2)} \right), \quad (\xi = -\frac{\pi}{8}).$$

Для ответа на вопрос о возможных показаниях  $D^{(2)}$  необходимо найти собственные числа операторов  $\hat{B}$  и  $\hat{B}'$ . Используя матричное представление операторов  $\hat{S}_1$  (7.7) и  $\hat{S}_2$  (7.11), получим для оператора  $\hat{B}$  следующее матричное представление:

$$\hat{B} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (10.4)$$

Из (10.4) можно получить характеристическое уравнение:

$$(1 - \sqrt{2}b)(-1 - \sqrt{2}b) - 1 = 0, \quad (10.5)$$

откуда для собственных чисел имеем:  $b = \pm 1$ . В случае оператора  $\hat{B}'$  можно получить из (7.7) и (7.11) следующее матричное представление:

$$\hat{B}' = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (10.6)$$

и соответствующее ему характеристическое уравнение

$$(1 - \sqrt{2}b)(-1 - \sqrt{2}b) - 1 = 0. \quad (10.7)$$

Как нетрудно заметить, уравнение (10.7) имеет те же самые решения, что и (10.5), таким образом показаниями  $D^{(2)}$ , так же как и для  $D^{(1)}$ , будут только два значения  $\pm 1$ .

Проводятся 4 серии экспериментов по  $N$  испытаний в каждой, в которых измеряются пары операторов  $(\hat{A}, \hat{B})$ ,  $(\hat{A}', \hat{B})$ ,  $(\hat{A}, \hat{B}')$  и  $(\hat{A}', \hat{B}')$ . В результате получаются следующие наборы чисел  $(a_i, b_i)$ ,  $(a'_i, b_i)$ ,  $(a_i, b'_i)$  и  $(a'_i, b'_i)$ . Как только что было показано, каждое из полученных чисел может быть или  $+1$  или  $-1$ .

В дальнейшем из этих пар вычисляется следующее значение

$$f_i = \frac{1}{2} (a_i b_i + a'_i b_i + a_i b'_i - a'_i b'_i)$$

для которого вычисляется среднее

$$\langle F \rangle_N = \frac{1}{N} \sum_i f_i. \quad (10.8)$$

При  $N \rightarrow \infty$  можно принять

$$\langle F \rangle_N \rightarrow \langle F \rangle.$$

**Комментарий 10.2.1** (Об эксперименте Белла). Как было указано выше в эксперименте мы производим измерения следующих пар физических величин  $(\hat{A}, \hat{B})$ ,  $(\hat{A}', \hat{B})$ ,  $(\hat{A}, \hat{B}')$  и  $(\hat{A}', \hat{B}')$ , при этом для вычисления (10.8) необходимо предполагать, что все эти измерения делаются в один приём, т.е. одновременно. В классическом случае, в отличие от квантового, это допустимо. При этом с классической точки зрения  $\hat{A}$  и  $\hat{A}'$  две независимых наблюдаемые, равно как и  $\hat{B}, \hat{B}'$ . Вместе с тем, с квантовой точки зрения они уже не являются независимыми, например для  $\hat{A}, \hat{A}'$  мы имеем (7.5):

$$[\hat{A}, \hat{A}'] = 2i\hat{S}_3.$$

Кроме того, с классической точки зрения, измерения величин  $\hat{A}(\hat{A}')$  и  $\hat{B}, \hat{B}'$  так же независимы, потому что производятся в разных точках пространства. Т.о. в классическом случае 4 пары  $(\hat{A}, \hat{B})$ ,  $(\hat{A}', \hat{B})$ ,  $(\hat{A}, \hat{B}')$  и  $(\hat{A}', \hat{B}')$  являются независимыми и не важно в одном они измеряются эксперименте или в нескольких.

При этом стоит отметить, что несмотря на то что  $\hat{A}$  и  $\hat{A}'$  являются независимыми с квантовой точки зрения, мы не можем их измерить в одном эксперименте одновременно (см. [разд. 14.3.3](#)) вместе с тем, измерения в разных точках пространства связаны через общую волновую функцию, что ведет к связи величин  $\hat{A}, \hat{A}'$  с одной стороны и  $\hat{B}, \hat{B}'$  с другой и следовательно к отличающимся результатам усреднения для величины (10.8)

Квантово механический подход дает следующее выражение для среднего в рассматриваемом состоянии (10.3)

$$\begin{aligned} \langle F \rangle &\sim \langle F \rangle_{quant} = \frac{1}{2} \langle \psi | \hat{A}\hat{B} + \hat{A}'\hat{B} + \hat{A}\hat{B}' - \hat{A}'\hat{B}' | \psi \rangle = \\ &= \frac{1}{2} \langle \psi | \hat{A} (\hat{B} + \hat{B}') + \hat{A}' (\hat{B} - \hat{B}') | \psi \rangle = \\ &= \frac{1}{\sqrt{2}} \langle \psi | \hat{S}_1^{(1)} \hat{S}_1^{(2)} + \hat{S}_2^{(1)} \hat{S}_2^{(2)} | \psi \rangle = \\ &= \frac{1}{\sqrt{2}} (-1 - 1) = -\sqrt{2}. \end{aligned} \quad (10.9)$$

Если же принять тезис о неполноте квантовой механики, то мы предполагаем, что поляризация фотонов, а следовательно и параметры Стокса, определены уже сразу после выхода двух фотонов из источника  $S$ . Таким образом существуют априорные значения  $a$ ,  $a'$ ,  $b$  и  $b'$ , а свойства источника могут быть описаны с помощью классической теории вероятностей. Таким образом существует 16 элементарных вероятностей  $p(a, b, a', b')$ , так что среднее значение может быть записано следующим образом

$$\langle F \rangle \sim \langle F \rangle_{class} = \sum_{a,b,a',b'=\pm 1} p(a, b, a', b') f(a, b, a', b'), \quad (10.10)$$

где

$$\begin{aligned} f(a, b, a', b') &= \frac{1}{2} (ab + a'b + ab' - a'b') = \\ &= \frac{1}{2} (a(b + b') + a'(b - b')). \end{aligned} \quad (10.11)$$

Функция (10.11) может принимать только два значения  $f = \pm 1$ . Действительно возможны два варианта:  $b = b'$  или  $b = -b'$ . В первом случае

$$f = \frac{1}{2} (2ab) = \pm 1.$$

Во втором случае также

$$f = \frac{1}{2} (2a'b) = \pm 1.$$

Таким образом функция  $f$  может принимать значения в следующем интервале  $f_{min} = -1 \leq f \leq f_{max} = +1$  (в отличие от измеряемой величины  $f_i = 0, \pm 1, \pm 2$ ). Очевидно, что в классическом случае

$$|\langle F \rangle_{class}| \leq 1. \quad (10.12)$$

Сравнивая выражения (10.9) и (10.12), которые называют неравенствами Белла, можно увидеть, что квантовые корреляции имеют большее количественное значение. Это количественное различие может быть проверено в эксперименте. Первый эксперимент был проведен в 1972 году [7] и его результаты свидетельствуют о полноте квантового описания. Эксперимент по проверке полноты квантовой механики может иметь не только теоретический интерес, но и чисто практическое применение, например в квантовой криптографии, которую мы рассмотрим ниже (см. 12.3).

Следует отметить, что выражение (10.9) может быть получено с помощью формулы (10.10), при этом очевидно необходимо принять, что некоторые из вероятностей  $p(a, b, a', b') < 0$ . Таким образом мы можем говорить о неклассичности перепутанного состояния.

### 10.3 Базисные состояния Белла

Любое двухфотонное перепутанное состояние вида (10.1):

$$\begin{aligned} |\psi\rangle = & c_{xx} |x\rangle_1 |x\rangle_2 + c_{xy} |x\rangle_1 |y\rangle_2 + \\ & + c_{yx} |y\rangle_1 |x\rangle_2 + c_{yy} |y\rangle_1 |y\rangle_2 \end{aligned}$$

может быть разложено по следующим базисным состояниям Белла:

$$\begin{aligned} |\psi^\dagger\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 + |y\rangle_1 |x\rangle_2), \\ |\psi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2), \\ |\phi^\dagger\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |x\rangle_2 + |y\rangle_1 |y\rangle_2), \\ |\phi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |x\rangle_2 - |y\rangle_1 |y\rangle_2). \end{aligned} \quad (10.13)$$

Для доказательства разложимости нам достаточно доказать, что волновые функции (10.13) являются ортогональными. Для этого запишем каждую из этих функций в матричном виде в базисе, образованном  $|x\rangle_1 |x\rangle_2$ ,  $|x\rangle_1 |y\rangle_2$ ,  $|y\rangle_1 |x\rangle_2$  и  $|y\rangle_1 |y\rangle_2$ , в результате получим

$$\begin{aligned} |\psi^\dagger\rangle_{12} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \\ |\psi^-\rangle_{12} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \\ |\phi^\dagger\rangle_{12} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \\ |\phi^-\rangle_{12} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}. \end{aligned} \quad (10.14)$$



В случае проверки ортогональности  $|\psi^\dagger\rangle_{12}$  и  $|\psi^-\rangle_{12}$  имеем

$$\begin{aligned}\langle\psi^\dagger|_{12}\psi^-\rangle_{12} &= |\psi^\dagger\rangle_{12} = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \\ &= \frac{1}{2}(1 - 1) = 0.\end{aligned}$$

Аналогично можно доказать ортогональность остальных состояний (10.13).

Кроме этого, воспользовавшись (10.14), можно показать, что состояния (10.13) нормированы, например для  $|\psi^\dagger\rangle_{12}$  получим

$$\begin{aligned}\langle\psi^\dagger|_{12}\psi^\dagger\rangle_{12} &= |\psi^\dagger\rangle_{12} = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \\ &= \frac{1}{2}(1 + 1) = 1.\end{aligned}$$

## 10.4 Получение Белловских состояний

Для получения перепутанных состояний может быть использован процесс параметрического рассеяния света, рассмотренный нами ранее для описания процесса получения сжатых состояний электромагнитного поля (см. 9.4). Тогда нами рассматривался фазовый синхронизм I рода при котором поляризации двух фотонов одинаковы. При фазовом синхронизме второго рода поляризации фотонов различны. При этом фотоны распространяются вдоль двух конусов, как показано на рис. 10.2.

Вдоль одного конуса излучение поляризовано как обыкновенные волны, а вдоль второго как необыкновенные. Таким образом в точках пересечения конусов (см. рис. 10.3) состояние света записывается следующим образом

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 + e^{i\alpha} |y\rangle_1 |x\rangle_2),$$

где разность фаз  $\alpha$  возникает из за разности показателей преломления для обыкновенного и необыкновенного фотонов. Используя дополнительную двулучепреломляющую фазовую пластинку можно получить любое значение разности фаз  $\alpha$ , например 0 или  $\pi$ . В результате мы получим следующие

оптическая ось кристалла

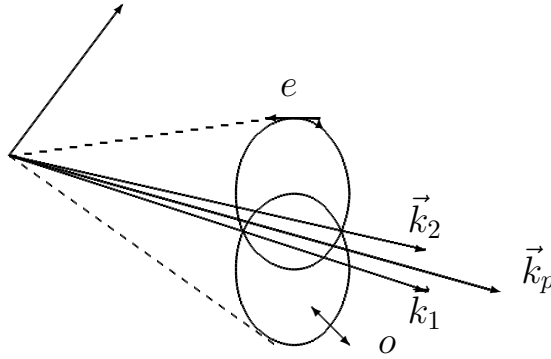


Рис. 10.2: Спонтанное параметрическое рассеяние с синхронизмом II типа.  $\vec{k}_p$  - волновой вектор накачки,  $e$  - конус, вдоль которого распространяются необыкновенно поляризованные фотоны,  $o$  - конус, вдоль которого распространяются обыкновенно поляризованные фотоны,  $\vec{k}_{1,2}$  - направления, в которых распространяются перепутанные фотоны

белловские состояния:

$$\begin{aligned} |\psi^+\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 + |y\rangle_1 |x\rangle_2), \\ |\psi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2). \end{aligned} \quad (10.15)$$

Теперь если перед одним из пучков, например первым, поместить полуволновую фазовую пластинку, которая меняет поляризацию на ортогональную:

$$|x\rangle_2 \rightarrow |y\rangle_2, \quad |y\rangle_2 \rightarrow |x\rangle_2,$$

то из (10.15) мы получим

$$\begin{aligned} |\phi^+\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |x\rangle_2 + |y\rangle_1 |y\rangle_2), \\ |\phi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |x\rangle_2 - |y\rangle_1 |y\rangle_2). \end{aligned} \quad (10.16)$$

Таким образом, объединив (10.15) и (10.16), мы получим полный базис (10.13).

## 10.5 Регистрация Белловских состояний

Из четырех базисных состояний (10.13) лишь  $|\psi^-\rangle_{12}$  является антисимметричным, т. е. меняет свой знак при перестановке частиц (фотонов). Это позволяет выделить это состояние среди всех остальных. Для этого может быть

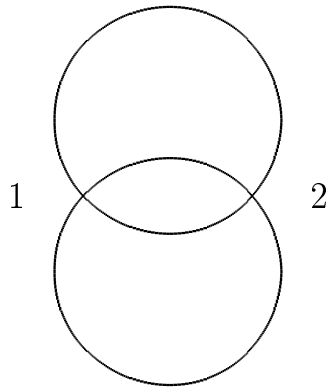


Рис. 10.3: Схематическое изображение, которое получается при фотографировании излучения, испускаемого нелинейным кристаллом. Цифрами 1 и 2 обозначены направления, в которых распространяются перепутанные фотоны.

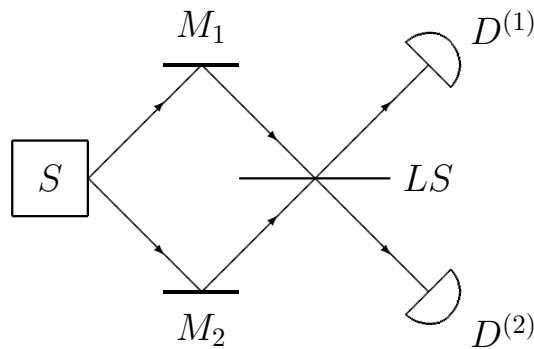


Рис. 10.4: Схема регистрации Белловских состояний.  $S$  - источник перепутанных фотонов,  $M_1$  и  $M_2$  - два глухих зеркала,  $LS$  - светоделитель,  $D^{(1)}$  и  $D^{(2)}$  - два фотодетектора

использована схема, изображенная на [рис. 10.4](#), в которой два фотона будут зарегистрированы в разных фотодетекторах только для антисимметричного состояния, для всех остальных состояний оба фотона регистрируются либо в  $D^{(1)}$ , либо в  $D^{(2)}$ .

Для доказательства рассмотрим, как действует светоделитель на однофотонное состояние. Фотон может падать на светоделитель из полуплоскости (1) ([рис. 10.5](#)), в этом случае с вероятностью 0.5 фотон окажется в полуплоскости (1), и с вероятностью 0.5 в (2). Если фотон падает из полуплоскости (2), то он опять же с равной вероятностью может оказаться в любой полуплоскости. Таким образом, для описания светоделителя мы будем пользоваться выражением для матрицы рассеяния в виде (6.4), в котором  $r = t = \frac{1}{\sqrt{2}}$ , т. е. действие светоделителя может быть выражено следующим оператором

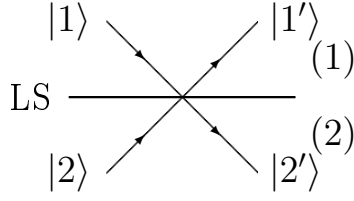


Рис. 10.5: Прохождение фотона через светоделитель

(Адамара[62]):

$$\begin{aligned}\hat{H} |1\rangle &= \frac{1}{\sqrt{2}} (|1'\rangle + |2'\rangle), \\ \hat{H} |2\rangle &= \frac{1}{\sqrt{2}} (|1'\rangle - |2'\rangle).\end{aligned}\tag{10.17}$$

В нашем случае два фотона падают с разных сторон светоделителя, следовательно возможны только две волновые функции, описывающие пространственную часть нашего начального состояния:

$$\begin{aligned}|S\rangle_{12} &= \frac{1}{\sqrt{2}} (|1\rangle_1 |2\rangle_2 + |2\rangle_1 |1\rangle_2), \\ |A\rangle_{12} &= \frac{1}{\sqrt{2}} (|1\rangle_1 |2\rangle_2 - |2\rangle_1 |1\rangle_2).\end{aligned}\tag{10.18}$$

Как видно из (10.18), состояние  $|S\rangle_{12}$  является симметричным, т. е. сохраняет свой вид при перестановке фотонов, а состояние  $|A\rangle_{12}$  - антисимметричным (меняет свой знак при перестановке фотонов).

Рассмотрим, как преобразуются состояния (10.18) при прохождении через светоделитель. В силу того, что оператор  $\hat{H}$  действует на каждый из фотонов независимо, для  $|S\rangle_{12}$  имеем

$$\hat{H} |S\rangle_{12} = |S'\rangle_{12} = \frac{1}{\sqrt{2}} \left( \hat{H} |1\rangle_1 \hat{H} |2\rangle_2 + \hat{H} |2\rangle_1 \hat{H} |1\rangle_2 \right),$$

откуда с помощью (10.17) получаем

$$\begin{aligned}
\hat{H} |S\rangle_{12} &= \frac{1}{\sqrt{2}} \left( \frac{1}{2} (|1'\rangle_1 + |2'\rangle_1) (|1'\rangle_2 - |2'\rangle_2) + \right. \\
&\quad \left. + \frac{1}{2} (|1'\rangle_1 - |2'\rangle_1) (|1'\rangle_2 + |2'\rangle_2) \right) = \\
&= \frac{1}{2\sqrt{2}} (|1'\rangle_1 |1'\rangle_2 + |2'\rangle_1 |1'\rangle_2 - |1'\rangle_1 |2'\rangle_2 - |2'\rangle_1 |2'\rangle_2 + \\
&\quad + |1'\rangle_1 |1'\rangle_2 - |2'\rangle_1 |1'\rangle_2 + |1'\rangle_1 |2'\rangle_2 - |2'\rangle_1 |2'\rangle_2) = \\
&= \frac{1}{2\sqrt{2}} (|1'\rangle_1 |1'\rangle_2 - |2'\rangle_1 |2'\rangle_2 + |1'\rangle_1 |1'\rangle_2 - |2'\rangle_1 |2'\rangle_2) = \\
&\quad \frac{1}{\sqrt{2}} (|1'\rangle_1 |1'\rangle_2 - |2'\rangle_1 |2'\rangle_2).
\end{aligned}$$

Таким образом для состояния  $|S'\rangle_{12}$  оба фотона оказываются либо в полуплоскости (1), либо в полуплоскости (2).

Для антисимметричного состояния имеем

$$\begin{aligned}
\hat{H} |A\rangle_{12} &= |A'\rangle_{12} = \frac{1}{\sqrt{2}} \left( \hat{H} |1\rangle_1 \hat{H} |2\rangle_2 - \hat{H} |2\rangle_1 \hat{H} |1\rangle_2 \right) = \\
&= \frac{1}{\sqrt{2}} \left( \frac{1}{2} (|1'\rangle_1 + |2'\rangle_1) (|1'\rangle_2 - |2'\rangle_2) - \right. \\
&\quad \left. - \frac{1}{2} (|1'\rangle_1 - |2'\rangle_1) (|1'\rangle_2 + |2'\rangle_2) \right) = \\
&= \frac{1}{2\sqrt{2}} (|1'\rangle_1 |1'\rangle_2 + |2'\rangle_1 |1'\rangle_2 - |1'\rangle_1 |2'\rangle_2 - |2'\rangle_1 |2'\rangle_2 - \\
&\quad - |1'\rangle_1 |1'\rangle_2 + |2'\rangle_1 |1'\rangle_2 - |1'\rangle_1 |2'\rangle_2 + |2'\rangle_1 |2'\rangle_2) = \\
&= \frac{1}{2\sqrt{2}} (|2'\rangle_1 |1'\rangle_2 - |1'\rangle_1 |2'\rangle_2 + |2'\rangle_1 |1'\rangle_2 - |1'\rangle_1 |2'\rangle_2) = \\
&\quad - \frac{1}{\sqrt{2}} (|1'\rangle_1 |2'\rangle_2 - |2'\rangle_1 |1'\rangle_2).
\end{aligned}$$

Таким образом в случае антисимметричного состояния после прохождения светоделителя фотоны окажутся в разных полуплоскостях.

В силу того, что фотоны являются бозонами, общая волновая функция, описывающая и поляризационные и пространственные свойства, должна быть симметричной [58] (см. разд. 14.8). Таким образом из объединения

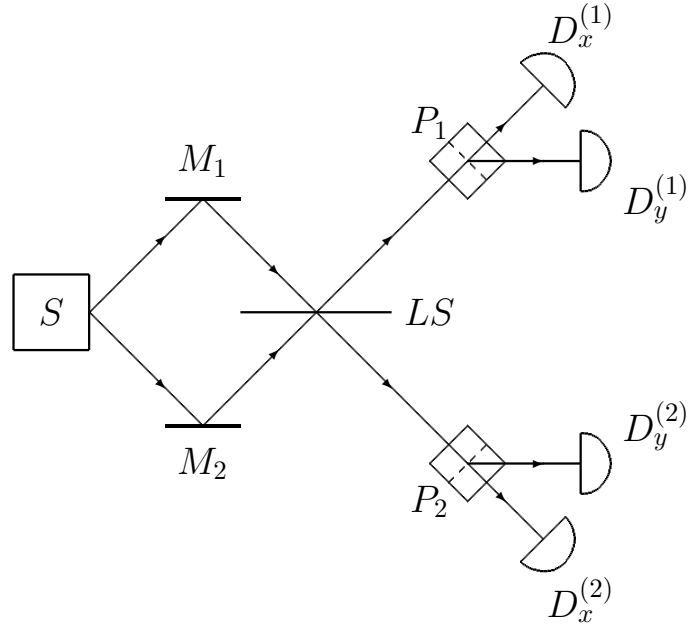


Рис. 10.6: Схема регистрации Белловских состояний.  $S$  - источник перепутанных фотонов,  $M_1$  и  $M_2$  - два глухих зеркала,  $LS$  - светоделитель,  $P_1$  и  $P_2$  - призмы Николя,  $D_x^{(1)}$  и  $D_x^{(2)}$  - фотодетекторы для  $x$  поляризации,  $D_y^{(1)}$  и  $D_y^{(2)}$  - фотодетекторы для  $y$  поляризации

(10.13) и (10.18) возможны только следующие комбинации:

$$\begin{aligned} &|\psi^{\dagger}\rangle_{12} |S\rangle_{12}, \\ &|\psi^{-}\rangle_{12} |A\rangle_{12}, \\ &|\phi^{\dagger}\rangle_{12} |S\rangle_{12}, \\ &|\phi^{-}\rangle_{12} |S\rangle_{12}. \end{aligned}$$

Следовательно в случае белловских состояний  $|\psi^{\dagger}\rangle_{12}$ ,  $|\phi^{\dagger}\rangle_{12}$  и  $|\phi^{-}\rangle_{12}$  оба фотона после прохождения светоделителя попадут в один фотодетектор, а в случае  $|\psi^{-}\rangle_{12}$  - в разные, что и позволяет нам однозначно отделить состояние  $|\psi^{-}\rangle_{12}$  от всех остальных.

Схема на рис. 10.4 может быть изменена так, чтобы она смогла регистрировать также и состояние  $|\psi^{\dagger}\rangle_{12}$ . Для этого заметим, что из всех симметричных белловских состояний только в этом фотоны имеют разную поляризацию. Таким образом это состояние может быть выделено путем измерения поляризации фотонов.

На рис. 10.6 приведена схема, которая позволяет регистрировать  $|\psi^{-}\rangle_{12}$  и  $|\psi^{\dagger}\rangle_{12}$ . Для состояния  $|\psi^{\dagger}\rangle_{12}$  одновременно сработают фотодетекторы  $D_x^{(1)}$  и  $D_y^{(1)}$  или  $D_x^{(2)}$  и  $D_y^{(2)}$ . Для  $|\psi^{-}\rangle_{12}$  -  $D_x^{(1)}$  и  $D_y^{(2)}$  или  $D_x^{(2)}$  и  $D_y^{(1)}$ . Для  $|\phi^{\dagger}\rangle_{12}$  и  $|\phi^{-}\rangle_{12}$  оба фотона будут зарегистрированы одновременно на одном из 4-х фотодетекторов. В последнее время появились работы [14] в которых была

проведена регистрация всех четырех Белловских состояний.

## 10.6 Теорема о запрете клонирования и квантовая телепортация.

В квантовой механике существует так называемая теорема о запрете клонирования [27]. Смысл этой теоремы может быть пояснен на нашем примере фотона с двумя взаимно ортогональными поляризациями, волновая функция которого задается соотношением (7.3). Теорема о запрете клонирования утверждает что невозможно создать прибор, на вход которого подается частица в состоянии (7.3), а на выходе получают две частицы в этом же состоянии.

Действительно допустим, что у нас имеется прибор, который производит клонирование состояний. Действие этого прибора на фотон, поляризованный по  $x$  будет описываться оператором клонирования  $\hat{D}$  следующим образом

$$\hat{D} |D_I\rangle |x\rangle = |D_{F_x}\rangle |x\rangle |x\rangle ,$$

где  $|D_I\rangle$  волновая функция, описывающая начальное состояние прибора для клонирования, а  $|D_{F_x}\rangle$  волновая функция, описывающая состояние прибора после клонирования фотона в вертикальной  $x$ -поляризации. Для фотона, поляризованного по  $y$ , имеем

$$\hat{D} |D_I\rangle |y\rangle = |D_{F_y}\rangle |y\rangle |y\rangle ,$$

где  $|D_{F_y}\rangle$  волновая функция, описывающая состояние прибора после клонирования этого фотона.

Если подействовать оператором клонирования  $\hat{D}$  на фотон в произвольном состоянии (7.3), получим

$$\hat{D} |D_I\rangle |\psi\rangle = \hat{D} |D_I\rangle (\alpha |x\rangle + \beta |y\rangle) = \alpha |D_{F_x}\rangle |x\rangle |x\rangle + \beta |D_{F_y}\rangle |y\rangle |y\rangle ,$$

откуда никоим образом не получить ожидаемый результат

$$\hat{D} |D_I\rangle |\psi\rangle = |D_{F_{xy}}\rangle (\alpha |x\rangle + \beta |y\rangle) (\alpha |x\rangle + \beta |y\rangle) .$$

Но если состояние фотона нельзя клонировать, то оказывается, что его можно передать из одной точки пространства в другую (естественно, с разрушением исходного состояния), что демонстрируют эксперименты по квантовой телепортации.

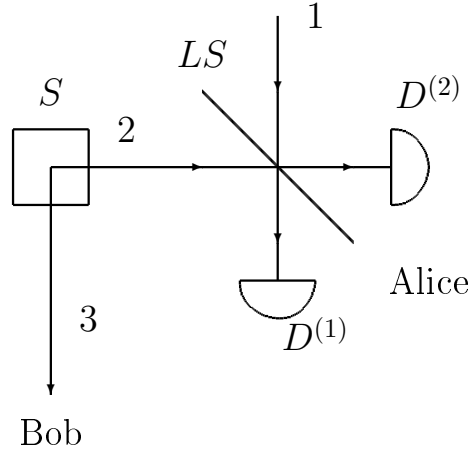


Рис. 10.7: Схема протокола квантовой телепортации.  $S$  источник перепутанных пар фотонов,  $LS$  - светоделитель,  $D^{(1)}$  и  $D^{(2)}$  - два фотодетектора, 1 - телепортируемый фотон, 2 и 3 - пара перепутанных фотонов.

Схема протокола квантовой телепортации представлена на [рис. 10.7](#). На этом рисунке Алиса хочет передать Бобу состояние фотона 1, которое описывается волновой функцией (7.3).

$$|\psi\rangle_1 = \alpha |x\rangle_1 + \beta |y\rangle_1,$$

Имеется также источник перепутанных фотонов  $S$ , который излучает пары фотонов 2 и 3 в состоянии, описываемом следующей волновой функцией

$$|\psi\rangle_{23} = |\psi^-\rangle_{23} = \frac{1}{\sqrt{2}} (|x\rangle_2 |y\rangle_3 - |y\rangle_2 |x\rangle_3).$$

Алиса смешивает фотоны 1 и 2 на светоделителе  $LS$  и в дальнейшем регистрирует некоторое Белловское состояние с помощью детекторов  $D^{(1,2)}$ . Проще всего произвести регистрацию состояния  $|\psi^-\rangle_{12}$ , в котором оба фотодетектора должны сработать одновременно.

Общее состояние трех частиц записывается в виде

$$|\psi\rangle_{123} = |\psi\rangle_1 |\psi\rangle_{23},$$

который может быть разложен по Белловским состояниям фотонов 1 и 2:

$$\begin{aligned} |\psi\rangle_{123} = & c_{|\psi^\dagger\rangle_{12}} |\psi^\dagger\rangle_{12} + c_{|\psi^-\rangle_{12}} |\psi^-\rangle_{12} + \\ & + c_{|\phi^\dagger\rangle_{12}} |\phi^\dagger\rangle_{12} + c_{|\phi^-\rangle_{12}} |\phi^-\rangle_{12}. \end{aligned} \quad (10.19)$$

В разложении (10.19) нас будет интересовать коэффициент  $c_{|\psi^-\rangle_{12}}$ , так как именно он будет описывать состояние третьего фотона при регистрации Али-



сой Белловского состояния  $|\psi^-\rangle_{12}$ . Для искомого коэффициента получим:

$$\begin{aligned} c_{|\psi^-\rangle_{12}} &= \langle \psi^- |_{12} \psi \rangle_{123} = \\ &= \frac{1}{\sqrt{2}} (\langle x|_1 \langle y|_2 - \langle y|_1 \langle x|_2) (\alpha |x\rangle_1 + \beta |y\rangle_1) \frac{1}{\sqrt{2}} (|x\rangle_2 |y\rangle_3 - |y\rangle_2 |x\rangle_3) = \\ &= \frac{1}{2} (\alpha \langle y|_2 - \beta \langle x|_2) (|x\rangle_2 |y\rangle_3 - |y\rangle_2 |x\rangle_3) = -\frac{1}{2} (\alpha |x\rangle_3 + \beta |y\rangle_3). \end{aligned}$$

Это значит, что всякий раз, когда Алиса регистрирует пару фотонов 1 и 2 в состоянии  $|\psi^-\rangle_{12}$ , т. е. когда оба детектора  $D^{(1)}$  и  $D^{(2)}$  срабатывают одновременно, фотон 3 на стороне Боба оказывается в состоянии, идентичном состоянию исходного фотона 1, т. е. произойдет телепортация фотона 1 к Бобу.

## 10.7 Квантовые псевдотелепатические игры

Неклассичность перепутанных состояний может быть ярко продемонстрирована в так называемых квантовых псевдотелепатических играх [4, 1]

### 10.7.1 Описание игры

Рассмотрим игру Мермина-Переса (Mermin-Peres) в которой два игрока, Алиса и Боб, играют против казино. Алиса и Боб заполняют числами  $\pm 1$  квадрат  $3 \times 3$ . Казино говорит Алисе номер строки которую Алиса должна заполнить, а Бобу номер столбца. У Алисы произведение всех цифр должно быть равным  $+1$ , а у Боба  $-1$ . Игроки выигрывают если число на пересечении строки и столбца совпало. Проигрывают в противном случае.

Алиса и Боб изолируются друг от друга до того момента как они получают от казино номер строки и столбца, соответственно. Т. о. договорится о стратегии игры они могут только до этого момента.

**Пример 10.7.1** (Игра Мермина-Переса). *Допустим Алиса (A) получила номер строки 1, а Боб (B) номер столбца 3. В этом случае выигрышная комбинация может выглядеть следующим образом*

$$A = \begin{pmatrix} +1 & -1 & -1 \\ * & * & * \\ * & * & * \end{pmatrix},$$

$$B = \begin{pmatrix} * & * & -1 \\ * & * & +1 \\ * & * & +1 \end{pmatrix}.$$

Комбинация является выигрышной потому что и у Алисы и у Боба на пересечении выбранных строки и столбца стоит одно и то же число  $-1$ .

В противном случае (строка 1, столбец 1)

$$A = \begin{pmatrix} +1 & -1 & -1 \\ * & * & * \\ * & * & * \end{pmatrix},$$

$$B = \begin{pmatrix} -1 & * & * \\ +1 & * & * \\ +1 & * & * \end{pmatrix},$$

игроки проиграют, поскольку Алиса получает на пересечении  $+1$ , а Боб  $-1$ .

### 10.7.2 Классическая стратегия

В классической стратегии Алиса и Боб не смогут договориться о всех элементах матрицы поскольку условия Боба и Алисы будут конфликтовать друг с другом: по условиям Алисы произведение всех элементов матрицы будет равняться  $(+1)^3 = 1$ , а по условиям Боба -  $(-1)^3 = -1$ . Т. о. иногда Алиса и Боб выигрывают, но всегда будут игры в которых они проиграют, поскольку вероятность выигрыша  $p < 1$ .

### 10.7.3 Квантовая стратегия

Как мы выяснили классической стратегии не существует, но с другой стороны, если Алиса и Боб смогут заранее создать некоторое перепутанное состояние и договориться о тех измерениях которые они будут проводить над этим состоянием<sup>1</sup>, то существует способ обеспечить выигрыш с вероятностью  $p = 1$ .

Перепутанное состояние используемое Алисой и Бобом:

$$|\psi\rangle = |\psi\rangle_{A_1, B_1} \otimes |\psi\rangle_{A_2, B_2}$$

Матрица используемая для измерений

$$X = \begin{pmatrix} \hat{S}_0 \otimes \hat{S}_3 & \hat{S}_3 \otimes \hat{S}_0 & \hat{S}_3 \otimes \hat{S}_3 \\ \hat{S}_1 \otimes \hat{S}_0 & \hat{S}_0 \otimes \hat{S}_1 & \hat{S}_1 \otimes \hat{S}_1 \\ -\hat{S}_1 \otimes \hat{S}_3 & -\hat{S}_3 \otimes \hat{S}_1 & \hat{S}_2 \otimes \hat{S}_2 \end{pmatrix} \quad (10.20)$$

---

<sup>1</sup> естественно измерения проводятся Алисой и Бобом отдельно друг от друга, каждым в своей лаборатории

В силу того, что

$$\hat{S}_1^2 = \hat{S}_2^2 = \hat{S}_3^2 = \hat{S}_0^2 = \hat{I}$$

для каждого элемента  $\hat{x}_{ij}$  матрицы (10.20) имеем  $\hat{x}_{ij}^2 = \hat{I}$  и следовательно при измерении мы получаем в качестве значений собственные числа  $\pm 1$ .

Кроме этого Алиса и Боб могут проводить измерения, т.к. операторы в одной строке или в одном столбце коммутируют, т.е. могут быть измерены одновременно. При этом значения которые получает Алиса подчиняются требованиям налагаемым на строку, а Бобом на столбец.

И наконец, измерения проводимые Алисой и Бобом для совпадающей позиции также совпадут. Это следует из следующего соотношения

$$(\hat{x}_{ij}^A \otimes \hat{x}_{ij}^B) |\psi\rangle = |\psi\rangle,$$

где  $\hat{x}_{ij}^A$  измерение Алисы, а  $\hat{x}_{ij}^B$  измерение Боба. Таким образом произведение результатов получаемых Алисой и Бобом будет равно 1, или же в силу того что результатом может быть только  $\pm 1$ , результаты Алисы и Боба совпадут.

TBD

## 10.8 Упражнения

1. Доказать ортонормированность базисных Белловских состояний (10.13).
2. Какое Белловское состояние должна регистрировать Алиса, в схеме изображенной на рис. 10.7, для подтверждения факта телепортации в случае когда источник перепутанных пар фотонов  $S$  производит фотоны в состоянии

$$|\psi\rangle_{23} = |\psi^\dagger\rangle_{23} = \frac{1}{\sqrt{2}} (|x\rangle_2 |y\rangle_3 + |y\rangle_2 |x\rangle_3).$$

3. Получить выражения для коэффициентов  $c_{|\psi^\dagger\rangle_{12}}$ ,  $c_{|\phi^\dagger\rangle_{12}}$  и  $c_{|\phi^-\rangle_{12}}$  в разложении (10.19)



## Часть 4

# Квантовая теория информации



## Глава 11

# Введение в квантовую теорию информации

Классическая теория информации была разработана Клодом Шеноном [20] в применении к задачам теории связи и в данный момент находит все большее применение. В этом разделе мы рассмотрим основные понятия и результаты теории информации, в том числе в применении ее к квантовым явлениям.

### 11.1 Информация и энтропия

Само понятие информации тесно связано с мерой неопределенности системы, т. е. тем, что в статистической физике называется энтропией. Чем более неупорядочена система, тем меньше информации нам о ней известно. Приобретение информации уменьшает меру неопределенности. Соответственно, чем более неупорядочена была исходная система, тем больше информации мы о ней приобретаем в результате исхода некоторого опыта. Таким образом в качестве меры информации можно взять сложность (неопределенность) системы. Следуя в дальнейшем Шенону мы будем эту меру называть энтропией, при этом мы не будем делать различия между “мерой количества информации” и “энтропией”, т. е. будем считать эти понятия синонимами.

#### 11.1.1 Энтропия в классической теории информации

Определение понятия энтропии мы начнем с опыта с равновероятными исходами. Допустим у нас имеется некоторое событие  $\mathcal{A}$ , которое имеет  $a$  равновероятных исходов. В качестве энтропии (меры неопределенности) разумно использовать некоторую положительную функцию, которая будет зависеть

от числа исходов  $a$  и будет возрастать с ростом  $a$ :

$$H_{\mathcal{A}} = f(\mathcal{A}) = f(a).$$

При этом разумно предположить, что  $f(1) = 0$ , т. к. результат опыта с одним возможным значением полностью определен.

Рассмотрим теперь еще один опыт  $\mathcal{B}$  с числом исходов  $b$ . Очевидно, что для него справедливо соотношение

$$H_{\mathcal{B}} = f(b).$$

Если же рассмотреть событие  $\mathcal{AB}$ , которое состоит в одновременном выполнении событий  $\mathcal{A}$  и  $\mathcal{B}$ , то число равновероятных исходов такого события есть величина  $a \cdot b$ , т. е. можно записать

$$H_{\mathcal{AB}} = f(ab).$$

С другой стороны хотелось бы выразить  $H_{\mathcal{AB}}$  через  $H_{\mathcal{A}}$  и  $H_{\mathcal{B}}$ . Для этого вспомним свойство роста энтропии с ростом сложности системы, т. е. справедливо следующее неравенство

$$H_{\mathcal{AB}} \geq H_{\mathcal{A}}, H_{\mathcal{B}}. \quad (11.1)$$

Если для искомой связи использовать только 4 простейшие арифметические операции, то только сложение и умножение будут удовлетворять свойству (11.1). При этом если рассмотреть ситуацию, когда число исходов события  $\mathcal{B}$  равно 1, то окажется, что для искомой связи может быть использована только операция сложения:

$$H_{\mathcal{AB}} = H_{\mathcal{A}} + H_{\mathcal{B}},$$

откуда

$$f(ab) = f(a) + f(b).$$

Соберем теперь вместе те сведения, которые нам известны про искомую функцию  $f$

$$\begin{aligned} f(1) &= 0, \\ f(a) &> f(b), \text{ если } a > b, \\ f(ab) &= f(a) + f(b). \end{aligned} \quad (11.2)$$

Существует только одна непрерывная функция, которая удовлетворяет требованиям (11.2) (доказательство см. [30]):

$$f(a) = K \log a. \quad (11.3)$$



Коэффициент  $K$  в (11.3) определяет показатель логарифма и величину единицы измерения информации. Например если мы используем в качестве единицы измерения энтропию опыта с двумя равновероятными исходами (например выпадения “орла” или “решки” при бросании монеты), то в формуле (11.3) используется логарифм по основанию 2:

$$f(a) = \log_2 a, \quad (11.4)$$

а соответствующая единица измерения информации называется **бит**<sup>1</sup>. Выбор этой единицы при измерении количества информации объясняется тем, что часто информация кодируется с помощью объектов, которые имеют только два стабильных состояния (например, превышает сигнал некоторый уровень или нет). Наряду с логарифмом по основанию 2 в (11.3) часто используется натуральный логарифм:

$$f(a) = \ln a, \quad (11.5)$$

соответствующая единица измерения информации называется **нат**. В дальнейшем мы будем использовать определение энтропии в форме (11.3) при этом основание логарифма будет приниматься равным 2.

Выражение (11.3) получено нами в предположении равновероятных исходов. Как известно, вероятность события  $\mathcal{A}$  определяется как

$$p_{\mathcal{A}} = \frac{1}{a},$$

откуда энтропия  $H_{\mathcal{A}}$  может быть записана как

$$H_{\mathcal{A}} = -\log p_{\mathcal{A}}. \quad (11.6)$$

Рассмотрим теперь случай, когда событие  $\mathcal{A}$  имеет не равновероятные исходы. В этом случае каждому исходу  $\xi$  события  $\mathcal{A}$  следует сопоставить вероятность этого исхода  $p_{\xi}$ . Для определения меры количества информации, которое мы приобретем при реализации исхода  $\xi$ , мы будем попрежнему использовать выражение (11.6):

$$H_{\xi} = -\log p_{\xi}. \quad (11.7)$$

Величина  $H_{\xi}$  в (11.7) является характеристикой только одного конкретного исхода события  $\xi$  и, соответственно, не может быть использована в качестве меры неопределенности всего события  $\mathcal{A}$ . В качестве такой меры разумно использовать усредненное значение энтропии:

$$H_{class} = H_{\mathcal{A}} = \sum_{\xi} -p_{\xi} \log p_{\xi}. \quad (11.8)$$

---

<sup>1</sup>от англ. **binary digit** - двоичный разряд

В выражении (11.8) принимается что

$$0 \cdot \log 0 = 0. \quad (11.9)$$

Несмотря на кажущуюся условность ввода (11.8), это выражение действительно описывает количество информации, в частности, живые организмы обрабатывают информацию со скоростью которая пропорциональна (11.8). В [30] описаны эксперименты по скорости реакции человека на внешний раздражитель. В качестве раздражителя выступала одна из нескольких лампочек, каждая из которых загоралась с разной частотой. Перед экспериментом экзаменуемым давалось время на тренировку, после которой оказывалась, что скорость реакции определяется именно выражением (11.8).

Энтропия (11.8) обладает следующим свойством:

$$H_{min} \leq H_A \leq H_{max}, \quad (11.10)$$

при этом  $H_{min} = 0$  и достигается в случае, когда вероятность одного из исходов события  $\mathcal{A}$  равна 1, а остальных 0 (минимальная неопределенность системы).  $H_{max} = \log a$  и достигается, когда все исходы равновероятны (максимальная неопределенность системы).

### 11.1.2 Энтропия в квантовых системах

Аналогом распределения вероятностей  $\{p_\xi\}$  в квантовом случае служит матрица плотности  $\hat{\rho}$ . При этом в качестве усреднения используется операция взятия следа в некотором базисе. То есть выражению (11.8) в квантовых системах соответствует:

$$H_{quant} = -Sp(\hat{\rho} \log \hat{\rho}). \quad (11.11)$$

При анализе соотношения (11.11) возникают следующие вопросы:

- Как считать энтропию (11.11)
- В каких случаях энтропия будет максимальна и в каких минимальна, т. е. каким будет квантовый аналог классического выражения 11.10.

Для ответа на первый вопрос вспомним что операция взятия следа не зависит от представления (см. разд. 14.1.7), поэтому достаточно рассмотреть матрицу плотности в том базисе, в котором она имеет диагональное представление. Если обозначить через  $\rho_{nn}$  диагональный элемент матрицы плотности, то с помощью (14.27) можно будет переписать (11.11) следующим образом

$$H_{quant} = -Sp(\hat{\rho} \log \hat{\rho}) = -\sum_n \rho_{nn} \log \rho_{nn}. \quad (11.12)$$

Начнем анализ выражения (11.12) с рассмотрения случая чистых состояний. Если взять произвольное чистое состояние  $|\psi\rangle$ , записанное в некотором базисе  $\{|n\rangle\}$ :

$$|\psi\rangle = \sum_n c_n |n\rangle,$$

то всегда можно найти такой базис  $\{|m\rangle\}$ , в котором  $|\psi\rangle$  будет одним из базисных состояний, например первым:

$$|\psi\rangle = \sum_m c_m |m\rangle = |m\rangle|_{m=1},$$

таким образом, в диагональной матрице плотности останется только один не нулевой член  $\rho_{11} = 1$ , и энтропия будет равна

$$H_{pure} = 0, \quad (11.13)$$

при этом мы использовали выражение (11.9). Это выражение говорит нам о том, что чистое состояние является полностью определенным.

Если рассматривать смешанное состояние, то матрица плотности будет диагональной, при этом сами диагональные элементы будут равны вероятностям нахождения системы в соответствующем состоянии:

$$\rho_{nn} = p_n.$$

Если теперь воспользоваться (11.12), то можно получить, что выражение для энтропии смешанного состояния совпадает с классическим выражением энтропии (11.8):

$$H_{misc} = - \sum_n p_n \log p_n = H_{class}, \quad (11.14)$$

которое, как уже указывалось ранее, максимально при равномерном распределении вероятностей и минимально при вырожденном (когда один из исходов имеет вероятность 1, а остальные 0).

Наряду с выражениями (11.12) и (11.14), в которых единицей измерения количества информации является нат удобно использовать логарифм с основанием два - в этом случае единица измерения будет называться кубит (quantum bit).

## 11.2 Передача информации. Канал связи.

Такие общие характеристики информации как энтропия не учитывают самого конкретного содержания информации, которое также может быть



Рис. 11.1: Передача информации. Канал связи

важно, и соответственно, могут быть применены не всегда. Вместе с тем существуют ситуации, когда конкретное значение не важно, а имеет значение именно количество информации. В качестве примера таких систем можно рассмотреть системы передачи информации.

### 11.2.1 Классический канал связи

Типичная система передачи информации изображена на [рис. 11.1](#). Как видно из этого рисунка, прежде чем информация будет передана, она должна быть закодирована, т. е. представлена в тех состояниях, которые могут быть переданы через канал. На выходе канала информация должна быть раскодирована, т. е. преобразована в ту форму, которая использовалась на входе.

Наиболее удобным представляется кодирование информации классическими объектами, которые имеют всего два стабильных состояния (например превышение или нет мощностью сигнала некоторого порога). Очевидно, что классические состояния выбираются таким образом, чтобы их можно было легко детектировать.

### 11.2.2 Квантовый канал связи

Использование для передачи информации квантовых объектов значительно расширяет возможности канала связи, потому как у квантовой системы имеется гораздо больший выбор состояний, которые могут быть использованы для передачи информации.

Вместе с тем и сам канал связи в квантовом случае характеризуется некоторыми особыми свойствами. В качестве примера можно рассмотреть передачу информации, которая кодируется с помощью чистых квантовых состояний. Как уже указывалось ранее (см. [10.6](#)), произвольное квантовое состояние не может быть копировано, откуда вытекает, что в такой системе, в отличие

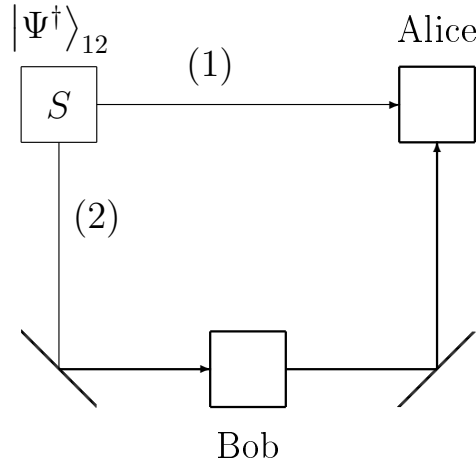


Рис. 11.2: Протокол квантовой плотной кодировки

от классического канала связи, невозможна не только подмена информации, но даже ее несанкционированное чтение. Это имеет особое значение для защиты информации.

### 11.2.3 Квантовая плотная кодировка

В качестве примера квантового канала связи рассмотрим протокол квантовой плотной кодировки, предложенный Беннетом и Виснером [3], [6]. В этом протоколе используется перепутанное по поляризации двухфотонное состояние, рассмотренное нами ранее (см. [гл. 10](#)).

Каждый из фотонов по отдельности имеет два ортогональных состояния  $|x\rangle_{1,2}$  и  $|y\rangle_{1,2}$ . Таким образом с классических позиций с помощью этих двух фотонов можно закодировать четыре бита информации, для этого можно использовать следующие состояния:  $|x\rangle_1 |x\rangle_2$ ,  $|x\rangle_1 |y\rangle_2$ ,  $|y\rangle_1 |x\rangle_2$ , и  $|y\rangle_1 |y\rangle_2$ .

В протоколе квантовой плотной кодировки тоже можно закодировать 4 бита информации, но при этом оперируя *только одним* из двух фотонов. Схема этого протокола изображена на [рис. 11.2](#). Источник  $S$  производит пару перепутанных фотонов в некотором белловском состоянии, например  $|\Psi^\dagger\rangle_{12}$ . Первый фотон из этой пары отсылается Алисе, а второй Бобу. Изменяя свойства своего (второго) фотона, Боб преобразует исходное состояние к одному

из 4 белловских состояний (10.13):

$$\begin{aligned} |\psi^\dagger\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 + |y\rangle_1 |x\rangle_2), \\ |\psi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2), \\ |\phi^\dagger\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |x\rangle_2 + |y\rangle_1 |y\rangle_2), \\ |\phi^-\rangle_{12} &= \frac{1}{\sqrt{2}} (|x\rangle_1 |x\rangle_2 - |y\rangle_1 |y\rangle_2). \end{aligned} \quad (11.15)$$

В случае состояния  $|\Psi^\dagger\rangle_{12}$  никаких дополнительных действий не требуется, т. к. оно является исходным:

$$|y\rangle_2 \rightarrow |y\rangle_2, |x\rangle_2 \rightarrow |x\rangle_2. \quad (11.16)$$

Для получения состояния  $|\psi^-\rangle_{12}$  Боб должен произвести зависимый от поляризации фазовый сдвиг:

$$|y\rangle_2 \rightarrow |y\rangle_2, |x\rangle_2 \rightarrow e^{i\pi} |x\rangle_2. \quad (11.17)$$

В случае состояния  $|\phi^\dagger\rangle_{12}$  Боб производит изменение поляризации на ортогональное

$$|y\rangle_2 \rightarrow |x\rangle_2, |x\rangle_2 \rightarrow |y\rangle_2. \quad (11.18)$$

И, наконец, для состояния  $|\phi^-\rangle_{12}$  Боб производит одновременно и смену поляризации и зависимый от поляризации фазовый сдвиг:

$$|y\rangle_2 \rightarrow |x\rangle_2, |x\rangle_2 \rightarrow e^{i\pi} |y\rangle_2. \quad (11.19)$$

После того как Боб произвел одно из преобразований (11.16) - 11.19 он отправляет свою частицу Алисе. Алиса в свою очередь измеряет полученное белловское состояние (11.15), например с помощью детектора описанного в 10.5, определяет какое из четырех действий было совершено Бобом. Таким образом Боб может передать Алисе 4 бита информации.

## 11.3 Кодирование информации

### 11.3.1 Теорема кодирования Шенона

Допустим у нас имеется сообщение, которое может состоять из некоторого ограниченного набора символов (алфавита). Предположим, что в нашем алфавите  $k$  символов:

$$\{a_1, \dots, a_k\} \quad (11.20)$$

Каждый символ появляется с некоторой известной вероятностью  $p_k = p(a_k)$ . Далее рассмотрим сообщение, состоящее из  $n \gg 1$  символов. Нас интересует вопрос: можно ли сжать это сообщение, т. е. можно ли закодировать это сообщение таким образом, чтобы результат содержал меньше чем  $n$  символов и при этом была бы возможность получить исходное сообщение без потери информации.

Ответ был дан Шеноном, и он гласит, что максимальное сжатое сообщение будет состоять из  $nH$  бит, где  $H = -\sum_k p_k \log p_k$  - количество информации, которое характеризует наш алфавит. Данный результат известен как теорема Шенона для канала без шума.

В качестве примера удобно использовать двоичный алфавит, при этом 0 будет встречаться с вероятностью  $p$ , а 1 с вероятностью  $1-p$ . Таким образом, если у нас имеется сообщение длиной  $n$  бит - то имеется возможность сжать его до  $nH$  бит. При этом очевидно что

$$n \geq nH > 0. \quad (11.21)$$

При этом знак равенства в (11.21) будет иметь место только при равновероятном распределении вероятности  $p = \frac{1}{2}$ . Действительно в этом случае

$$nH = n \left( -\frac{1}{2} \log \frac{1}{2} - \frac{1}{2} \log \frac{1}{2} \right) = n.$$

### 11.3.2 Квантовая теорема кодирования

Как будет выглядеть квантовый аналог теоремы Шенона для канала без шума? Для это прежде всего рассмотрим квантовый аналог алфавита (11.20). Квантовое сообщение кодируется некоторым набором состояний

$$\{|a_1\rangle, \dots, |a_k\rangle\}. \quad (11.22)$$

Каждое из состояний появляется с некоторой вероятностью  $p_k = p(|a_k\rangle)$ . Таким образом мы можем записать матрицу плотности для каждого символа нашего сообщения:

$$\hat{\rho} = \sum_k p_k |a_k\rangle \langle a_k|. \quad (11.23)$$

Сообщение, состоящее из  $n$  символов, имеет следующую матрицу плотности

$$\hat{\rho}^n = \hat{\rho} \otimes \dots \otimes \hat{\rho}.$$

Можно ли сжать это сообщение и если да, то до какого предела? Ответ дает квантовая теорема кодирования для канала без шума (теорема Шумахера).

Предел достигается при использовании

$$nH = -nSp(\hat{\rho} \log \hat{\rho}),$$

В качестве примера рассмотрим кодировку с помощью поляризационных состояний фотона. Допустим, что наш алфавит состоит из двух состояний:

1.  $|x\rangle$  - фотон поляризован по оси  $x$
2.  $|y\rangle$  - фотон поляризован по оси  $y$

При это предполагаем, что состояние  $|x\rangle$  встречается с вероятностью  $p_{|x\rangle} = p$ , а состояние  $|y\rangle$  - с вероятностью  $p_{|y\rangle} = 1 - p_{|x\rangle} = 1 - p$ . Таким образом матрица плотности (11.23) будет иметь вид

$$\hat{\rho} = p |x\rangle \langle x| + (1 - p) |y\rangle \langle y|. \quad (11.24)$$

В этом случае удобно использовать в качестве единицы измерения информации кубит и, соответственно, если исходное сообщение кодируется  $n$  фотонами, то его можно сжать до  $nH = -nSp(\hat{\rho} \log \hat{\rho})$  кубит, т. е. можно использовать меньше чем  $n$  фотонов для передачи этого сообщения. Главное отличие квантового случая от классического в том, что возможно сжатие информации даже в том случае, если  $p = \frac{1}{2}$ .

## 11.4 Упражнения

1. Доказать квантовое выражение для энтропии (11.12).



## Глава 12

# Криптография

С того момента, как была осознана важность информации, стали появляться средства ее защиты.

Изобретались новые методы шифрования, такие например, как шифр Цезаря, в котором каждая буква алфавита заменялась на другую (например, следующую через три позиции в алфавите после нее). Наряду с новыми методами шифрования появлялись способы вскрытия этих шифров, например для шифра Цезаря можно воспользоваться статистическими свойствами языка, на котором писалось исходное сообщение.

Очень часто безопасность шифра обеспечивалась тем, что алгоритм, по которому обеспечивалось шифрование, держался в секрете, как например в рассмотренном выше шифре Цезаря. В современной классической криптографии чаще всего алгоритмы публикуются и доступны для изучения каждому. Секретность обеспечивается тем, что само сообщение смешивается с секретным ключом по некоторому открытому алгоритму.

Допустим нам надо передать некоторое сообщение от Алисы к Бобу по некоторому защищенному каналу связи. Сообщение должно быть представлено в некоторой цифровой форме. Протокол, описывающий такую передачу, состоит из нескольких этапов. На первом Алиса и Боб должны получить некоторую общую случайную последовательность чисел, которая будет называться ключом. Эта процедура называется распределением ключа.

На следующем этапе Алиса должна с помощью некоторого алгоритма  $E$  получить из исходного сообщения  $P$  и ключа  $K$  зашифрованное сообщение  $C$ . Данная процедура может быть описана следующим соотношением:

$$E_K(P) = C. \quad (12.1)$$

На третьем этапе полученное зашифрованное сообщение должно быть передано Бобу.

На последнем этапе Боб с помощью известного алгоритма  $D$  и полученного на первом этапе ключа  $K$  должен восстановить исходное сообщение  $P$

из полученного зашифрованного  $C$ . Данная процедура может быть описана следующим соотношением

$$D_K(C) = P. \quad (12.2)$$

При анализе данного протокола возникают следующие вопросы. Как реализовать безопасное распределение ключа. Второй - существует ли абсолютно стойкий алгоритм. И наконец последний - возможна ли безопасная передача зашифрованного сообщения, когда оно не может быть прослушано или подменено.

Классическая криптография дает однозначный ответ только на второй вопрос. Абсолютно криптостойкий алгоритм существует - он носит название одноразового блокнота. Ниже представлено детальное описание этого алгоритма.

## 12.1 Одноразовый блокнот

Схема одноразового блокнота была предложена в 1917 году Мэйджором Дж. Моборном и Г. Вернамом. Классический одноразовый блокнот представляет собой некоторый набор случайных ключей, каждый из которых равен по размеру отправляемому сообщению и используется только один раз.

Предположим что мы хотим зашифровать сообщение на некотором языке (например на английском). Число символов (букв) которое используется в алфавите обозначим через  $X$ . Для английского языка (без знаков препинания и различия регистра)  $X = 26$ . Далее каждому из символов языка мы назначим некоторое число  $c$ , такое что  $0 \leq c \leq X$ . Например для английского языка можно записать

$$\begin{aligned} A &\rightarrow 0 \\ B &\rightarrow 1 \\ &\dots \\ Z &\rightarrow 25 \end{aligned}$$

Процедура шифрования (12.1) описывается следующим выражением

$$E_{K_i}(P_i) = P_i + K_i \mod X = C_i, \quad (12.3)$$

где  $i$  номер шифруемого символа.

Процедура дешифрования (12.2) описывается следующим выражением

$$D_{K_i}(C_i) = C_i - K_i \mod X = P_i, \quad (12.4)$$

где  $i$  номер шифруемого символа.

| $a$ | $b$ | $a \oplus b$ |
|-----|-----|--------------|
| 0   | 0   | 0            |
| 0   | 1   | 1            |
| 1   | 0   | 1            |
| 1   | 1   | 0            |

Таблица 12.1: XOR  $a \oplus b$ 

Эта процедура легко обобщается на случай двоичных данных, при этом вместо сложения по модулю используется операция XOR ( $a \oplus b$ ) как для шифрования, так и для дешифрования :

Клод Шенон показал [21], что если ключ действительно случайный, имеет такую же длину, как исходное сообщение, и не используется повторно, то предложенная схема одноразового блокнота абсолютно защищена.

Согласно Шенону абсолютная защищенность (perfect security) может быть определена следующим образом.

**Определение 12.1.1.** Шифр  $(E, D)$  абсолютно защищен если для любых двух сообщений одинаковой длины  $m_0$  и  $m_1$ , некоторого шифротекста  $c$  и ключа  $k \leftarrow_R K$  вероятности того что исходный текст  $m_0$  или  $m_1$  равны:

$$P(E(m_0, k) = c) = P(E(m_1, k) = c)$$

Перефразируя это определение можно сказать, что по исходной статистике шифротекста невозможно получить никакой информации об исходном сообщении.

**Теорема 12.1.1** (Криптостойкость одноразового блокнота). *Схема одноразового блокнота имеет абсолютную защищенность.*

*Доказательство.* Обозначим через  $|K|$  - число всех возможных ключей длины  $l$ . Где  $l$  также длина исходных сообщений:  $|m_{0,1}| = l$ . В силу того, что ключ которым зашифровано сообщение определяется единственным образом:

$$k_{0,1} = c \oplus m_{0,1},$$

получаем для вероятностей

$$P(E(m_0, k) = c) = P(E(m_1, k) = c) = \frac{1}{|K|}.$$

□

## 12.2 Проблемы классической криптографии

Если существует абсолютно защищенная криптографическая система (одноразовый блокнот) то что же не так в классической криптографии? Проблема заключается в получении ключей, удовлетворяющих требованиям одноразового блокнота (длина ключа равна длине сообщения, ключ состоит из случайных данных и ни разу не используется повторно) и передачи этих ключей Бобу и Алисе.

Проблемы возникают как на этапе генерации ключей,<sup>1</sup> так и на этапе передачи этих ключей.

Для передачи ключей в классической криптографии используются так называемые алгоритмы с открытым ключом. Существует несколько протоколов обмена ключей, основанных на криптографических системах с открытым ключом. Все они основаны на том, что существует два ключа, первый из которых, называемый открытым (public key), используется только для зашифрования, а второй - закрытый (private key) для дешифрования. Для того чтобы получить закрытый ключ из открытого, необходимо произвести какую-то сложную математическую операцию. Например безопасность одной из наиболее популярных систем с открытым ключом - RSA(см. 19.6), основана на трудности факторизации<sup>2</sup> больших чисел.

Схема протокола распределения ключа, основанная на криптографии с открытым ключом, может быть описана следующим образом. На первом этапе Алиса создает открытый и закрытый ключи и первый из них отправляет Бобу. Боб со своей стороны создает тот ключ, который хотелось бы иметь и Алисе и Бобу (который требуется распределить). Этот ключ шифруется (например по RSA) с помощью открытого ключа Алисы и пересылается ей. Алиса, получая этот зашифрованный ключ, может расшифровать его с помощью своего закрытого ключа.

Если злоумышленник (Ева) хочет узнать передаваемый ключ, она должна решить сложную математическую задачу по факторизации больших чисел. Считается, но не доказано, что сложность факторизации растет экспоненциально с ростом числа цифр в числе [62].<sup>3</sup> Таким образом при увеличении числа цифр задача быстро становится не решаемой.

В этой схеме имеется несколько проблем. Первая связана с тем что сложность факторизации не доказана. Мало того, существуют алгоритмы для квантовых компьютеров - алгоритм Шора(см. 13.3), которые решают задачу

<sup>1</sup>получение больших последовательностей случайных чисел является не тривиальной математической задачей

<sup>2</sup>разложении на простые множители

<sup>3</sup>Наиболее быстрый из известных алгоритмов решает задачу о факторизации числа  $N$  за время порядка  $O\left(\exp\left(\log^{\frac{1}{3}} N (\log \log N)^{\frac{2}{3}}\right)\right)$ .



Рис. 12.1: Схема распределения ключа, основанная на проверке неравенств Белла

о факторизации числа  $N$  за время  $O(\log N)$ , т. е. за время порядка числа цифр в  $N$ . Таким образом в тот момент, когда будет построен квантовый компьютер, все системы, основанные на RSA, утратят свою актуальность.

## 12.3 Квантовая криптография

Случайность, присущая квантовым объектам, наталкивает на мысль использовать их для распределения ключа. Существует много различных безопасных схем распределения ключа, основанных на использовании квантовых объектов. Мы исследуем схему, базирующуюся на проверке неравенств Белла (см. 10.2). Рассматриваемая схема изображена на рис. 12.1.

Источник перепутанных фотонов  $S$  создает пары фотонов, один из которых отсылается Алисе, а второй Бобу, которые выполняют измерения параметров Стокса своих фотонов.

Алиса в случайном порядке измеряет либо  $\hat{A} = \hat{S}_1^{(1)}$  либо  $\hat{A}' = \hat{S}_2^{(1)}$ . Боб в случайном порядке производит измерения следующих величин

$$\begin{aligned}\hat{B} &= \frac{1}{\sqrt{2}} \left( \hat{S}_1^{(2)} + \hat{S}_2^{(2)} \right), \\ \hat{B}' &= \frac{1}{\sqrt{2}} \left( \hat{S}_1^{(2)} - \hat{S}_2^{(2)} \right) \\ \hat{C} &= \hat{S}_1^{(2)}, \\ \hat{C}' &= \hat{S}_2^{(2)}.\end{aligned}$$

Таким образом в результате эксперимента мы получим 8 пар значений, которые могут быть объединены в три группы.

В первой находятся коррелирующие комбинации операторов  $\hat{A}$ ,  $\hat{A}'$ ,  $\hat{C}$  и  $\hat{A}'$ :  $(a, c)$  и  $(a', c')$ . Для этих комбинаций мы можем сказать, что если одно из чисел  $a$  или  $a'$  равно  $\pm 1$ , то второе ( $c$  или  $c'$ ) равно  $\mp 1$ . Таким образом эти числа могут быть использованы для получения случайной последовательности чисел, которая будет в дальнейшем использоваться в качестве ключа.

Во второй группе находятся 4 пары значений, которые будут использоваться для проверки неравенств Белла:  $(a, b)$ ,  $(a', b)$ ,  $(a, b')$  и  $(a', b')$ .

В последней группе находятся пары значений  $(a, c')$  и  $(a', c)$ . В дальнейшем эта группа значений отбрасывается.

На начальном этапе Боб и Алиса в случайном порядке (независимо друг от друга) производят измерения. По завершении измерений они говорят друг другу (по обычному открытому каналу связи) какие величины они измеряли в каждом конкретном испытании, при этом результат самих измерений не сообщается. В дальнейшем отбрасываются те испытания, в которых кто-либо из них не смог зарегистрировать фотон, и результаты, относящиеся к третьей группе измерений. Результаты второй группы измерений открыто публикуются и по ним считается среднее значение  $\langle F \rangle$  (10.8).

Если полученное значение по модулю близко к предсказаниям квантовой механики (10.9)

$$\langle F \rangle_{quant} = -\sqrt{2},$$

то результат первой группы измерений может быть интерпретирован в качестве ключа.

Если злоумышленник Ева хочет попытаться узнать результаты первой группы измерений, которые составляют распределяемый ключ, то один из способов сделать это - подменить собой источник перепутанных пар фотонов и отсылать Алисе и Бобу по паре фотонов с определенными поляризационными свойствами, тогда результаты опытов Алисы и Боба будут предопределены заранее. Но в этом случае  $\langle F \rangle$ , согласно (10.12), будет лежать в интервале:

$$-1 \leq \langle F \rangle_{class} \leq 1.$$

Таким образом Алиса и Боб по результатам проверки неравенств Белла могут определить факт вмешательства Евы и считать полученный ключ скомпрометированным, если проверка установит факт присутствия Евы.

## Глава 13

# Квантовые вычисления

Алгоритмы играют большую роль в вычислительной технике. Алгоритм представляет собой последовательность шагов необходимых для получения ответа на некоторую задачу. Каждая задача характеризуется некоторым числом, который определяет ее размер. Сложность алгоритма оценивается как число простейших операций необходимых для решения поставленной задачи. Очевидно, что в большинстве случаев (но не всегда) это число растет с размером задачи.

**Пример 13.0.1.** Поиск элемента массива *Задача - найти элемент массива, удовлетворяющий некоторым условиям. Размером задачи является число элементов массива  $N$ .*

*В общем случае (не структурированный массив данных) поиск ведется простым перебором. Этот поиск требует число операций (сравнений) которое растет линейно с размером массива  $O(N)$ .*

*В случае структурированных данных число операций требуемое для поиска может быть уменьшено. Например в случае отсортированного массива сложность задачи растет как  $O(\log N)$ .*

Вместе с тем существование алгоритма еще не гарантирует его практической реализуемости. В частности алгоритмы требующие экспоненциального числа шагов от размера исходной задачи считаются практически не реализуемыми не смотря на то, что с теоретической точки зрения решение существует.

Одним из примеров является задача о факторизации натурального числа, т. е. задача о разложении его на простые множители (см. пример [13.0.2](#)).

**Пример 13.0.2.** Факторизация натуральных чисел *Задача - найти разложение числа на простые множители. Размером задачи является разрядность исходного числа. Например для случая разрядности  $r = 4$ :  $1 \leq N = 15 \leq 2^r = 2^4 = 16$ ). Результат может быть найден легко и быстро:  $15 = 3 \cdot 5$ .*

С ростом числа разрядов  $r$  число операций необходимых для факторизации в классических алгоритмах растет как  $O(2^r)$ , что для случая  $r = 1000 - 2000$  означает практическую невозможность факторизации таких чисел.

Квантовые объекты обладают свойствами отличающимися от классических объектов, соответственно алгоритмы, построенные на базе квантовых объектов могут в ряде случаев обладать характеристиками недоступными для классических алгоритмов. Например квантовый алгоритм Гровера [9] решает задачу о поиске в неструктурированном массиве данных (см. пример 13.0.1) с помощью  $O(\sqrt{N})$  операций. Алгоритм Шора [22] позволяет решить задачу о факторизации числа (см. пример 13.0.2) используя линейное число операций  $O(r)$ .

## 13.1 Основные принципы квантовых вычислений

### 13.1.1 Представление информации. Классические и квантовые состояния

Основное отличие квантовых и классических компьютеров заключается в том как они хранят информацию.

В классическом случае информация хранится в некоторых ячейках памяти. Состояние каждой ячейки памяти описывается одним числом которое может принимать значение 0 или 1. Если объединяются  $m$  ячеек памяти то общее состояние классической системы (которое она может принимать в конкретный момент времени) описывается  $m$  числами.

В квантовом случае ячейка памяти представлена кубитом для описания которого необходимо два комплексных числа  $\alpha_0$  и  $\alpha_1$ <sup>1</sup>:

$$|\psi\rangle_1 = \alpha_0 |0\rangle + \alpha_1 |1\rangle.$$

Для описания составной системы состоящей из  $m$  кубитов необходимо  $2^m$  комплексных чисел. Иначе можно сказать что квантовое состояние содержит в качестве суперпозиции все возможные классические состояния. В качестве примера можно рассмотреть систему состоящую из 3 кубитов:

$$|\psi\rangle_3 = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle. \quad (13.1)$$

<sup>1</sup>Более правильно говорить тремя вещественными числами, потому что на  $\alpha_{0,1}$  действует следующее ограничение  $|\alpha_0|^2 + |\alpha_1|^2 = 1$  откуда с учетом  $\alpha_{0,1} = r_{0,1}e^{i\theta_{0,1}}$  получим что  $r_0^2 = 1 - r_1^2$





Рис. 13.1: Классические вычисления. На вход подается число  $x$  состоящее из  $n$  бит, а на выходе имеем результат  $y = f(x)$  описываемый  $m$  битами

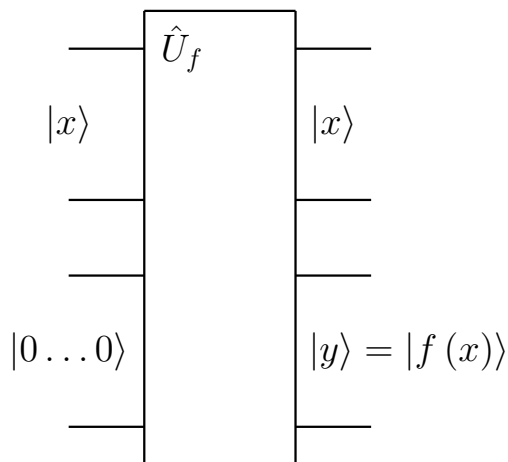


Рис. 13.2: Квантовые обратимые вычисления. На вход подается число  $|x\rangle$  состоящее из  $n$  кубит и затравка из нулевых состояний ( $m$  кубит), а на выходе имеем результат  $|y\rangle = |f(x)\rangle$  описываемый  $m$  кубитами и исходное состояние  $|x\rangle$

Как видно любое классическое состояние системы из 3 бит представлено в качестве одного из членов суперпозиции (13.1). Например число  $5_{10} = 101_2$  входит в (13.1) с коэффициентом  $\alpha_5$ .

### 13.1.2 Обратимые вычисления

В классическом случае вычисление состоит в преобразовании исходных  $n$  битов в результат, описываемый  $m$  битами (см. рис. 13.1). Преобразование при этом задается некоторой функцией  $f(x)$ . Типичный пример - сложение по модулю 2 (см. табл. 12.1) в котором на входе имеем 2 бита ( $n = 2$ ), а на выходе - 1 бит ( $m = 1$ ).

Такая схема не будет работать в квантовом случае прежде всего потому что изменение чистых квантовых состояний во времени должно осуществляться посредством унитарного оператора эволюции (14.35), т. е. должно быть обра-

тимым что для нашего классического примера невозможно <sup>2</sup>. В силу этого в квантовых вычислениях используют другую схему (см. [рис. 13.2](#)) при которой возможны обратимые вычисления.

На вход вместе с исходными данными  $x$  описываемыми  $n$  кубитами подаются  $m$  кубитов в состоянии  $|0\rangle$ , таким образом чтобы общее число входов и выходов соответствовало друг другу. Следовательно связь между входом и выходом может быть описана в виде <sup>3</sup>

$$\underbrace{|x\rangle}_n \underbrace{|f(x)\rangle}_m = \hat{U}_f \underbrace{|x\rangle}_n \underbrace{|0\dots 0\rangle}_m. \quad (13.2)$$

## 13.2 Квантовые логические элементы

Каким образом может быть сконструирован элемент осуществляющий преобразование  $\hat{U}_f$  (13.2). Существует набор элементов из которых можно построить, с заданной точностью, элемент осуществляющий необходимое преобразование  $\hat{U}_f$ . Такие наборы называются универсальными.

### 13.2.1 Универсальный набор квантовых вентилей

**Тождественное преобразование**

$$\hat{\sigma}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

**Отрицание**

$$\hat{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

**Фазовый сдвиг**

$$\hat{\sigma}_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

<sup>2</sup>невозможно получить из одного бита (результат) два бита исходной информации

<sup>3</sup>Более правильно записывать в общем виде как  $\underbrace{|x\rangle}_n \underbrace{|f(x)\rangle}_m \underbrace{|r\rangle}_k = \hat{U}_f \underbrace{|x\rangle}_n \underbrace{|0\dots 0\rangle}_{m+k}$ , где  $|r\rangle$  остаток размером  $k$  кубит который не используется в вычислениях и служит цели обеспечения унитарности оператора  $\hat{U}_f$

$$|x\rangle \text{---} \boxed{\hat{H}} \text{---} |y\rangle$$

Рис. 13.3: Преобразование Адамара на одном кубите

## Преобразование Адамара

Одним из базовых квантовых логических элементов является преобразование Адамара (см. [рис. 13.3](#)), которое определяется следующими соотношениями

$$\begin{aligned}\hat{H}|0\rangle &= |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \\ \hat{H}|1\rangle &= |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},\end{aligned}$$

В матричной форме это преобразование может быть записано в виде

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (13.3)$$

где в качестве базиса выбраны вектора

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

и

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Из (13.3) можно получить следующее свойство оператора  $\hat{H}$ :

$$\hat{H}\hat{H} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (13.4)$$

Это преобразование используется для получения суперпозиции состояний содержащие все возможные значения аргумента вычисляемой функции (см. [рис. 13.4](#)).

## CNOT

Матрица преобразования имеет вид

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

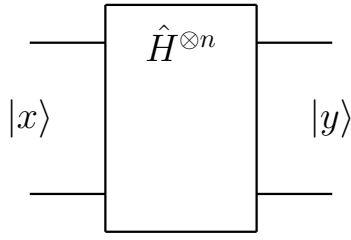


Рис. 13.4: Преобразование Адамара  $\hat{H}^{\otimes n}$  на нескольких кубитах

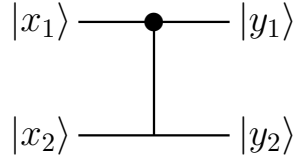


Рис. 13.5: Управляющий элемент CNOT

Данный вентиль (см. [рис. 13.5](#)) применяется для двух кубит и инвертирует состояние второго кубита только если первый кубит равен единице.

Таким образом если наше исходное состояние двух кубит было

$$|\psi_i\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

то оно преобразуется в

$$CNOT |\psi_i\rangle = |\psi_f\rangle = a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle$$

## Универсальный набор

**Определение 13.2.1** (Универсальный набор квантовых вентилях). Набор квантовых вентилях называют универсальным, если любое унитарное преобразование можно аппроксимировать с заданной точностью конечной последовательностью вентилях из этого набора.

**Теорема 13.2.1** (Китаев). *Набор  $\hat{\sigma}_0, \hat{\sigma}_1, \hat{\sigma}_2, \hat{H}, CNOT$  является универсальным.*

*Доказательство.* TBD

□

## 13.2.2 Управляющие элементы

## 13.3 Алгоритм Шора

Один из наиболее популярных алгоритмов шифрования RSA (см. [разд. 19.6](#)) построен на предположении о сложности факторизации (разложимости на

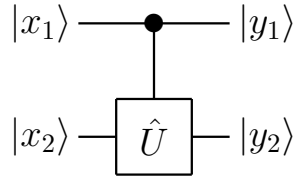
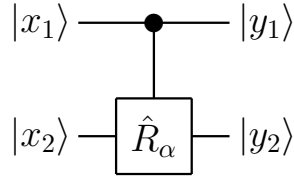


Рис. 13.6: Управляющий элемент

Рис. 13.7: Управляемый фазовый сдвиг  $\hat{R}_\alpha$ 

простые множители) больших чисел. Соответственно алгоритмы позволяющие осуществлять разложение на простые множители представляют особый интерес. Ниже представлено описание такого алгоритма предложенное Шором [22].

### 13.3.1 Факторизация чисел и нахождение периода функций

Задача факторизации некоторого числа  $N$  тесно связана с нахождением периода функций. Рассмотрим следующую, которая называется функцией возведения в степень по модулю

$$f(x, a) = a^x \mod N. \quad (13.5)$$

Функция (13.5) зависит от анализируемого числа  $N$  и двух аргументов  $x$  и  $a$ . Аргумент  $a$  выбирается из следующих условий

$$\begin{aligned} 0 < a < N, \\ \text{НОД}(N, a) &= 1. \end{aligned} \quad (13.6)$$

Типичный график функции (13.5) представлен на рис. 13.8.

Условия выбора коэффициента  $a$  (13.6) такие что  $a$  и  $N$  не имеют общих делителей. Если же такие делители существуют, то они являются искомым решением задачи факторизации и легко находятся с помощью алгоритма Евклида (см. разд. 19.1).

Функция (13.5) периодическая, т. е. существует такое число  $r$ , что  $f(x + r, a) = f(x, a)$ . Минимальное из возможных чисел  $r$  называется периодом функции (13.5).

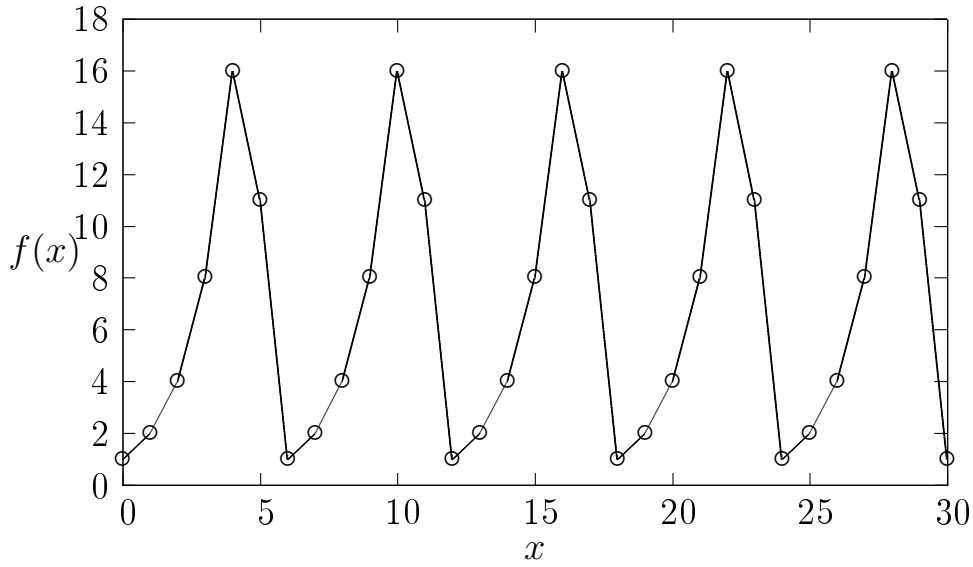


Рис. 13.8: График функции  $f(x, a) = a^x \bmod N$  при  $a = 2$ ,  $N = 21$ . Период функции  $r = 6$ .

Для доказательства периодичности отметим, что  $f(x, a)$  не может быть равной нулю. Действительно если выполнено условие  $f(x, a) = 0$ , то

$$\exists x \in \{0, 1, \dots\} : a^x = k \cdot N,$$

где  $k$  - целое число, что не возможно в силу взаимной простоты  $a$  и  $N$  (13.6) <sup>4</sup>.

Таким образом область значений функции (13.5) ограничена множеством

$$f(x, a) \in \{1, \dots, N-1\},$$

откуда

$$\exists k, j : k > j, k, j \in \{0, 1, \dots, N\}, f(k, a) = f(j, a),$$

что и доказывает периодичность функции (13.5).

Пусть  $k = j + r$ , тогда

$$a^k \bmod N = a^{j+r} \bmod N = a^j a^r \bmod N = a^j \bmod N,$$

т. к.  $a$  и  $N$  взаимно просты то мы можем записать

$$a^r \equiv 1 \bmod N. \quad (13.7)$$

Период функции (13.5) может быть как четным так и нечетным. В алгоритме Шора нам интересен первый вариант: период - четное число. В противном случае выбирают новое число  $a$  и повторяют нахождение периода.

<sup>4</sup>При это предполагается очевидно, что  $N > 1$

Таким образом с учетом  $r = 2 \cdot l$  мы можем переписать (13.7) в виде

$$a^{2 \cdot l} \equiv 1 \pmod{N},$$

при этом в силу того  $r$  - минимальное число удовлетворяющее условию периодичности, то

$$a^l \not\equiv 1 \pmod{N}.$$

Если при этом подобрать число  $a$  таким образом, что

$$a^l \not\equiv -1 \pmod{N},$$

то имеем

$$(a^l - 1)(a^l + 1) = k \cdot N, \quad (13.8)$$

где  $k$  - некоторое целое число. Из (13.8) получаем что  $a^l \pm 1$  имеют общие нетривиальные (отличные от 1) делители с  $N$ .

**Пример 13.3.1.** Нахождение делителей числа  $N = 21$  В качестве примера рассмотрим задачу о нахождении делителей числа  $N = 21$ . Выбрав  $a = 2$  мы получим период функции (13.5)  $r = 6$  (см. рис. 13.8). Очевидно что

$$2^3 \equiv 8 \pmod{21} \not\equiv -1 \pmod{21}.$$

Таким образом находя соответствующие наибольшие общие делители решаем задачу

$$\begin{aligned} \text{НОД}(2^3 - 1, 21) &= \text{НОД}(7, 21) = 7, \\ \text{НОД}(2^3 + 1, 21) &= \text{НОД}(9, 21) = 3, \\ 21 &= 7 \cdot 3. \end{aligned}$$

Таким образом задача факторизации числа  $N$  может быть сведена к задаче о нахождении периода некоторой функции посредством следующего алгоритма:

---

**Алгоритм 1** Алгоритм Шора

---

$a \leftarrow 0$

**repeat**

Выбрать новое число  $a$  такое, что  $0 < a < N$

**if**  $\text{НОД}(a, N) \neq 1$  **then**

**return**  $a$

**end if**

Найти период  $r$  функции  $f(x, a) = a^x \pmod{N}$

**until**  $(r \not\equiv 0 \pmod{2})$  **or**  $(a^{\frac{r}{2}} \equiv -1 \pmod{N})$

**return**  $\text{НОД}(a^{\frac{r}{2}} \pm 1, N)$

---

## 13.4 Квантовое преобразование Фурье

Для анализа периодических последовательностей (функций) может быть использовано дискретное преобразование Фурье (см. [разд. 18.2](#)), которое определяется следующим соотношением (18.4):

$$\tilde{X}_k = \sum_{m=0}^{M-1} x_m e^{-\frac{2\pi}{M} k \cdot m}, \quad (13.9)$$

где исходная последовательность чисел  $\{x_m\}$  имеет  $M$  членов.

### 13.4.1 Схема квантового преобразования Фурье

Квантовое преобразование Фурье <sup>5</sup> имеет дело с состояниями вида

$$|x\rangle = \sum_{k=0}^{M-1} x_k |k\rangle, \quad (13.10)$$

где имеется последовательность амплитуд  $\{x_k\}$ , которая задает исходную последовательность для преобразования Фурье (13.9). В базисном векторе  $|k\rangle$  записан номер члена этой последовательности.

Очевидно, что члены последовательности (13.10) должны удовлетворять условию нормировки

$$\sum_k |x_k|^2 = 1.$$

Допустим что некоторый оператор  $\hat{F}^M$  (оператор квантового преобразования Фурье) преобразует базисный вектор  $|k\rangle$  по правилу задаваемому соотношением (18.4):

$$\hat{F}^M |k\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{-i\omega k j} |j\rangle_{inv} \quad (13.11)$$

Системы базисных векторов  $\{|k\rangle\}$  и  $\{|k\rangle_{inv}\}$  представляют собой один и тот же набор векторов которые пронумерованны различным способом.

---

<sup>5</sup>Для анализа работы схемы квантового преобразования Фурье была использована работа [13]



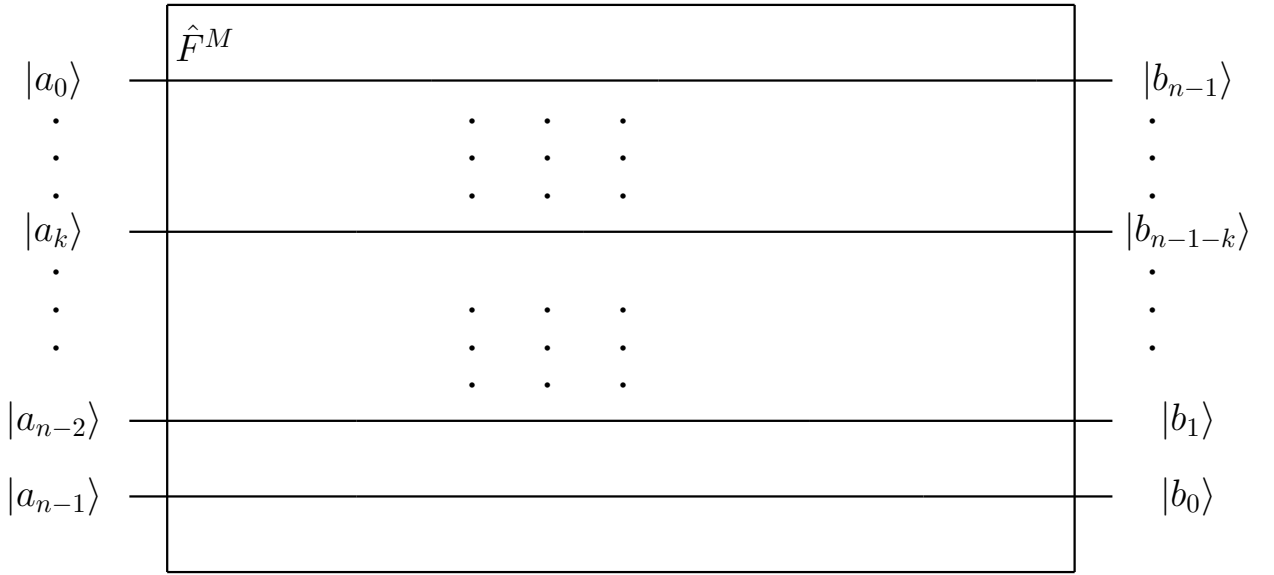


Рис. 13.9: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье. Исходные данные и данные на выходе

Из (13.10) и (13.11) получим

$$\begin{aligned}
 \hat{F}^M |x\rangle &= \sum_{j=0}^{M-1} x_j \hat{F}^M |j\rangle = \\
 &= \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \sum_{j=0}^{M-1} e^{-i\omega k j} x_k |j\rangle_{inv} = \\
 &= \sum_{j=0}^{M-1} \left\{ \frac{1}{\sqrt{M}} \left( \sum_{k=0}^{M-1} e^{-i\omega k j} x_k \right) \right\} |j\rangle_{inv} = \\
 &= \sum_{j=0}^{M-1} \tilde{X}_j |j\rangle_{inv} = |\tilde{X}\rangle_{inv},
 \end{aligned}$$

где

$$\tilde{X}_j = \tilde{X}_j^M = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{-i\omega k j} x_k. \quad (13.12)$$

Выражение (13.12) повторяет классический аналог (18.4), т. е. можно записать

$$|x\rangle \longleftrightarrow |\tilde{X}\rangle_{inv}.$$

Допустим теперь, что на вход нашей системы подается состояние вида (13.10) которое представляет собой суперпозицию  $M$  базисных состояний

$\{|k\rangle\}$  (см. рис. 13.9). Предположим что число базисных состояний является степенью двойки, т. е. базисное состояние представимо в виде тензорного произведения  $n = \log_2 M$  кубитов:

$$|k\rangle = |a_0^{(k)}\rangle \otimes |a_1^{(k)}\rangle \otimes \cdots \otimes |a_{n-1}^{(k)}\rangle,$$

где

$$k = a_0^{(k)} + 2^1 a_1^{(k)} + \cdots + 2^{n-1} a_{n-1}^{(k)},$$

$$a_i^{(k)} \in \{0, 1\}.$$

На выходе (см. рис. 13.9) мы имеем суперпозицию  $M$  базисных состояний  $\{|j\rangle_{inv}\}$ , где для состояния  $|j\rangle_{inv}$  получим

$$|j\rangle_{inv} = |b_{n-1}^{(j)}\rangle \otimes |b_{n-2}^{(j)}\rangle \otimes \cdots \otimes |b_0^{(j)}\rangle,$$

где

$$j = b_0^{(j)} + 2^1 b_1^{(j)} + \cdots + 2^{n-1} b_{n-1}^{(j)},$$

$$b_i^{(j)} \in \{0, 1\}.$$

Из формулы (18.10) можно заметить, что если у нас имеется входной сигнал  $x$  состоящий из  $n = \log_2 M$  битов, то бит  $a_0^{(k)}$  может быть использован для выбора четных (первого члена суммы (18.10)) или нечетных (второго члена суммы (18.10)).

Действительно, исключая  $a_0^{(k)}$ , состояние (13.10) можно представить в виде суммы четных и нечетных компонент:

$$\begin{aligned} |x\rangle &= \sum_{k=0}^{M-1} x_k |k\rangle = \sum_{k=0}^{M-1} x_k |a_0^{(k)}\rangle \otimes |a_1^{(k)}\rangle \otimes \cdots \otimes |a_{n-1}^{(k)}\rangle = \\ &= \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m} |0\rangle \otimes |a_1^{(k)}\rangle \otimes \cdots \otimes |a_{n-1}^{(k)}\rangle + \\ &+ \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m+1} |1\rangle \otimes |a_1^{(k)}\rangle \otimes \cdots \otimes |a_{n-1}^{(k)}\rangle = \\ &= \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m} |0\rangle \otimes |m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m+1} |1\rangle \otimes |m\rangle = \\ &= \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle, \end{aligned}$$



Рис. 13.10: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье. Шаг 1:  $|x\rangle \rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle$

где

$$m = a_1^{(k)} + 2^1 a_2^{(k)} + \dots + 2^{n-2} a_{n-1}^{(k)}.$$

Применяя преобразование Фурье только для старших бит  $\hat{F}^{\frac{M}{2}}$ , т. е. исключая  $a_0^{(k)}$ , получим (см. рис. 13.10):

$$\begin{aligned} |x\rangle &\rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle = \\ &= \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes |m\rangle + \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes |m\rangle = \\ &= \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle. \end{aligned} \quad (13.13)$$

С учетом выражения (13.11) получим

$$\hat{F}^{\frac{M}{2}} |m\rangle = \sqrt{\frac{2}{M}} \sum_{j=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} |j\rangle_{inv}.$$

Таким образом для (13.13) имеем

$$\begin{aligned}
|x\rangle &\rightarrow \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle = \\
&= \sqrt{\frac{2}{M}} \sum_{j=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes |j\rangle_{inv} + \\
&+ \sqrt{\frac{2}{M}} \sum_{j=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes |j\rangle_{inv} = \\
&= \sum_{j=0}^{\frac{M}{2}-1} \left( \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} \right) |j\rangle_{inv} + \\
&+ \sum_{j=0}^{\frac{M}{2}-1} \left( \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m+1} \right) \left| \frac{M}{2} + j \right\rangle_{inv} = \\
&= \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{B}_j \left| \frac{M}{2} + j \right\rangle_{inv},
\end{aligned}$$

где

$$\begin{aligned}
\tilde{A}_j &= \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} \\
\tilde{B}_j &= \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m+1}
\end{aligned} \tag{13.14}$$

Если добавить теперь фазовый сдвиг для нечетных элементов, т. е. для тех у которых  $a_0^k = 1$  то получим схему изображенную на рис. 13.11:

$$\begin{aligned}
|x\rangle &\rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{R} \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle = \\
&= \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{B}_j \hat{R} \left| \frac{M}{2} + j \right\rangle_{inv}, \\
&= \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{C}_j \left| \frac{M}{2} + j \right\rangle_{inv}.
\end{aligned} \tag{13.15}$$



Рис. 13.11: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье. Шаг 2:  $|x\rangle \rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{R} \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1}$

Воспользовавшись выражением

$$\hat{R}_l |b_l^{(j)}\rangle = \exp\left(-2\pi i \frac{b_l^{(j)}}{2^{n-l}}\right) |b_l^{(j)}\rangle$$

получим, что оператор  $\hat{R}$  действует на состояние  $|\frac{M}{2} + j\rangle_{inv}$  следующим образом:

$$\begin{aligned} \hat{R} \left| \frac{M}{2} + j \right\rangle_{inv} &= \hat{R} |1\rangle \otimes |j\rangle_{inv} = \\ &= |1\rangle \otimes \hat{R}_0 |b_0^{(j)}\rangle \otimes \cdots \otimes \hat{R}_{n-2} |b_{n-2}^{(j)}\rangle = \\ &= \prod_{l=0}^{n-2} \exp\left(-2\pi i \frac{2^l b_l^{(j)}}{2^n}\right) |1\rangle \otimes |j\rangle_{inv} = \\ &= \exp\left(-2\pi i \frac{j}{M}\right) \left| \frac{M}{2} + j \right\rangle_{inv} \end{aligned} \quad (13.16)$$

При выводе (13.16) было учтено, что  $j = b_0^{(j)} + 2^1 b_1^{(j)} + \cdots + 2^{n-2} b_{n-2}^{(j)}$ .

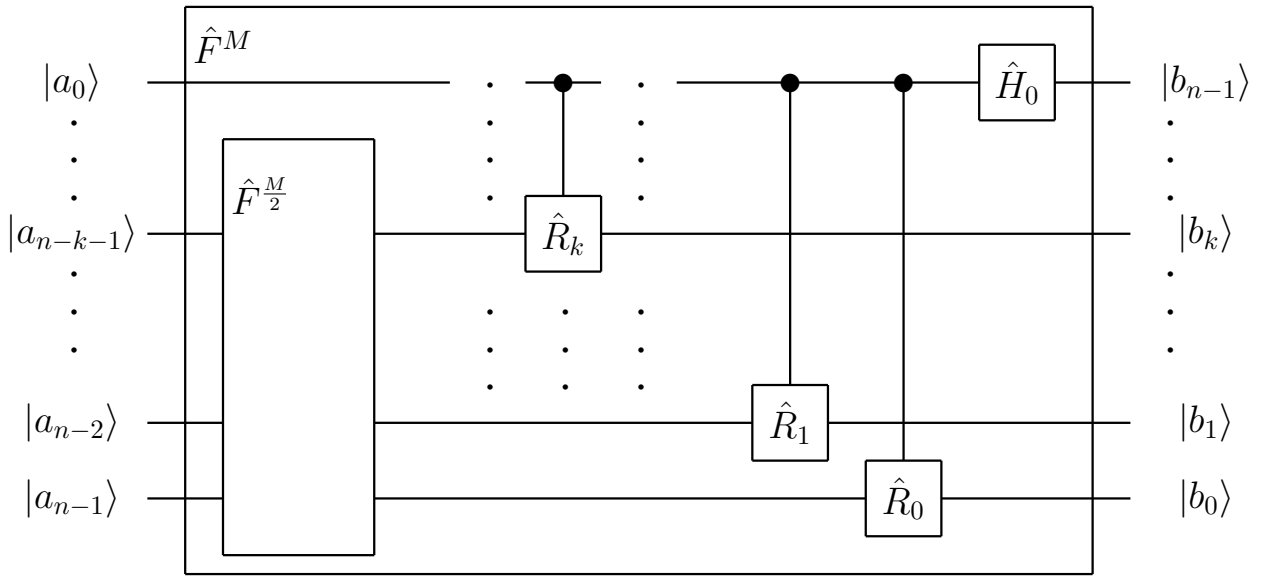


Рис. 13.12: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье

Таким образом для  $\tilde{C}_j$  в (13.15) имеем

$$\begin{aligned}
 \tilde{C}_j &= \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-2\pi i \frac{j}{M}} e^{-i \frac{4\pi}{M} m j} x_{2m+1} = \\
 &= \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i \frac{2\pi}{M} (2m+1) j} x_{2m+1}
 \end{aligned} \tag{13.17}$$

Если теперь применить преобразование Адамара для кубита  $|a_0\rangle$ , то получим схему изображенную на рис. 13.12. При этом исходное состояние пре-

образуется по следующему закону:

$$\begin{aligned}
|x\rangle &\rightarrow \hat{H}_0 \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{H}_0 \hat{R} \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} = \\
&= \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j \hat{H} |0\rangle \otimes |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{C}_j \hat{H} |1\rangle \otimes |j\rangle_{inv} = \\
&= \frac{1}{\sqrt{2}} \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j (|0\rangle + |1\rangle) \otimes |j\rangle_{inv} + \frac{1}{\sqrt{2}} \sum_{j=0}^{\frac{M}{2}-1} \tilde{C}_j (|0\rangle - |1\rangle) \otimes |j\rangle_{inv} = \\
&= \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j + \tilde{C}_j}{\sqrt{2}} |0\rangle \otimes |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j - \tilde{C}_j}{\sqrt{2}} |1\rangle \otimes |j\rangle_{inv} = \\
&= \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j + \tilde{C}_j}{\sqrt{2}} |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j - \tilde{C}_j}{\sqrt{2}} \left| \frac{M}{2} + j \right\rangle_{inv}. \quad (13.18)
\end{aligned}$$

Для членов (13.18) с учетом равенств (13.14) и (13.17) имеем:

$$\begin{aligned}
\frac{\tilde{A}_j + \tilde{C}_j}{\sqrt{2}} &= \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} + \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{2\pi}{M}(2m+1)j} x_{2m+1} = \\
&= \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m \quad (13.19)
\end{aligned}$$

и

$$\begin{aligned}
\frac{\tilde{A}_j - \tilde{C}_j}{\sqrt{2}} &= \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} - \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{2\pi}{M}(2m+1)j} x_{2m+1} = \\
&= \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m \frac{1 + e^{-i\pi m}}{2} - \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m \frac{1 - e^{-i\pi m}}{2} = \\
&= \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} e^{-i\pi m} x_m = \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} e^{-i\frac{2\pi}{M}m\frac{M}{2}} x_m = \\
&= \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}m(\frac{M}{2}+j)} x_m \quad (13.20)
\end{aligned}$$

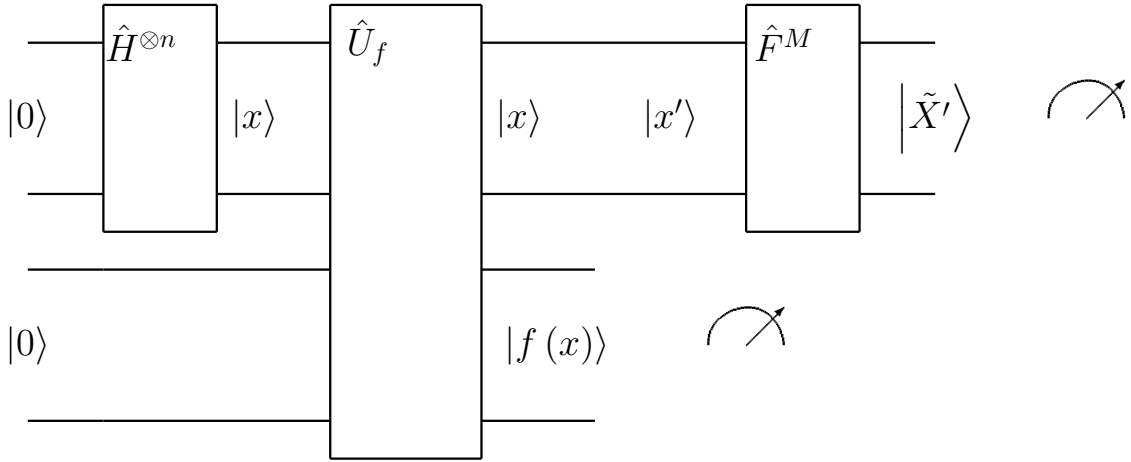


Рис. 13.13: Определение периода функций с помощью квантового преобразования Фурье

Объединяя (13.18), (13.19) и (13.20) окончательно получим

$$\begin{aligned}
 |x\rangle &\rightarrow \sum_{j=0}^{\frac{M}{2}-1} \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m |j\rangle_{inv} + \\
 &+ \sum_{j=0}^{\frac{M}{2}-1} \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}m(\frac{M}{2}+j)} x_m \left| \frac{M}{2} + j \right\rangle_{inv} = \\
 &= \sum_{j=0}^{M-1} \tilde{X}_j^M |j\rangle_{inv}
 \end{aligned}$$

### 13.4.2 Нахождение периода функций с помощью квантового преобразования Фурье

Для определения периода функции (13.5) используется схема представленная на рис. 13.13.

Первым элементом стоит преобразование Адамара  $n$  кубит, которое подготавливает исходное состояние в виде:

$$|in\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle.$$

После элемента вычисляющего функцию  $\hat{U}_f$  имеем для состояния

$$\hat{U}_f |in\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle.$$



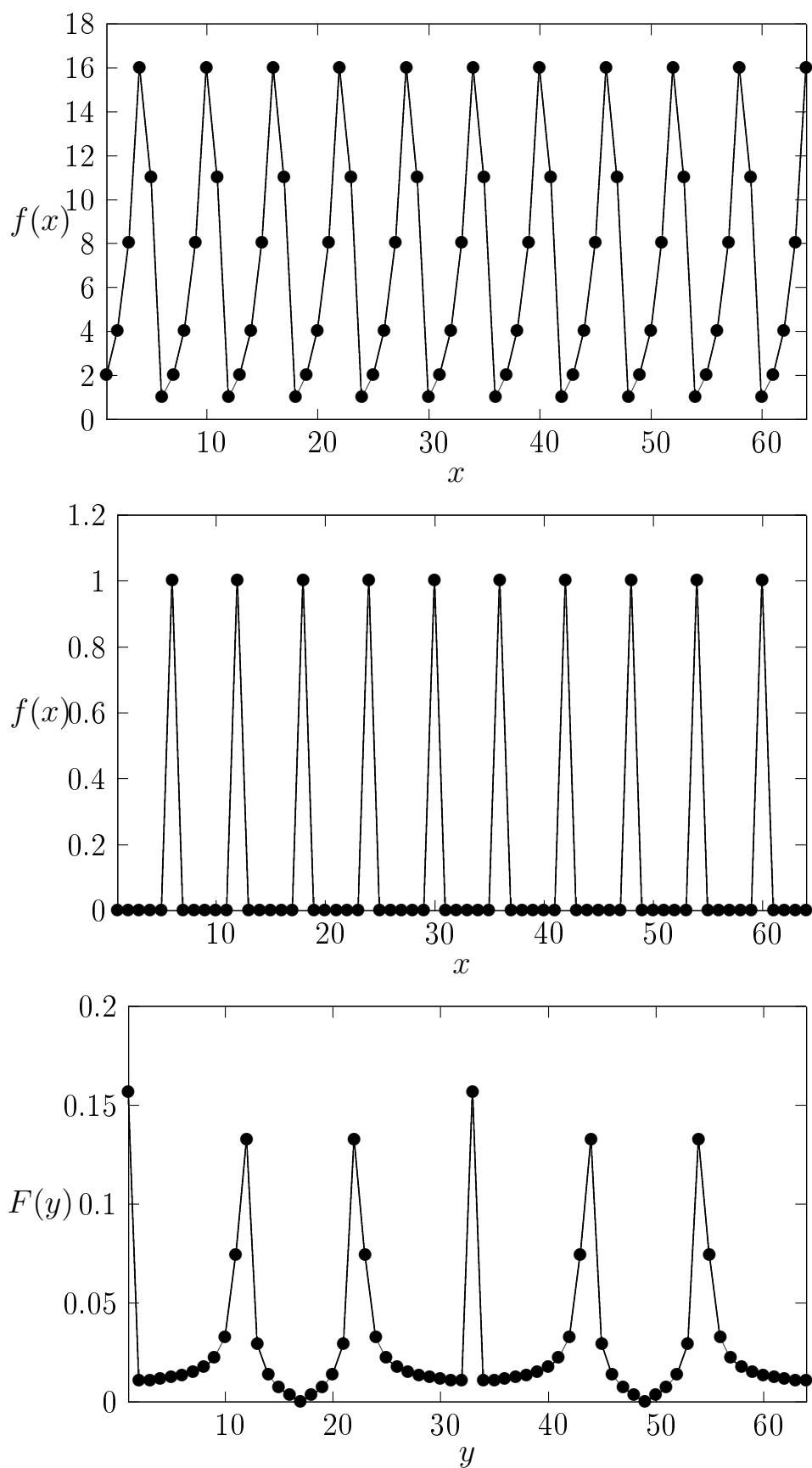


Рис. 13.14: Алгоритм Шора. Нахождение периода функции  $f(x, a) = a^x \bmod N$  при  $a = 2$ ,  $N = 21$  (верхний график). Значение функции 1 повторяется с периодом  $r = 6$  (средний график). Локальные максимумы преобразования Фурье от среднего графика идут с периодом  $\frac{M}{r} \approx 10.67$  (нижний график). См прим. [13.4.1](#)

После измерения значения функции в списке координат останутся только те элементы для которых значение функции будет равно измеренному значению. В результате на вход элемента, измеряющего преобразование Фурье подается состояние вида

$$|in'\rangle = \sum_{x'} |x'\rangle,$$

где все ненулевые элементы имеют одинаковую амплитуду и следуют с периодом равным периоду исследуемой функции. При этом начальное значение будет со сдвигом который зависит от эксперимента (в разных экспериментах будет разный сдвиг). В силу леммы 18.2.1 фурье образ будет одинаковым для различных измерений функций.

Далее в силу леммы 18.2.2 (о периодичности) (см. также комментарий 18.2.1) следует что наиболее вероятные отсчеты (максимумы вероятности) следуют с периодом связанным с исходным периодом функции. Таким образом в результате нескольких экспериментов период искомой функции может быть найден с требуемым уровнем вероятности (см. рис. 13.14).

**Пример 13.4.1.** Нахождение периода функции  $f(x) = 2^x \bmod 21$  В качестве примера рассмотрим задачу о нахождении периода функции  $f(x, a) = a^x \bmod N$  при  $a = 2$ ,  $N = 21$  см. рис. 13.14

Число отсчетов  $M$  должно быть степенью двойки. В нашем примере мы выбираем  $M = 2^6 = 64$  в качестве числа отсчетов. Таким образом необходимо 6 кубит для нашего примера.

Исходное состояние после преобразования Адамара имеет вид:

$$|in\rangle = \frac{1}{8} \sum_{x=0}^{63} |x\rangle \otimes |0\rangle,$$

где  $|x\rangle$  представляет собой тензорное произведение 6 кубит которые кодируют бинарное представление аргумента исследуемой функции. Например при  $x = 5_{10} = 000101_2$  имеем

$$|x\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle$$

После вычисления функции мы имеем состояние вида (см. верхний график на рис. 13.14)

$$\begin{aligned} \hat{U}_f |in\rangle &= \frac{1}{8} \sum_{x=0}^{63} |x\rangle \otimes |f(x)\rangle = \\ &= \frac{1}{8} (|0\rangle \otimes |2\rangle + |1\rangle \otimes |4\rangle + |2\rangle \otimes |8\rangle + \dots + \\ &\quad + |62\rangle \otimes |8\rangle + |63\rangle \otimes |16\rangle). \end{aligned} \quad (13.21)$$

Если результат измерения функции был равен 1, то из всей суммы (13.21) останутся члены для которых значение функции равно 1 (см. средний график на рис. 13.14):

$$|in'\rangle = \frac{1}{\sqrt{10}} (|5\rangle \otimes |1\rangle + |11\rangle \otimes |1\rangle + |17\rangle \otimes |1\rangle + \dots + |60\rangle \otimes |1\rangle). \quad (13.22)$$

Выражение (13.22) содержит 10 членов одинаковой амплитуды, поэтому нормирующий множитель имеет вид  $\frac{1}{\sqrt{10}}$ .

Преобразование Фурье для последовательности (13.22) изображено на нижнем графике рис. 13.14. Наиболее вероятными значениями результата измерения Фурье образа будут значения соответствующие локальным максимумам которые повторяются с периодом  $\frac{M}{r} \approx 10.67$  откуда можно найти период искомой функции  $r = 6$ .

## 13.5 Квантовое преобразование Фурье и дискретное логарифмирование

Дискретный логарифм (см. разд. 19.7) является основой для большого числа современных криптографических алгоритмов (см. разд. 19.9, разд. 19.8). Вместе с тем метод предложенный Шором для факторизации целых чисел может быть также применен для вычисления дискретных логарифмов, что делает возможным взлом соответствующих криптографических алгоритмов.

Поставим задачу следующим образом: имеется выражение

$$b = a^x \mod p,$$

в котором числа  $a, b$  и  $p$  заданны, а число  $x$  является неизвестным, которое необходимо определить. По аналогии с применением квантового преобразования Фурье для факторизации чисел (см. разд. 13.3.1), мы должны построить некоторую периодическую функцию, период которой даст нам возможность определить искомое число  $x$ . Выберем в качестве анализируемой функции

$$f(x_1, x_2) = b^{x_1} a^{x_2} = a^{x \cdot x_1} a^{x_2} \mod p \quad (13.23)$$

В качестве примера мы будем рассматривать квантовый аналог решения задачи из прим. 19.7.1:

**Пример 13.5.1.** ( $ind_3 14 \mod 17$ ) В нашем примере  $p = 17$ ,  $b = 14$  и  $a = 3$ . Функция (13.23) имеет вид

$$f(x_1, x_2) = b^{x_1} a^{x_2} = 14^{x_1} 3^{x_2}.$$

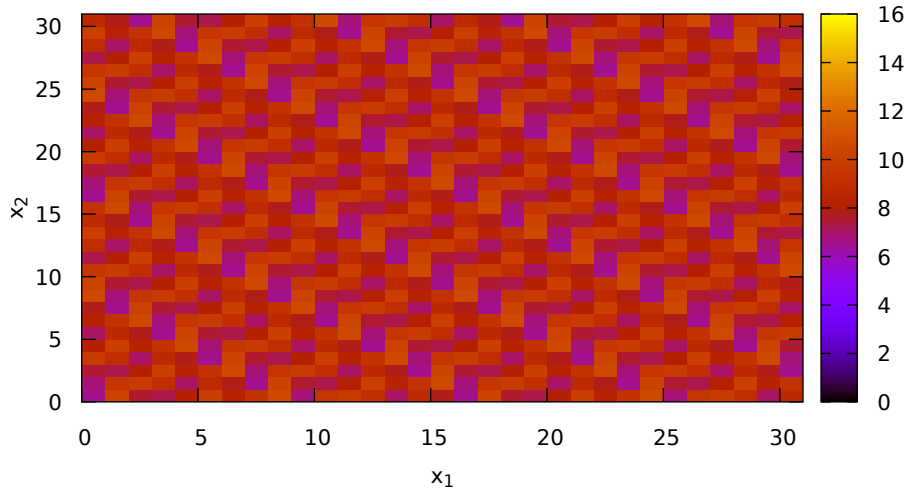


Рис. 13.15: Исследуемая функция  $f(x_1, x_2) = 14^{x_1} 3^{x_2}$

и изображена на [рис. 13.15](#).

$b = 14$ , так же как и  $a = 3$  является генератором  $(\mathbb{Z}/17\mathbb{Z})^\times$ . При этом  $3 \equiv 14^9 \pmod{17}$ . При этом периодами изображенной функции, как это видно из [рис. 13.15](#), будут следующие числа

$$\begin{aligned} t_1 &\equiv 1 \pmod{16}, \\ t_2 &\equiv 9 \pmod{16} \end{aligned} \tag{13.24}$$

В по аналогии с решением задачи факторизации производится измерение этой функции. Допустим в результате измерения мы получили число  $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ . В силу того, что  $a$  является порождающим элементом (см. опред. [16.1.4](#)) мультипликативной группы  $(\mathbb{Z}/p\mathbb{Z})^\times$  (см. опред. [16.1.5](#))  $\exists x_0 : c = a^{x_0}$ . Т. о. с учетом малой теоремы Ферма ([Теорема 19.4.1](#))  $a^{p-1} \equiv 1 \pmod{p}$  и следовательно

$$x_0 \equiv x x_1 + x_2 \pmod{q},$$

где  $q = p - 1$ . Из этого выражения следует, что

$$x_2 \equiv x_0 - x x_1 \pmod{q}.$$

Т. е. если функция является периодической по первому аргументу:

$$f(x_1 + t_1, x_2) = f(x_1, x_2),$$

то она будет периодической по второму аргументу

$$f(x_1, x_2 + t_2) = f(x_1, x_2),$$

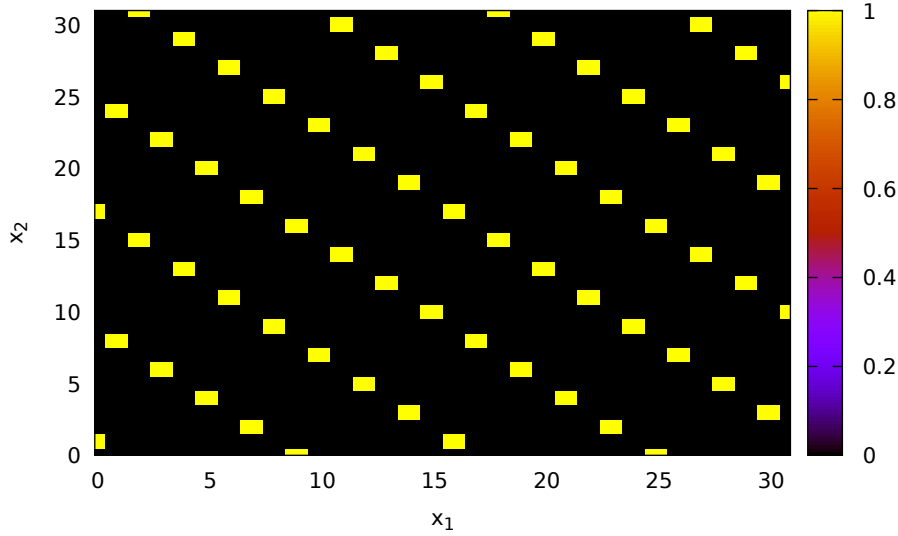


Рис. 13.16: Исследуемая функция  $f(x_1, x_2) = 14^{x_1}3^{x_2}$ . Отмечены только те пары  $x_1, x_2$  при которых  $f(x_1, x_2) = 3, x_0 = 1$ .

при этом

$$t_2 \equiv xt_1 \pmod{q}. \quad (13.25)$$

### 13.5.1 Двумерное преобразование Фурье и период функции $f(x_1, x_2)$

Нашей исследуемой функцией будет являться следующая:

$$f'(x_1, x_2) = \begin{cases} 1, & xx_1 + x_2 \equiv x_0 \pmod{q} \\ 0, & xx_1 + x_2 \not\equiv x_0 \pmod{q} \end{cases} \quad (13.26)$$

#### Пример 13.5.2. ( $\text{ind}_3 14 \pmod{17}$ )

Продолжая пример 13.5.1 допустим, что в результате измерения функции  $f$  мы получили значение  $f = 3$ . Т. е.  $f = a^{x_0} = 3^{x_0} \equiv 3 \pmod{17}$ . В результате для  $x_1, x_2$  останутся только те значения, которые соответствуют наблюдаемому значению функции (см. рис. 13.16), т.е.  $xx_1 + x_2 = x_0 \equiv 1 \pmod{16}$ . При этом при фиксированных значениях  $x, x_1$  и числе отсчетов  $M = q = 16$ .

Для Фурье образа  $\tilde{f}'$  имеем

$$\tilde{f}'(j_1, j_2) = \frac{1}{M} \sum_{x_1=0}^{M-1} \sum_{x_2=0}^{M-1} f'(x_1, x_2) e^{-i\omega(x_1 j_1 + x_2 j_2)}, \quad (13.27)$$

где  $\omega = \frac{2\pi}{M}$ ,  $M$  - число отсчетов.

Прежде всего рассмотрим случай когда  $M = q$ . В этом случае имеется два варианта для  $x_2$ :

1.  $x_2 = x_0 - xx_1$ , если  $x_0 \geq xx_1$
2.  $x_2 = x_0 + q - xx_1$ , если  $x_0 < xx_1$

Т. о.

$$\begin{aligned} e^{-i\omega x_2 j_2} &= e^{-i\omega(x_0 - xx_1 + q)j_2} = \\ &= e^{-i\omega(x_0 - xx_1)j_2 - i\omega q j_2} = e^{-i\omega(x_0 - xx_1)j_2}, \end{aligned}$$

т. е. оба варианта совпадают и могут быть сведены к первому:  $x_2 = x_0 - xx_1$ .

Т. о. продолжая (13.27) получим

$$\begin{aligned} \tilde{f}'(j_1, j_2) &= \frac{1}{M} \sum_{x_1=0}^{M-1} \sum_{x_2=0}^{M-1} f'(x_1, x_2) e^{-i\omega(x_1 j_1 + x_2 j_2)} = \\ &= \frac{1}{M} \sum_{x_1=0}^{M-1} e^{-i\omega(x_1 j_1 + (x_0 - xx_1)j_2)} = \\ &= e^{-i\omega x_0 j_2} \frac{1}{M} \sum_{x_1=0}^{M-1} e^{-i\omega x_1(j_1 - x j_2)} = \frac{1}{M} e^{-i\omega x_0 j_2} \sum_{x_1=0}^{M-1} e^{-i\omega x_1(j_1 - x j_2)}. \end{aligned} \quad (13.28)$$

В выражении (13.28)  $\tilde{f}'(j_1, j_2) = e^{-i\omega x_0 j_2} \neq 0$ , если выполнено

$$j_1 \equiv x j_2 \pmod{M}. \quad (13.29)$$

В противном случае по формуле геометрической прогрессии

$$\begin{aligned} \tilde{f}'(j_1 \neq x j_2, j_2) &= e^{-i\omega x_0 j_2} \frac{1}{M} \sum_{x_1=0}^{M-1} e^{-i\omega x_1(j_1 - x j_2)} = \\ &= \frac{e^{-i\omega x_0 j_2} e^{-i\omega M(j_1 - x j_2)} - 1}{M \frac{e^{-i\omega(j_1 - x j_2)} - 1}{e^{-i\omega x_0 j_2} e^{-i\omega M(j_1 - x j_2)} - 1}} = \\ &= \frac{e^{-i\omega x_0 j_2} e^{-i\omega M(j_1 - x j_2)} - 1}{M \frac{e^{-i\omega(j_1 - x j_2)} - 1}{e^{-i\omega x_0 j_2} e^{-i\omega M(j_1 - x j_2)} - 1}} = 0. \end{aligned}$$

Т. о. для определения периода нам необходимо найти координаты  $(j_1, j_2)$  некоторого максимума преобразования Фурье и воспользоваться выражением

$$x \equiv j_1 j_2^{-1} \pmod{M}, \quad (13.30)$$

которое следует из (13.29).

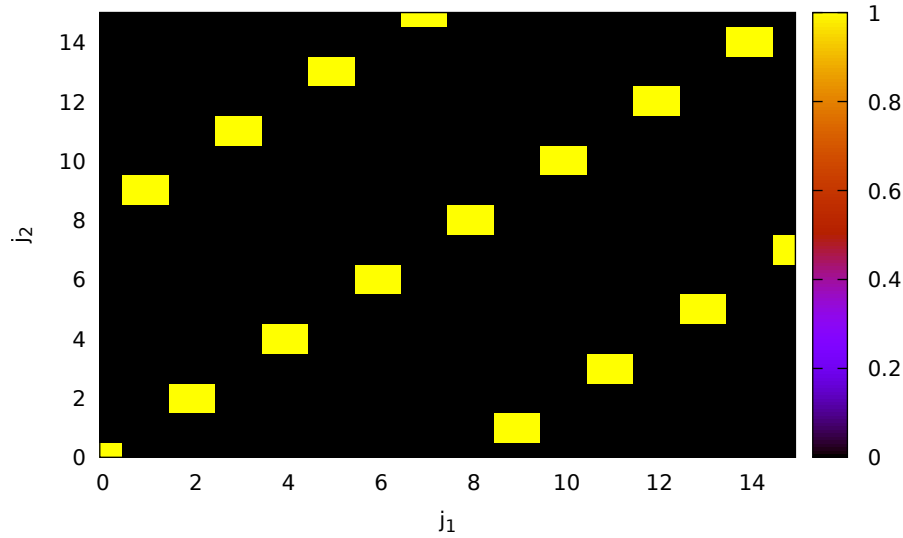


Рис. 13.17: Фурье образ функции с рис. 13.16. Число отсчетов  $M = 16$ . Координаты максимума  $j_1 = 9$ ,  $j_2 = 1$ . Решением уравнения  $3^x \equiv 14 \pmod{17}$  является  $x \equiv 9 \cdot 1^{-1} \equiv 9 \pmod{16}$ . С учетом того, что период меньше числа отсчетов, можно заключить, что  $x = 9$

**Комментарий 13.5.1** (О делителях нуля  $\mathbb{Z}/M\mathbb{Z}$ ). Если существует такое число  $y$ , что

$$j_2 y \equiv 0 \pmod{M},$$

то  $j_2$  называется делителем нуля. При этом очевидно также, что

$$\text{НОД}(j_2, M) \neq 1,$$

таким образом из [разд. 19.2.2](#) следует что  $j_2^{-1}$  не существует. Следовательно для таких  $j_2$  выражение (13.30) не определено. В этом случае необходимо использовать другие координаты  $(j_1, j_2)$ .

**Пример 13.5.3.** ( $\text{ind}_3 14 \pmod{17}$ )

Фурье образ функции с [рис. 13.16](#) изображен на [рис. 13.17](#) из которого видно, что с наибольшей вероятностью будут регистрироваться отсчеты которые следуют с интервалом  $T_{j_1} = 9$  по координате  $j_1$  и с интервалом  $T_{j_2} = 1$  по координате  $j_2$ . С учетом того, что число отсчетов  $M = 16$  можно получить координаты максимума преобразования Фурье  $j_1 = 9$  и  $j_2 = 1$ . Решением уравнения  $3^x \equiv 14 \pmod{17}$  является, в соответствии с (13.30),  $x = 9 \cdot 1^{-1} = 9$ , что соответствует результату прим. 19.7.1.

Аналогичный результат можно получить, если взять точку с координатами  $j_1 = 11, j_2 = 3$ . С учетом  $3 \cdot 11 = 33 \equiv 1 \pmod{16}$  имеем  $j_2^{-1} \equiv 11 \pmod{16}$ , т. е.  $x \equiv 11 \cdot 11 \equiv 121 \equiv 9 \pmod{16}$ , что опять же соответствует результату прим. 19.7.1.

Стоит отметить, что точки лежащие на диагонали, например  $j_1 = 6, j_2 = 6$  не дадут корректного результата потому как  $\text{НОД}(6, 16) = 2 \neq 1$

Стоит отметить, что полученный результат (13.30) находится в прямом соответствии с леммой 18.2.2 для одномерного преобразования Фурье. При этом также имеет место и аналог комментария 18.2.1, который гласит, что в случае когда число отсчетов преобразования Фурье не равно  $q$ :  $M \neq q$ , но при этом  $M \approx q$ , мы можем все равно приближенно считать верным выражение (13.30) [17].

**Пример 13.5.4.** ( $\text{ind}_2 14 \bmod 59$ )

В качестве примера рассмотрим  $p = 59$  при этом число отсчетов  $M = 64 \approx q = p - 1 = 58$ . Генератором группы  $\mathbb{F}_{59}$  (см. разд. 19.2.3) является  $g = 2$ , т. е.  $\mathbb{F}_{59} = \langle 2 \rangle$ . Это значит, что уравнение  $2^x \equiv b \bmod 59$  будет иметь решение для любых  $b$ , в частности  $x = 19$  является решением уравнения

$$2^x \equiv 14 \bmod 59.$$

Исследуемая функция имеет вид

$$f(x_1, x_2) = 14^{x_1} 2^{x_2} \bmod 59,$$

Допустим, что  $x_0 = 50$ , т.е. зарегистрировано значение функции  $f(x_1, x_2) = 2^{x_0} = 2^{50} \equiv 3 \bmod 59$ .

Как было указано выше, для числа отсчетов преобразования Фурье имеем  $M = 64$ . Стоит отметить, что  $q = p - 1 = 58 \not\equiv 0 \bmod 64$ .

Фурье образ отсчетов функции

$$f'(x_1, x_2) = \begin{cases} 1, & \text{если } 14^{x_1} 2^{x_2} \equiv 3 \bmod 59 \\ 0, & \text{если } 14^{x_1} 2^{x_2} \not\equiv 3 \bmod 59 \end{cases}$$

изображен на рис. 13.18. Три нижних максимума имеют координаты

$$(j_1, j_2) \approx (20, 1), (41, 2.2), (62, 3),$$

что дает следующие оценки для  $x$ :  $x \approx 20, 18.6, 20.6$ , что находится близко к реальному значению  $x = 19$ .

**Пример 13.5.5.** ( $\text{ind}_3 14 \bmod 19$ )

В качестве примера рассмотрим задачу определения  $x$  такого, что

$$3^x \equiv 14 \bmod 19.$$



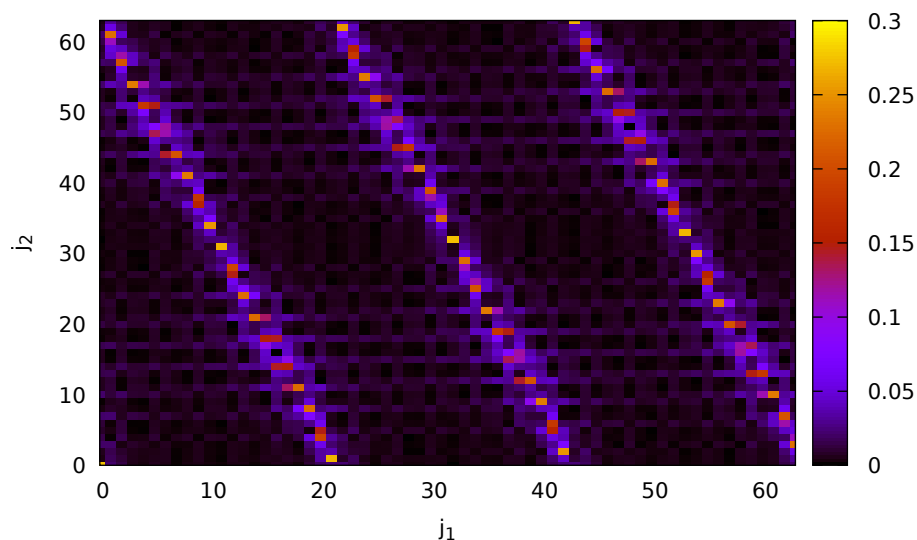


Рис. 13.18: Фурье образ отсчетов функции  $f'(x_1, x_2)$  Число отсчетов  $M = 64$ . Три нижних максимума имеют координаты  $\approx (20, 1), (41, 2.2), (62, 3)$ , что дает следующие оценки для  $x$ :  $x \approx 20, 18.6, 20.6$ , что находится близко к реальному значению  $x = 19$

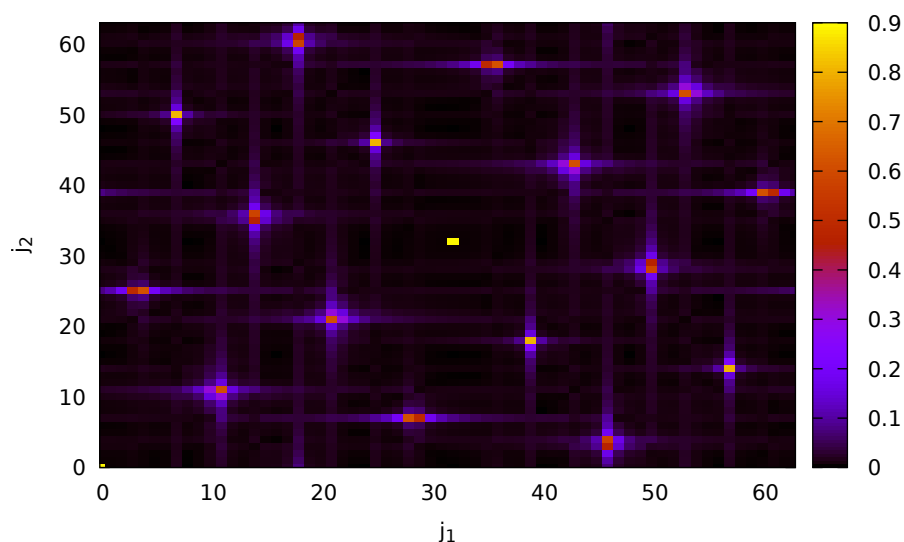


Рис. 13.19: Фурье образ отсчетов функции  $f'(x_1, x_2)$  Число отсчетов  $M = 64$ . Координаты максимума  $j_1 \approx 46, j_2 \approx 3.5$ . Решением уравнения  $3^x \equiv 14 \pmod{19}$  является  $x = 13 \approx \frac{46}{3.5} \approx 13.14$

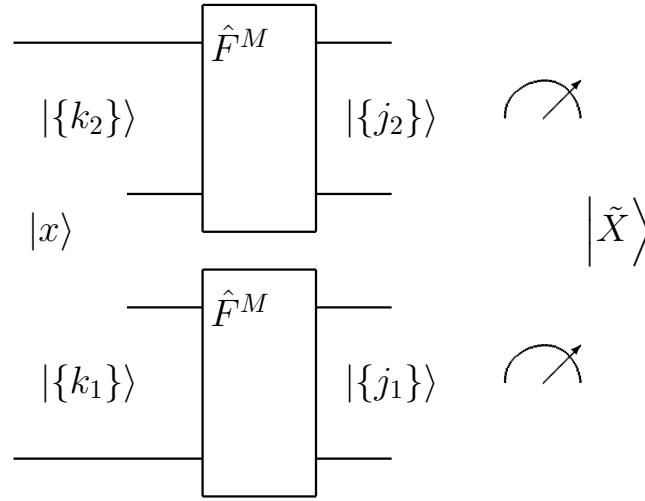


Рис. 13.20: Схема двумерного квантового преобразования Фурье. На входе имеем сигнал  $|x\rangle = \sum_{k_1, k_2=0}^{M-1} x(k_1, k_2) |k\rangle_1 \otimes |k\rangle_2$ . Сигнал на выходе  $|\tilde{X}\rangle = \sum_{k_1, k_2=0}^{M-1} \tilde{X}(j_1, j_2) |j_1\rangle \otimes |j_2\rangle$  является двумерным преобразованием Фурье от исходного  $|x\rangle$

Исследуемая функция имеет вид

$$f(x_1, x_2) = 14^{x_1} 3^{x_2} \mod 19,$$

Допустим, что  $x_0 = 1$ , т.е. зарегистрировано значение функции  $f(x_1, x_2) = 3$ .

Число отсчетов преобразования Фурье возьмем  $M = 64$ . Стоит отметить, что  $18 \not\equiv 0 \mod 64$ .

Фурье образ отсчетов функции

$$f'(x_1, x_2) = \begin{cases} 1, & \text{если } 14^{x_1} 3^{x_2} \equiv 3 \mod 19 \\ 0, & \text{если } 14^{x_1} 3^{x_2} \not\equiv 3 \mod 19 \end{cases}$$

изображен на [рис. 13.19](#). Самый нижний максимум имеет координаты  $j_1 = 46, j_2 = 3.5$  откуда имеем для оценки

$$x \approx \frac{46}{3.5} \approx 13.14.$$

Стоит отметить что решение искомого уравнения  $x = 13$  соответствует найденному приближенному решению.

### 13.5.2 Двумерное квантовое преобразование Фурье

Для определения периодов функции двух аргументов можно воспользоваться двумерным преобразованием Фурье, которое может быть построено из

блоков осуществляющих одномерное преобразование Фурье, как это изображено на [рис. 13.20](#). Для анализа этой схемы рассмотрим тривиальный случай когда на входе имеем (см. также (13.10))

$$\begin{aligned} |x\rangle &= |x\rangle_1 \otimes |x\rangle_2, \\ |x\rangle_{1,2} &= \sum_{k_{1,2}=0}^{M-1} x_{k_{1,2}}^{(1,2)} |k_{1,2}\rangle. \end{aligned}$$

С учетом того, что на выходе получается

$$|\tilde{X}\rangle = |\tilde{X}_1\rangle \otimes |\tilde{X}_2\rangle,$$

где

$$|\tilde{X}_{1,2}\rangle = \sum_{j_{1,2}=0}^{M-1} \tilde{X}_{j_{1,2}}^{(1,2)} |j_{1,2}\rangle$$

и в соответствии с (13.12)

$$\tilde{X}_{j_{1,2}}^{(1,2)} = \frac{1}{\sqrt{M}} \sum_{k_{1,2}=0}^{M-1} e^{-i\omega_{1,2}k_{1,2}j_{1,2}} x_{k_{1,2}}^{(1,2)}.$$

получим

$$\begin{aligned} |\tilde{X}\rangle &= |\tilde{X}_1\rangle \otimes |\tilde{X}_2\rangle = \\ &= \sum_{j_1=0}^{M-1} \sum_{j_2=0}^{M-1} \tilde{X}_{j_1}^{(1)} \tilde{X}_{j_2}^{(2)} |j_1\rangle \otimes |j_2\rangle = \\ &= \sum_{j_1=0}^{M-1} \sum_{j_2=0}^{M-1} \tilde{X}_{j_1, j_2} |j_1\rangle \otimes |j_2\rangle, \end{aligned}$$

где

$$\begin{aligned} \tilde{X}_{j_1, j_2} &= \frac{1}{(\sqrt{M})^2} \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1} e^{-i\omega(k_1 j_1 + k_2 j_2)} x_{k_1}^{(1)} x_{k_2}^{(2)} = \\ &= \frac{1}{(\sqrt{M})^2} \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1} e^{-i\omega(k_1 j_1 + k_2 j_2)} x_{k_1, k_2} \end{aligned}$$

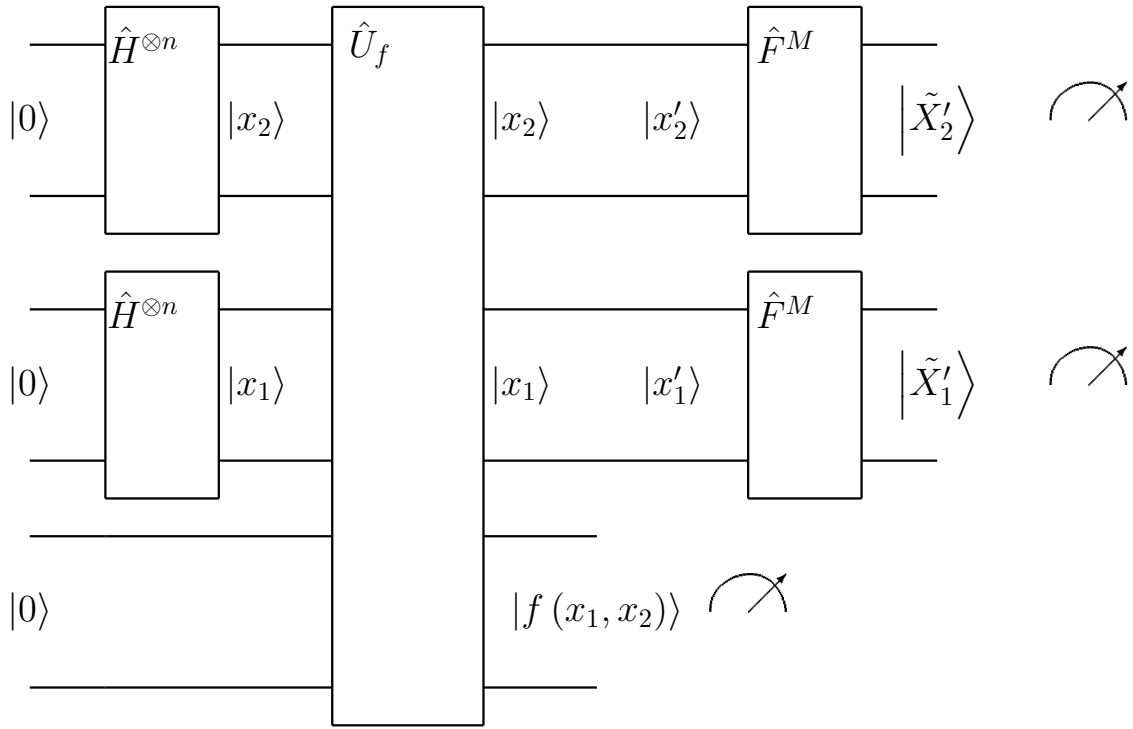


Рис. 13.21: Определение периода функций двух аргументов с помощью квантового преобразования Фурье

что, в соответствии с определением 18.3.1, является двумерным преобразованием Фурье от исходного двумерного сигнала

$$|x\rangle = \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1} x_{k_1}^{(1)} x_{k_2}^{(2)} |k_1\rangle \otimes |k_2\rangle = \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1} x_{k_1, k_2} |k_1\rangle \otimes |k_2\rangle.$$

Следовательно используя схему, изображенную на рис. 13.21 можно определить координаты максимумов двумерного преобразования Фурье  $j_1, j_2$  и в дальнейшем используя (13.30) определить искомое  $x$ .

## 13.6 Алгоритм Шора и дискретный логарифм на эллиптических кривых

Рассмотрим эллиптическую кривую

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p, y^2 = x^3 + ax + b, \}$$

с заданной базовой точкой  $g \in E(\mathbb{F}_p)$  такой что:

$$ng = 0.$$

Требуется решить следующую задачу: при заданном  $q \in E(\mathbb{F}_p)$  найти такое  $x$ , что

$$xg = q \pmod n \quad (13.31)$$

Рассмотрим следующую вспомогательную функцию

$$f(x_1, x_2) = x_1q + x_2g = (xx_1 + x_2)g, \quad (13.32)$$

где  $q, g \in E(\mathbb{F}_p)$  и взяты из условий нашей задачи (13.31). Данная функция аналогична (13.23) использованной в решении задачи дискретного логарифма. Далее производится измерение этой функции. Результатом этого измерения является некоторая точка  $s \in E(\mathbb{F}_p)$ . Вместе с тем из (13.32) следует что  $s \in \langle g \rangle$ , т.е.  $\exists x_0$  такая что  $s = x_0g$ .

Т.о., по аналогии с (13.26), мы составляем следующую функцию

$$f'(x_1, x_2) = \begin{cases} 1, & xx_1 + x_2 \equiv x_0 \pmod n \\ 0, & xx_1 + x_2 \not\equiv x_0 \pmod n \end{cases} \quad (13.33)$$

Координаты  $(j_1, j_2)$  максимума Фурье образа  $\tilde{f}'$  дают в соответствии с формулой (13.30) некоторое значение искомого числа  $x$ . В нашем случае практически всегда  $n \neq M$  поэтому мы можем использовать только приближенную оценку

$$x \approx \frac{j_1}{j_2}.$$

**Пример 13.6.1** (Дискретное логарифмирование на эллиптической кривой). Рассмотрим задачу из примера 19.11.1 Кривая и базовая точка (см. прим. 19.10.2) имеют вид

$$(p, a, b, g, n, h) = (97, -7, 10, (96, 93), 41, 2)$$

Допустим, что нам известен публичный ключ Алисы

$$A = (37, 35)$$

и мы хотим найти такое  $x \in \{0, 1, \dots, 40\}$  что  $xg = A$ , как это следует из примера 19.11.1 ответом является  $x = d_a = 5$ . Нашей исследуемой функцией будет являться

$$f(x_1, x_2) = x_1A + x_2g = x_1(37, 35) + x_2(96, 93)$$

В качестве результата измерения выберем  $s = g$ , т.е.  $x_0 = 1$ . График функции  $f'(x_1, x_2)$ , соответствующей этому измерению изображен на

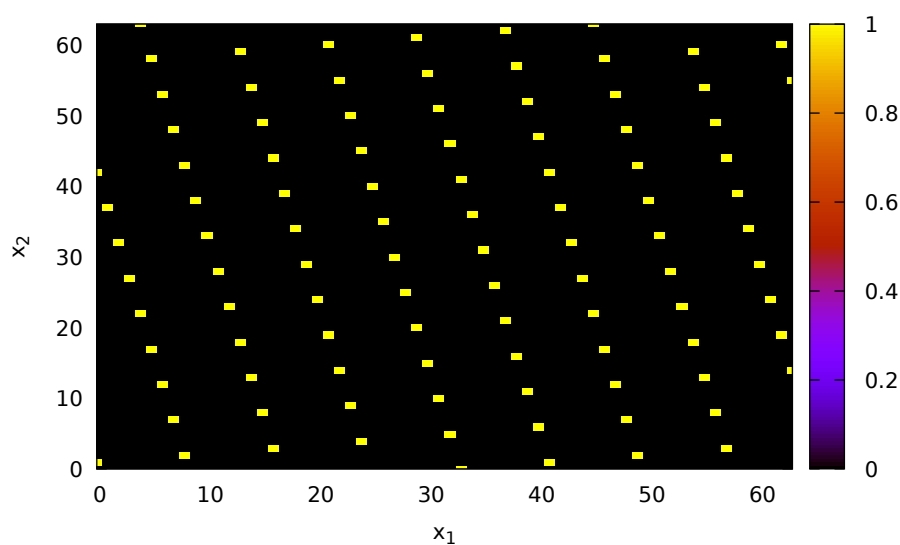


Рис. 13.22: График функции  $f'(x_1, x_2)$  при  $x_0 = 1$ . Т.о. изображены точки  $x_1, x_2$  соответствующие соотношению  $x_1A + x_2g = g$ :  $x_1(37, 35) + x_2(96, 93) = (96, 93)$ , например  $7(37, 35) + 7(96, 93) = (96, 93)$ ,  $8(37, 35) + 2(96, 93) = (96, 93)$  или  $16(37, 35) + 3(96, 93) = (96, 93)$ . Стоит отметить, что выбранные пары точек соответствуют условию (13.33), действительно имеем  $x \cdot 7 + 7 \equiv x \cdot 8 + 2 \pmod{41}$ . То есть если вычесть одно из другого то получим уравнение вида  $x(8 - 7) = -(2 - 7) = 5 \pmod{41}$ . Или же  $x \equiv 5 \pmod{41}$

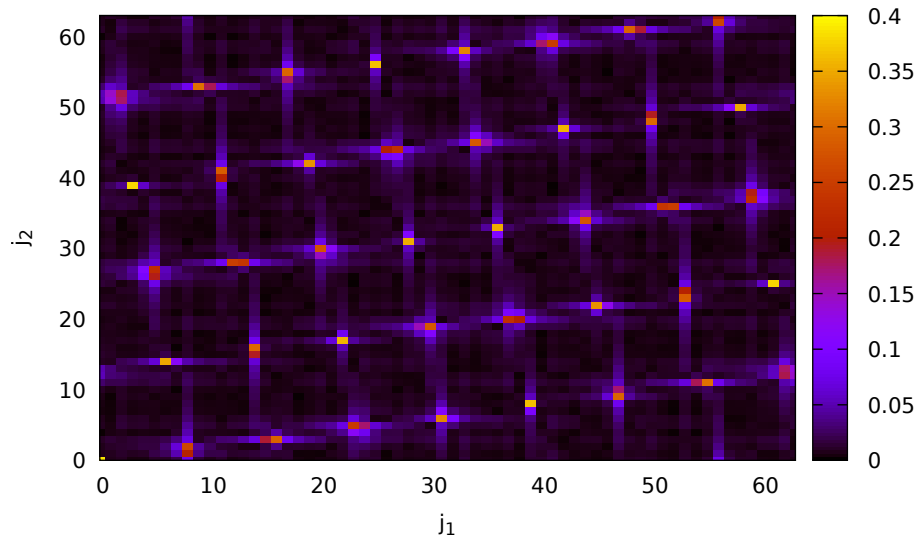


Рис. 13.23: Фурье образ отсчетов функции  $f'(x_1, x_2)$  Число отсчетов  $M = 64$ . Три левых нижних максимума имеют координаты  $\approx (8, 2), (15, 3), (24, 5)$ , что дает следующие оценки для  $x$ :  $x \approx 4, 5, 4.8$ , что находится близко к реальному значению  $x = 5$

*рис. 13.22.* Стоит отметить, что функция  $f'(x_1, x_2)$  периодическая и если взять любые две близко стоявшие точки например  $(8, 2)$  и  $(16, 3)$  то можно заметить, что период по координате  $x_1$  равен  $T_1 = 8$ , а по координате  $x_2$  -  $T_2 = 1$ . Решая уравнение  $x = T_2 T_1^{-1} \bmod n$  получим  $x = 8^{-1} \equiv 5 \bmod 41$ , что соответствует искомому решению.

Фурье образ функции  $f'(x_1, x_2)$ , изображен на [рис. 13.23](#). Из него можно найти искомое  $x = 5$ .

## 13.7 Алгоритм Гровера

Рассмотрим следующую задачу. Допустим имеется большой набор данных состоящий из  $N$  элементов в котором необходимо найти элемент удовлетворяющий некоторым условиям (см. [рис. 13.24](#)). Если данные отсортированы, то с помощью алгоритмов типа “разделяй и властвуй” искомый элемент может быть найден за время порядка  $O(\log N)$  (см. [разд. 20.2](#)). В ряде случаев исходный набор данных не может быть подготовлен для быстрого поиска, в этом случае классический поиск осуществляется за время порядка  $O(N)$ .

Одним из примеров являются алгоритмы симметричного шифрования в которых стоит задача определения ключа по известному зашифрованному тексту и соответствующему ему оригинальному тексту. В этом случае предварительная обработка данных представляется невозможной и решением задачи

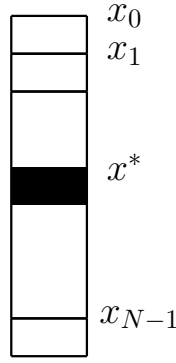


Рис. 13.24: Поиск в неструктурированном объеме данных (поиск "иголки в стоге сена")

“в лоб” является простой перебор всех возможных значений.

Алгоритм Гровера [9] решает задачу неструктурированного поиска за время порядка  $O(\sqrt{N})$ .

### 13.7.1 Описание алгоритма

Допустим у нас имеется квантовый контур который вычисляет значение функции  $f(x)$  которая может принимать только два значения: 0 и 1. При этом значение 1 справедливо только для искомого элемента:

$$\begin{aligned} f(x)|_{x=x^*} &= 1, \\ f(x)|_{x \neq x^*} &= 0. \end{aligned} \quad (13.34)$$

На рис. 13.25 изображена схема для вычисления искомой функции. На выходе мы имеем состояние вида

$$|out\rangle = \frac{1}{\sqrt{N}} \left( \sum_{x \neq x^*} |x\rangle \otimes |0\rangle + |x^*\rangle \otimes |1\rangle \right), \quad (13.35)$$

где  $N$  - общее число элементов в последовательности в которой производится поиск.

Если посмотреть на выражение (13.35), то можно заметить, что предложенная схема, несмотря на то что она производит вычисление функции в искомой точке, не позволяет выбрать искомый элемент, потому что все элементы результирующей последовательности равновероятны, т. е. каждый элемент может быть выбран (в результате измерения) с одинаковой вероятностью:  $\frac{1}{N}$ .



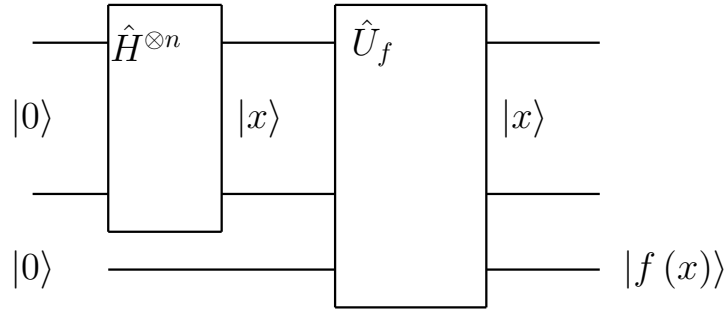


Рис. 13.25: Вычисление функции  $f(x)$ . На выходе схемы имеем суперпозицию состояний вида  $\frac{1}{\sqrt{N}} \left( \sum_{x \neq x^*} |x\rangle \otimes |0\rangle + |x^*\rangle \otimes |1\rangle \right)$

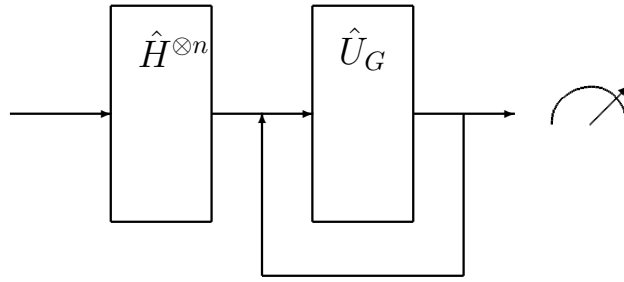


Рис. 13.26: Алгоритм Гровера

Гровером был предложен алгоритм, который позволил бы повысить вероятность обнаружения искомого элемента в результирующей суперпозиции (13.35).

Схема, реализующая алгоритм Гровера представляет собой некоторый блок, описываемый оператором  $\hat{U}_G$ , который повторяется некоторое число раз (см. рис. 13.26). При этом на каждом шаге итерации вероятность обнаружения искомого элемента повышается.

Базовый элемент  $\hat{U}_G$  представляет собой последовательное действие двух операторов (см. рис. 13.27):

$$\hat{U}_G = \hat{U}_s \hat{U}_{x^*},$$

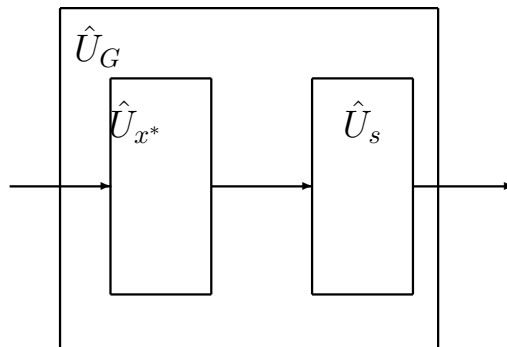


Рис. 13.27: Алгоритм Гровера. Базовый элемент

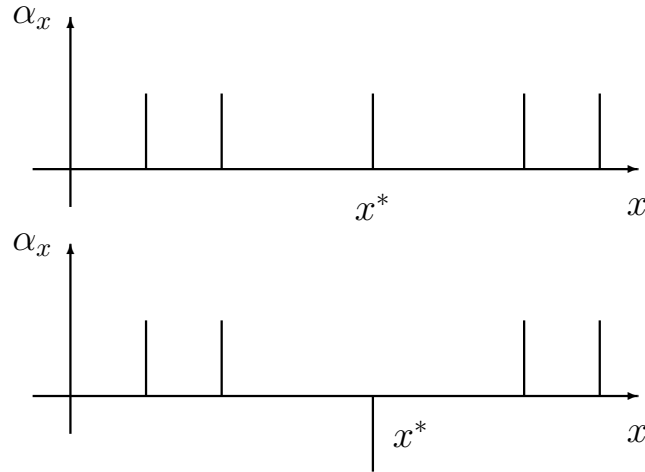


Рис. 13.28: Алгоритм Гровера. Инверсия фазы. Описывается следующим соотношением  $\hat{U}_{x^*} (\sum_x \alpha_x |x\rangle) = \sum_x \alpha_x (-1)^{f(x)} |x\rangle$

где  $\hat{U}_{x^*}$  - оператор инверсии фазы,  $\hat{U}_s$  - оператор обращения относительно среднего.

Действие оператора  $\hat{U}_{x^*}$  описывается следующим соотношением (см. [рис. 13.28](#)):

$$\hat{U}_{x^*} \left( \sum_x \alpha_x |x\rangle \right) = \sum_x \alpha_x (-1)^{f(x)} |x\rangle. \quad (13.36)$$

Оператор  $\hat{U}_{x^*}$  может быть переписан в виде

$$\hat{U}_{x^*} = \hat{I} - 2 |x^*\rangle \langle x^*|.$$

Действительно

$$\begin{aligned} & \left( \hat{I} - 2 |x^*\rangle \langle x^*| \right) \left( \sum_x \alpha_x |x\rangle \right) = \\ &= \sum_x \alpha_x |x\rangle - 2\alpha_{x^*} |x^*\rangle = \sum_{x \neq x^*} \alpha_x |x\rangle - \alpha_{x^*} |x^*\rangle = \\ &= \sum_x \alpha_x (-1)^{f(x)} |x\rangle, \end{aligned}$$

что совпадает с (13.36).

Действие оператора  $\hat{U}_s$  описывается следующим соотношением (см. [рис. 13.29](#)):

$$\hat{U}_s \left( \sum_x \alpha_x |x\rangle \right) = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle, \quad (13.37)$$

где  $\mathcal{M} = \sum_x \frac{\alpha_x}{N}$ .

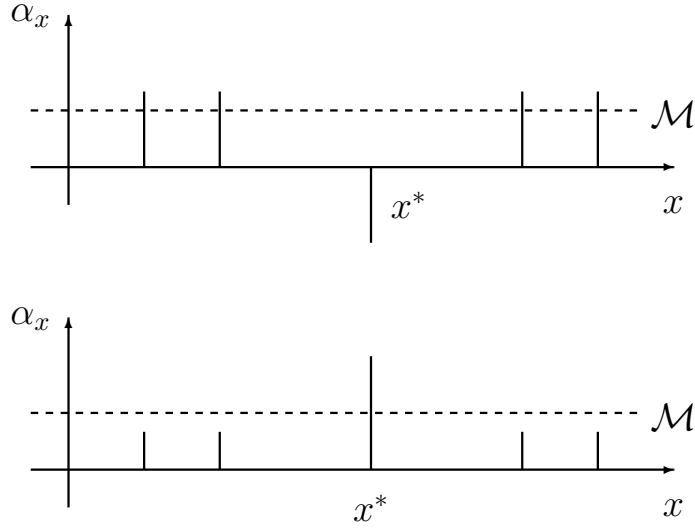


Рис. 13.29: Алгоритм Гровера. Обращение относительно среднего. Описывается следующим соотношением  $\hat{U}_s (\sum_x \alpha_x |x\rangle) = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle$

Оператор  $\hat{U}_s$  может быть переписан в следующем виде

$$\hat{U}_s = 2|s\rangle\langle s| - \hat{I},$$

где  $|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$  - начальное состояние в алгоритме Гровера. Действительно

$$\begin{aligned} & \left( 2|s\rangle\langle s| - \hat{I} \right) \left( \sum_x \alpha_x |x\rangle \right) = \\ &= 2 \sum_x \alpha_x \langle s|x\rangle |s\rangle - \sum_x \alpha_x |x\rangle = \\ &= \frac{2}{N} \sum_x \alpha_x \sum_x |x\rangle - \sum_x \alpha_x |x\rangle = \\ &= \sum_x (2\mathcal{M} - \alpha_x) |x\rangle, \end{aligned}$$

что совпадает с (13.37).

### 13.7.2 Анализ алгоритма Гровера

Схематическая форма записи алгоритма Гровера приведена в алг. 2.

Нас будет интересовать два вопроса: какова алгоритмическая сложность алгоритма Гровера и существуют ли алгоритмы которые могут выполнять задачу поиска в неструктурированном объеме данных более эффективно чем алгоритм Гровера.

---

**Алгоритм 2** Алгоритм Гровера
 

---

```

 $|\psi\rangle_0 \leftarrow \frac{1}{\sqrt{N}} \sum_x |x\rangle$ 
 $t \leftarrow 1$ 
repeat
   $|\psi\rangle_t \leftarrow \hat{U}_s \hat{U}_{x^*} |\psi\rangle_{t-1}$ 
   $t \leftarrow t + 1$ 
until  $(t < \frac{\pi}{4} \sqrt{N})$ 
return результат измерения состояния  $|\psi\rangle_t$ 

```

---

Критерием эффективности алгоритма служит следующий факт: хороший алгоритм должен находить искомое значение с минимальным числом вызовов функции (13.34).

Рассмотрим самую первую итерацию. Начальное состояние  $|\psi\rangle_0$  имеет следующий вид

$$|\psi\rangle_0 = \sum_x \alpha_x |x\rangle = |s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle + \frac{1}{\sqrt{N}} |x^*\rangle.$$

Таким образом коэффициент перед искомым элементом имеет вид  $\alpha_x^* = \frac{1}{\sqrt{N}}$ .

После применения оператора инверсии фазы  $U_{x^*}$  из (13.36) получим

$$\hat{U}_{x^*} |\psi\rangle_0 = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle - \frac{1}{\sqrt{N}} |x^*\rangle = \sum_x \beta_x |x\rangle,$$

где  $\beta_{x^*} = -\frac{1}{\sqrt{N}}$  и  $\beta_{x \neq x^*} = \frac{1}{\sqrt{N}}$ .

После применения оператора обращения относительно среднего  $\hat{U}_s$  из (13.37) получим

$$\begin{aligned} \hat{U}_G |\psi\rangle_0 &= \hat{U}_s \hat{U}_{x^*} |\psi\rangle_0 = \hat{U}_s \sum_x \beta_x |x\rangle = \\ &= \sum_x (2M - \beta_x) |x\rangle \approx \sum_{x \neq x^*} \left( 2\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}} \right) |x\rangle + \\ &+ \left( 2\frac{1}{\sqrt{N}} + \frac{1}{\sqrt{N}} \right) |x^*\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle + \frac{3}{\sqrt{N}} |x^*\rangle. \end{aligned} \quad (13.38)$$

При выводе (13.38) было принято

$$\mathcal{M} = \frac{\sum_x \alpha_x}{N} \approx \frac{N}{N\sqrt{N}} = \frac{1}{\sqrt{N}}.$$



Рис. 13.30: Алгоритм Гровера. Реализация инверсии фазы (оператор  $\hat{U}_{x^*}$ ). Приняв  $b = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$  получим для изображенной схемы  $\hat{U}_f(\sum_x \alpha_x |x\rangle) \otimes |-\rangle = \sum_x \alpha_x (-1)^{f(x)} |x\rangle \otimes |-\rangle$

Таким образом после первой итерации алгоритма Гровера амплитуда  $\alpha_{x^*}$  возросла на  $\frac{2}{\sqrt{N}}$ . Если аппроксимировать этот результат на произвольную итерацию, то можно получить, что 50% вероятность обнаружить  $|x^*\rangle$  будет достижима за следующее число итераций:

$$\frac{1}{\sqrt{2}} / \frac{2}{\sqrt{N}} = \frac{\sqrt{N}}{2\sqrt{2}} = O(\sqrt{N}).$$

Более точные расчеты [16] дают для числа итераций  $\frac{\pi}{4}\sqrt{N}$ .

Можно задать вопрос об оптимальности алгоритма Гровера: существует ли квантовый алгоритм, который выполняет поиск в неструктурированном объеме данных быстрее чем за  $O(\sqrt{N})$  обращений к функции (13.34). В статье [23] показано, что такого алгоритма не существует.

### 13.7.3 Реализация базовых элементов алгоритма Гровера

#### Инверсия фазы

Каким образом может быть реализована инверсия фазы: как выглядит квантовый логический элемент который осуществляет преобразование (13.36), т. е. каким образом  $f(x)$  может быть “послано” в фазу?

Рассмотрим схему изображенную на рис. 13.30. Предложенная схема осуществляет следующее преобразование:

$$|x\rangle \otimes |b\rangle \rightarrow |x\rangle \otimes |b \oplus f(x)\rangle,$$

где введено следующее обозначение:  $a \oplus b = a + b \pmod{2}$ .

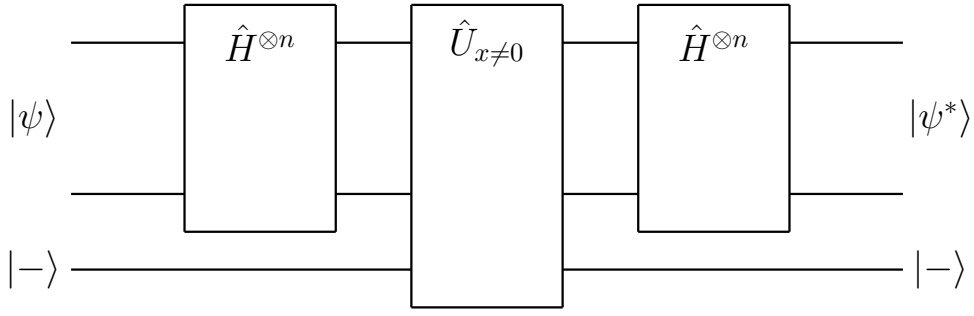


Рис. 13.31: Алгоритм Гровера. Реализация обращения относительно среднего (оператор  $\hat{U}_s$ ):  $|\psi\rangle \otimes |-\rangle \rightarrow |\psi^*\rangle \otimes |-\rangle$ , где  $|\psi\rangle = \sum_x \alpha_x |x\rangle$ ,  $|\psi^*\rangle = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle$ . Предложенная схема осуществляет следующее преобразование:  $\hat{H}^{\otimes n} \hat{U}_{x \neq 0} \hat{H}^{\otimes n} \sum_x \alpha_x |x\rangle \otimes |-\rangle = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle \otimes |-\rangle$

Для случая  $|b\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$  имеем

$$\begin{aligned}
 |x\rangle \otimes |-\rangle &\rightarrow |x\rangle \otimes \left( \frac{|0 \oplus 0\rangle - |1 \otimes 0\rangle}{\sqrt{2}} \right) = \\
 &= |x\rangle \otimes \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \otimes |-\rangle, x \neq x^*, \\
 |x\rangle \otimes |-\rangle &\rightarrow |x\rangle \otimes \left( \frac{|0 \oplus 1\rangle - |1 \oplus 1\rangle}{\sqrt{2}} \right) = \\
 &= |x\rangle \otimes \left( \frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) = -|x\rangle \otimes |-\rangle, x = x^*,
 \end{aligned}$$

т. о. мы имеем следующее преобразование

$$|x\rangle \otimes |-\rangle \rightarrow (-1)^{f(x)} |x\rangle \otimes |-\rangle. \quad (13.39)$$

### Обращение относительно среднего

Рассмотрим схему изображенную на рис. 13.31. Элемент  $\hat{U}_{x \neq 0}$  осуществляет преобразование аналогичное (13.39) при этом функция  $f(x=0) = 0$ , и  $f(x \neq 0) = 1$ , т. о.

$$\begin{aligned}
 \hat{U}_{x \neq 0} |x\rangle \otimes |-\rangle &= |x\rangle \otimes |-\rangle, x = 0, \\
 \hat{U}_{x \neq 0} |x\rangle \otimes |-\rangle &= -|x\rangle \otimes |-\rangle, x \neq 0,
 \end{aligned}$$

т. е. матрица преобразования выглядит следующим образом

$$\begin{aligned}\hat{U}_{x \neq 0} &= \begin{pmatrix} 1 \otimes |-\rangle & 0 & 0 & \cdots & 0 \\ 0 & -1 \otimes |-\rangle & 0 & \cdots & 0 \\ 0 & 0 & -1 \otimes |-\rangle & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \otimes |-\rangle \end{pmatrix} = \\ &= \left\{ \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\} \otimes |-\rangle.\end{aligned}$$

Объединяя этот результат с двумя преобразованиями Адамара , и воспользовавшись (13.4), получаем:

$$\begin{aligned}\hat{H}^{\otimes n} &\left\{ \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\} \otimes |-\rangle \hat{H}^{\otimes n} = \\ &= \left\{ \hat{H}^{\otimes n} \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \hat{H}^{\otimes n} - \hat{H}^{\otimes n} \hat{I} \hat{H}^{\otimes n} \right\} \otimes |-\rangle = \\ &= \left\{ \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix} - \hat{I} \right\} \otimes |-\rangle = \\ &= \left\{ \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix} \right\} \otimes |-\rangle. \quad (13.40)\end{aligned}$$

Если воздействовать оператором  $\hat{H}^{\otimes n} \hat{U}_{x \neq 0} \hat{H}^{\otimes n}$ , то используя результат

(13.40) получим:

$$\begin{aligned}
 & \hat{H}^{\otimes n} \hat{U}_{x \neq 0} \hat{H}^{\otimes n} \sum_x \alpha_x |x\rangle = \\
 & = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \\
 & = \begin{pmatrix} \frac{2}{N} \sum_x \alpha_x - \alpha_0 \\ \frac{2}{N} \sum_x \alpha_x - \alpha_1 \\ \frac{2}{N} \sum_x \alpha_x - \alpha_2 \\ \vdots \\ \frac{2}{N} \sum_x \alpha_x - \alpha_{N-1} \end{pmatrix} = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle.
 \end{aligned}$$

Т. о. схема предложенная на рис. 13.31 действительно осуществляет обращение относительно среднего.

## 13.8 Адиабатические квантовые компьютеры

Адиабатические компьютеры основаны на так называемой адиабатической теореме Теорема 14.7.1.

TBD

## 13.9 Теория сложности алгоритмов и квантовые вычисления

### 13.9.1 Классы сложности алгоритмов $P$ , $NP$ , $BQP$

TBD



# Часть 5

## Приложения



## Глава 14

# Основные положения квантовой механики

Необходимость этого раздела вызвана в первую очередь особенностями преподавания квантовой механики в технических вузах. Основной упор делается на практическое применение и при этом часто упускаются теоретические и философские основы квантовой механики.

Например подробно описываются практические приемы для обработки результатов множества однотипных измерений, т. е. описываются правила по которым производится расчет средних значений физических величин в заданном квантовом состоянии. При этом упускаются ответы на вопросы возникающие при анализе единичных экспериментов, такие как соотношение показаний прибора с изменением волновой функции при измерении, что такое декогеренция и многие другие. Актуальность этих вопросов повысилась в последнее время благодаря необходимости анализировать результаты единичных опытов, что привело к возможности проектировать новые приборы, которые опираются на эти свойства чистых квантовых состояний. В частности нобелевская премия по физике 2012 г. была присуждена Сержу Арошу (Serge Haroche) и Дэвиду Вайнленду (David J. Wineland) за “for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems.” <sup>1</sup>

---

<sup>1</sup> “прорывные экспериментальные методы, которые сделали возможными измерение отдельных квантовых систем и управление ими.”

## 14.1 Дираковская формулировка квантовой механики

В курсе лекций по квантовой оптике мы будем всюду использовать формализм Дирака [56]. В обычной формулировке квантовой механики мы имеем дело с волновыми функциями, например  $\psi(q, t)$  - волновая функция в координатном представлении. Одно и то же состояние системы можно описать волновыми функциями в различных представлениях, связанных друг с другом линейными преобразованиями. Например, волновая функция в импульсном представлении связана с волновой функцией в координатном представлении равенством

$$\phi(p, t) = \frac{1}{2\pi\hbar} \int_{-\infty}^{+\infty} \psi(q, t) e^{-i\frac{pq}{\hbar}} dq \quad (14.1)$$

Главное здесь, что одно и то же состояние можно описывать волновыми функциями, выраженными через различные переменные. Отсюда следует, что можно ввести более общее образование, характеризующее состояние системы независимо от представления. Для такого образования Дирак ввел понятие волнового вектора, или вектора состояния, обозначаемого:

$$|\dots\rangle \quad (14.2)$$

и называемого кет-вектором.

### 14.1.1 Кет-вектор

$|\dots\rangle$  общее обозначение кет-вектора;  $|a\rangle$ ,  $|x\rangle$ ,  $|\psi\rangle$  и т.д. означают кет-векторы, описывающие некоторые частные состояния, символы которых записываются внутри скобок.

### 14.1.2 Бра-векторы

Каждому кет-вектору соответствует сопряженный ему бра-вектор. Бра-вектор обозначается:

$$\langle \dots |, \quad \langle a |, \quad \langle \psi |. \quad (14.3)$$

Названия бра- и кет-векторы образованы от первой и второй половины английского слова *bra-ket* (скобка).

Таким образом, бра-векторам  $\langle a|$ ,  $\langle x|$ ,  $\langle \psi|$  соответствуют сопряженные им кет-векторы  $|a\rangle$ ,  $|x\rangle$ ,  $|\psi\rangle$  и наоборот. Для векторов состояний справедливы те

же основные соотношения, которые справедливы для волновых функций:

$$|u\rangle = |a\rangle + |b\rangle, \quad \langle u| = \langle a| + \langle b|, \quad |v\rangle = l|a\rangle, \quad \langle v| = l\langle a|. \quad (14.4)$$

Бра- и кет-векторы связаны между собой операцией эрмитового сопряжения:

$$|u\rangle = (\langle u|)^\dagger, \quad \langle u| = (|u\rangle)^\dagger. \quad (14.5)$$

В известных случаях это сводится к следующим соотношениям:

$$(\psi(q))^\dagger = \psi^*(q)$$

для волновой функции в координатном представлении;

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}^\dagger = (a_1^*, a_2^*, \dots, a_n^*)$$

в матричном представлении.

При помощи бра- и кет-векторов можно определить скалярное произведение

$$\langle v|u\rangle = \langle u|v\rangle^*. \quad (14.6)$$

В конкретных случаях это означает:

$$\langle \psi| \phi\rangle = \int \psi^* \phi dq$$

в координатном представлении;

$$\langle a|b\rangle = (a_1^*, a_2^*, \dots, a_n^*) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1^* b_1 + a_2^* b_2 + \dots + a_n^* b_n$$

в матричном представлении.

Из соотношения (14.6) следует, что норма вектора вещественна. Дополнительно полагаем, что норма вектора положительна или равна нулю:  $\langle a|a\rangle \geq 0$ .

### 14.1.3 Операторы

В квантовой механике используют линейные операторы. Операторы связывают один вектор состояния с другим:

$$|q\rangle = \hat{L} |p\rangle \quad (14.7)$$

Сопряженное равенство имеет вид

$$\langle q| = \langle p| \hat{L}^\dagger \quad (14.8)$$

где  $\hat{L}^\dagger$  - оператор, сопряженный оператору  $\hat{L}$ .

Приведем некоторые соотношения, справедливые для линейных операторов:

$$\begin{aligned} \hat{L}^{++} &= \hat{L}, \quad \left( l \hat{L} |a\rangle \right)^\dagger = l^* \langle a| \hat{L}^\dagger, \\ \left( \left( \hat{L}_1 + \hat{L}_2 \right) |a\rangle \right)^\dagger &= \langle a| \left( \hat{L}_1^\dagger + \hat{L}_2^\dagger \right), \\ \left( \left( \hat{L}_1 \hat{L}_2 \right) |a\rangle \right)^\dagger &= \langle a| \left( \hat{L}_2^\dagger \hat{L}_1^\dagger \right), \\ \left( \left( \hat{L}_1 \hat{L}_2 \hat{L}_3 \right) |a\rangle \right)^\dagger &= \langle a| \left( \hat{L}_3^\dagger \hat{L}_2^\dagger \hat{L}_1^\dagger \right), \text{ и т.д.} \end{aligned} \quad (14.9)$$

Заметим, что алгебра операторов совпадает с алгеброй квадратных матриц. Матричные элементы операторов обозначаются следующим образом:

$$\langle a| \hat{L} |b\rangle = L_{ab} \quad (14.10)$$

Для матричных элементов справедливы равенства

$$\langle a| \hat{L} |b\rangle^* = \langle b| \hat{L}^\dagger |a\rangle, \quad \langle a| \hat{L}_1 \hat{L}_2 |b\rangle^* = \langle b| \hat{L}_2^\dagger \hat{L}_1^\dagger |a\rangle \quad (14.11)$$

#### 14.1.4 Собственные значения и собственные векторы операторов

Собственные значения и собственные векторы операторов определяются равенством

$$\hat{L} |l_n\rangle = l_n |l_n\rangle, \quad (14.12)$$

где  $l_n$  собственное значение;  $|l_n\rangle$  собственный вектор.

Для бра-векторов имеем аналогичные равенства:

$$\langle d_n| \hat{D} = d_n \langle d_n|. \quad (14.13)$$

Если операторы соответствуют наблюдаемым величинам, они должны быть самосопряженными:

$$\hat{L} = \hat{L}^\dagger. \quad (14.14)$$

Собственные значения самосопряженного (эрмитова) оператора вещественны. Действительно из

$$\hat{L} |l\rangle = l |l\rangle$$

следует что

$$\langle l | \hat{L} | l \rangle = l \langle l | l \rangle .$$

С другой стороны, вспоминая про (14.9):  $\langle l | \hat{L}^\dagger = l^* \langle l |$ , из (14.14) имеем

$$\langle l | \hat{L} | l \rangle = l^* \langle l | l \rangle .$$

Таким образом  $l \langle l | l \rangle = l^* \langle l | l \rangle$ , т. е.  $l = l^*$

Собственные векторы самосопряженного оператора ортогональны. Действительно рассмотрим два собственных вектора  $|l_1\rangle$  и  $|l_2\rangle$ :

$$\hat{L} |l_1\rangle = l_1 |l_1\rangle , \quad \hat{L} |l_2\rangle = l_2 |l_2\rangle$$

Из второго соотношения получаем

$$\langle l_1 | \hat{L} | l_2 \rangle = l_2 \langle l_1 | l_2 \rangle$$

С учетом вещественности собственных чисел и соотношения (14.14) для вектора  $|l_1\rangle$  получим:

$$\langle l_1 | \hat{L} = l_1 \langle l_1 | .$$

Откуда

$$\langle l_1 | \hat{L} | l_2 \rangle = l_1 \langle l_1 | l_2 \rangle .$$

Таким образом

$$(l_1 - l_2) \langle l_1 | l_2 \rangle = 0, \quad \text{т. е. } \langle l_1 | l_2 \rangle = 0, \quad \text{т. к. } l_1 \neq l_2.$$

### 14.1.5 Наблюдаемые величины. Разложение по собственным векторам. Полнота системы собственных векторов

Операторы, соответствующие наблюдаемым физическим величинам, являются самосопряженными операторами. Это обеспечивает действительность значений наблюдаемой физической величины. Имеем набор собственных состояний некоторого эрмитового оператора  $|l_n\rangle$ ,  $\hat{L} |l_n\rangle = l_n |l_n\rangle$ . Если набор собственных состояний полный, согласно принципам квантовой механики любое состояние можно представить суперпозицией состояний  $|l_n\rangle$ :

$$|\psi\rangle = \sum_{(n)} c_n |l_n\rangle . \quad (14.15)$$

Отсюда для коэффициентов разложения имеем:  $c_n = \langle l_n | \psi \rangle$ , и, следовательно, справедливо равенство

$$|\psi\rangle = \sum_{(n)} \langle l_n | \psi \rangle |l_n\rangle = \sum_{(n)} |l_n\rangle \langle l_n | \psi \rangle. \quad (14.16)$$

Из равенства 14.16 следует важное соотношение:

$$\sum_{(n)} |l_n\rangle \langle l_n| = \hat{I}. \quad (14.17)$$

где  $\hat{I}$  - единичный оператор. Это равенство является условием полноты системы собственных векторов (условием разложимости).

### 14.1.6 Оператор проектирования

Рассмотрим оператор  $\hat{P}_n = |l_n\rangle \langle l_n|$ . Результатом действия этого оператора на состояние  $|\psi\rangle$  будет

$$\hat{P}_n |\psi\rangle = \sum_{(k)} |l_n\rangle \langle l_n | c_k |l_k\rangle = c_n |l_n\rangle. \quad (14.18)$$

Оператор  $\hat{P}_n = |l_n\rangle \langle l_n|$  называется оператором проектирования.

Можно написать следующие свойства этого оператора

$$\sum_{(n)} \hat{P}_n = \hat{I}. \quad (14.19)$$

$$\hat{P}_n^2 = \hat{P}_n. \quad (14.20)$$

Действие оператора проектирования имеет простую геометрическую интерпретацию (см. рис. 14.1):

$$\hat{P}_n |\psi\rangle = \cos \theta |l_n\rangle,$$

где  $\cos \theta = \langle \psi | l_n \rangle = c_n$ .

### 14.1.7 След оператора

В ортонормированном базисе  $\{|l_n\rangle\}$  величина

$$Sp \hat{L} = \sum_n \langle l_n | \hat{L} | l_n \rangle \quad (14.21)$$



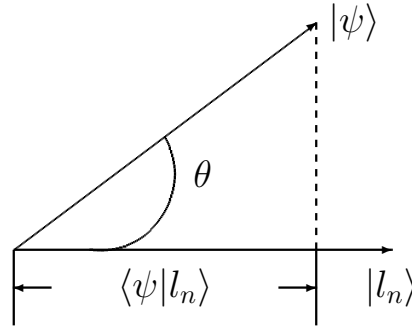


Рис. 14.1: Оператор проектирования. Действие оператора может быть интерпретировано как проекция вектора  $|\psi\rangle$  на ось  $|l_n\rangle$

называется следом оператора  $\hat{L}$ . При определенных условиях [36] ряд 14.21 абсолютно сходится и не зависит от выбора базиса.

Если использовать матричное представление

$$L_{kn} = \langle l_k | \hat{L} | l_n \rangle ,$$

то след оператора - сумма диагональных элементов матричного представления

$$Sp \hat{L} = \sum_n L_{nn}$$

Можно написать следующие свойства следа оператора:

$$\begin{aligned} Sp \left( l \hat{L} + m \hat{M} \right) &= l Sp \hat{L} + m Sp \hat{M}, \\ Sp \left( \hat{L} \hat{M} \right) &= Sp \left( \hat{M} \hat{L} \right). \end{aligned} \quad (14.22)$$

### 14.1.8 Средние значения операторов

Среднее значение оператора  $\hat{L}$  в состоянии  $|\psi\rangle$  дается равенством

$$\langle \hat{L} \rangle_\psi = \langle \psi | \hat{L} | \psi \rangle \quad (14.23)$$

при условии

$$\langle \psi | \psi \rangle = 1.$$

Действительно, если принять, что  $|\psi\rangle$  раскладывается в ряд по собственным функциям оператора  $\hat{L}$  следующим образом:

$$|\psi\rangle = \sum_n c_n |l_n\rangle ,$$

то  $\hat{L}|\psi\rangle$  можно записать как

$$\hat{L}|\psi\rangle = \sum_n l_n c_n |l_n\rangle,$$

где  $l_n$  собственное число соответствующее собственному состоянию  $|l_n\rangle$ . Если теперь подставить два последних выражения в (14.23) то получим:

$$\langle\psi|\hat{L}|\psi\rangle = \sum_{n,m} l_n c_n c_m^* \langle l_m|l_n\rangle = \sum_n l_n c_n c_n^* = \sum_n l_n |c_n|^2,$$

что (при условии  $\langle\psi|\psi\rangle = 1$ ) доказывает, что выражение (14.23) действительно представляет собой выражение для среднего значения оператора  $\hat{L}$  в состоянии  $|\psi\rangle$ .<sup>2</sup>

Если взять некоторый ортонормированный базис  $\{|n\rangle\}$ , образующий полный набор, т. е. подчиняющийся условию (14.17):  $\sum_n |n\rangle\langle n| = \hat{I}$ , то выражение (14.23) может быть переписано следующим образом:

$$\begin{aligned} \langle\hat{L}\rangle_\psi &= \langle\psi|\hat{L}|\psi\rangle = \langle\psi|\hat{I}\hat{L}|\psi\rangle = \\ &= \sum_n \langle\psi|n\rangle\langle n|\hat{L}|\psi\rangle = \sum_n \langle n|\hat{L}|\psi\rangle\langle\psi|n\rangle = Sp(\hat{L}\hat{\rho}), \end{aligned}$$

где  $\hat{\rho} = |\psi\rangle\langle\psi| = \hat{P}_\psi$  - оператор проектирования на состояние  $|\psi\rangle$ . С учетом (14.22) можно записать

$$\langle\hat{L}\rangle_\psi = Sp(\hat{\rho}\hat{L}). \quad (14.24)$$

### 14.1.9 Представление операторов через внешние произведения собственных векторов

Дважды используя условие полноты (14.16), получим

$$\hat{A} = \hat{I}\hat{A}\hat{I} = \sum_{(l)} \sum_{(l')} |l\rangle\langle l| \hat{A} |l'\rangle\langle l'| = \sum_{(l)} \sum_{(l')} |l\rangle\langle l'| A_{ll'}, \quad (14.25)$$

где  $A_{ll'} = \langle l|\hat{A}|l'\rangle$  - матричный элемент оператора  $\hat{A}$  в представлении  $|l\rangle$ .

Оператор, выраженный через свои же собственные векторы, может быть представляем разложением<sup>3</sup>

$$\hat{L} = \sum_{(l)} l |l\rangle\langle l|. \quad (14.26)$$

<sup>2</sup>Для этого достаточно вспомнить, что  $|c_n|^2$  задает вероятность получить систему в состоянии  $|l_n\rangle$ , то есть получить показание измерительного прибора в  $l_n$

<sup>3</sup>При условии нормировки собственных векторов:  $\langle l|l\rangle = 1$

Обобщение этого равенства для операторной функции имеет вид

$$F(\hat{L}) = \sum_{(l)} F(l) |l\rangle \langle l|. \quad (14.27)$$

### 14.1.10 Волновые функции в координатном и импульсном представлениях

Переход от вектора состояния к волновой функции осуществляется посредством скалярного умножения этого вектора состояния на вектор состояния соответствующей наблюдаемой величины. Например, для волновой функции в координатном представлении

$$\phi(q) = \langle q | \psi \rangle. \quad (14.28)$$

где  $\langle q |$  - собственный вектор оператора координаты. В импульсном представлении получим

$$\phi(p) = \langle p | \psi \rangle. \quad (14.29)$$

где  $\langle p |$  - собственный вектор оператора импульса.

## 14.2 Динамика изменения волновой функции

Волновая функция  $|\phi\rangle$  может изменяться посредством двух механизмов:

- Редукция волновой функции во время измерения
- Уравнение Шрёдингера в промежутках между двумя последовательными измерениями

### 14.2.1 Уравнение Шрёдингера

Изменение состояния чистой квантовой системы между двумя последовательными измерениями описывается следующим уравнением (Шрёдингера)

$$i\hbar \frac{\partial |\phi\rangle}{\partial t} = \hat{\mathcal{H}} |\phi\rangle. \quad (14.30)$$

Уравнение (14.30) является обратимым и, соответственно, не применимо к описанию изменения волновой функции в момент измерения.

Стоит отметить связь уравнения Шрёдингера с теоремой Стоуна ([Теорема 17.2.1](#)) TBD.

## Уравнение Шрёдингера в представлении взаимодействия

Допустим что в гамильтониане можно выделить две части:

$$\hat{\mathcal{H}} = \hat{\mathcal{H}}_0 + \hat{\mathcal{V}}.$$

Введем следующее преобразование волновой функции:

$$|\phi\rangle_I = \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} |\phi\rangle$$

и посмотрим чему будет равно следующее выражение:

$$\begin{aligned} i\hbar \frac{\partial |\phi\rangle_I}{\partial t} &= i\hbar \frac{i\hat{\mathcal{H}}_0}{\hbar} \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} |\phi\rangle + \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} i\hbar \frac{\partial |\phi\rangle}{\partial t} = \\ &= -\hat{\mathcal{H}}_0 \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} |\phi\rangle + \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} (\hat{\mathcal{H}}_0 + \hat{\mathcal{V}}) |\phi\rangle = \\ &= -\hat{\mathcal{H}}_0 \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} |\phi\rangle + \hat{\mathcal{H}}_0 \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} |\phi\rangle + \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} \hat{\mathcal{V}} |\phi\rangle = \\ &= \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} \hat{\mathcal{V}} |\phi\rangle = \\ &= \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} \hat{\mathcal{V}} \exp\left\{\left(-\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} |\phi\rangle = \\ &= \hat{\mathcal{V}}_I |\phi\rangle_I, \end{aligned}$$

где

$$\hat{\mathcal{V}}_I = \exp\left\{\left(\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} \hat{\mathcal{V}} \exp\left\{\left(-\frac{i\hat{\mathcal{H}}_0 t}{\hbar}\right)\right\} \quad (14.31)$$

гамильтониан взаимодействия в представлении взаимодействия.

Таким образом получаем уравнение Шрёдингера в представлении взаимодействия:

$$i\hbar \frac{\partial |\phi\rangle_I}{\partial t} = \hat{\mathcal{V}}_I |\phi\rangle_I. \quad (14.32)$$

## Уравнение движения матрицы плотности

Из соотношения (14.30) имеем

$$\begin{aligned} i\hbar \frac{\partial |\phi\rangle}{\partial t} &= \hat{\mathcal{H}} |\phi\rangle, \\ -i\hbar \frac{\partial \langle\phi|}{\partial t} &= \hat{\mathcal{H}} \langle\phi|, \end{aligned}$$

таким образом для матрицы плотности  $\hat{\rho} = |\phi\rangle \langle\phi|$  получаем

$$\begin{aligned} i\hbar \frac{\partial \hat{\rho}}{\partial t} &= i\hbar \frac{\partial |\phi\rangle \langle\phi|}{\partial t} = i\hbar \left( \frac{\partial |\phi\rangle}{\partial t} \langle\phi| + |\phi\rangle \frac{\partial \langle\phi|}{\partial t} \right) = \\ &= \hat{\mathcal{H}} |\phi\rangle \langle\phi| - |\phi\rangle \langle\phi| \hat{\mathcal{H}} = [\hat{\mathcal{H}}, \hat{\rho}] \end{aligned} \quad (14.33)$$

Уравнение (14.33) часто называется квантовым уравнением Лиувилля и уравнением фон Неймана.

## Оператор эволюции. Представление Гейзенберга и представление Шредингера

Изменение волновой функции по закону (14.30) может быть также описано с помощью некоторого оператора (эволюции)  $\hat{U}(t, t_0)$ :

$$|\phi(t)\rangle = \hat{U}(t, t_0) |\phi(t_0)\rangle. \quad (14.34)$$

Уравнение (14.30) может быть переписано в виде

$$|\phi(t)\rangle = \exp\left(-\frac{i}{\hbar} \hat{\mathcal{H}}(t - t_0)\right) |\phi(t_0)\rangle,$$

откуда для оператора эволюции имеем

$$\hat{U}(t, t_0) = \exp\left(-\frac{i}{\hbar} \hat{\mathcal{H}}(t - t_0)\right) \quad (14.35)$$

Оператор эволюции - унитарный. Действительно:

$$\begin{aligned} &\hat{U}(t, t_0) \hat{U}^\dagger(t, t_0) = \\ &= \exp\left(-\frac{i}{\hbar} \hat{\mathcal{H}}(t - t_0)\right) \exp\left(+\frac{i}{\hbar} \hat{\mathcal{H}}(t - t_0)\right) = \hat{I} \end{aligned}$$

Наряду с представлением Шредингера где операторы от времени не зависят а меняются волновые функции существует представление Гейзенберга где операторы меняются во времени.

Очевидно средние значения операторов не должны зависеть от представления:

$$\begin{aligned}\langle \phi_H(t_0) | \hat{A}_H(t) | \phi_H(t_0) \rangle &= \langle \phi_S(t) | \hat{A}_S | \phi_S(t) \rangle = \\ &= \langle \phi_H(t_0) | \hat{U}^\dagger(t, t_0) \hat{A}_S \hat{U}(t, t_0) | \phi_H(t_0) \rangle,\end{aligned}$$

откуда с учетом  $\hat{A}_H(t_0) = \hat{A}_S(t_0)$  получаем закон эволюции операторов в представлении Гейзенберга:

$$\hat{A}_H(t) = \hat{U}^\dagger(t, t_0) \hat{A}_H(t_0) \hat{U}(t, t_0) \quad (14.36)$$

При этом уравнение для оператора  $\hat{A}_H$  будет выглядеть следующим образом:

$$\begin{aligned}\frac{\partial \hat{A}_H}{\partial t} &= \frac{i}{\hbar} \hat{\mathcal{H}} \hat{U}^\dagger(t, t_0) \hat{A}_H(t_0) \hat{U}(t, t_0) - \\ &- \frac{i}{\hbar} \hat{U}^\dagger(t, t_0) \hat{A}_H(t_0) \hat{U}(t, t_0) \hat{\mathcal{H}} = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{A}_H]\end{aligned} \quad (14.37)$$

## 14.2.2 Различия между чистыми и смешанными состояниями. Декогеренция

**Определение 14.2.1** (Чистое состояние). Если состояние системы описывается матрицей плотности  $\hat{\rho}$  которая представима в виде

$$\hat{\rho} = |\psi\rangle \langle \psi| \quad (14.38)$$

то данное состояние называется чистым.

**Определение 14.2.2** (Смешанное состояние). Если состояние системы описывается матрицей плотности  $\hat{\rho}$  которая **не** представима в виде (14.38), т.е.

$$\hat{\rho} \neq |\psi\rangle \langle \psi|$$

то данное состояние называется смешанным.

Особый интерес представляет собой различие между чистыми и смешанными состояниями, в частности - каким образом происходит переход от чистых состояний к смешанным.

Рассмотрим двухуровневое состояние (см. [рис. 14.2](#)). В чистом состоянии оно описывается следующей волновой функцией:

$$|\phi\rangle = c_a |a\rangle + c_b |b\rangle,$$



Рис. 14.2: Модель двухуровневого атома, используемого для описания декогеренции.

соответствующая матрица плотности имеет вид

$$\begin{aligned}\hat{\rho} &= |\phi\rangle \langle \phi| = \\ &= |c_a|^2 |a\rangle \langle a| + |c_b|^2 |b\rangle \langle b| + \\ &\quad + c_a c_b^* |a\rangle \langle b| + c_b c_a^* |b\rangle \langle a|,\end{aligned}\tag{14.39}$$

или в матричном виде

$$\hat{\rho} = \begin{pmatrix} |c_a|^2 & c_a c_b^* \\ c_b c_a^* & |c_b|^2 \end{pmatrix}.$$

Матрица плотности для смешанного состояния имеет только диагональные элементы:

$$\begin{aligned}\hat{\rho} &= \begin{pmatrix} |c_a|^2 & 0 \\ 0 & |c_b|^2 \end{pmatrix} = \\ &= |c_a|^2 |a\rangle \langle a| + |c_b|^2 |b\rangle \langle b|.\end{aligned}\tag{14.40}$$

Переход от (14.39) к (14.40) называется декогеренцией. В описании процесса декогеренции мы будем следовать [54].

Отличие смешанных состояний от чистых проявляется во влиянии окружения  $\mathcal{E}$ . В случае чистых состояний рассматриваемая система и ее окружение независимы, т. е.

$$|\phi\rangle_{pure} = |\phi\rangle_{at} \otimes |\mathcal{E}\rangle.\tag{14.41}$$

В случае смешанных состояний атом и его окружение образуют так называемое перепутанное состояние в котором состояниям  $|a\rangle$  и  $|b\rangle$  соответствуют различные состояния окружения  $|\mathcal{E}_a\rangle$  и  $|\mathcal{E}_b\rangle$ .

$$|\phi\rangle_{mix} = c_a |a\rangle |\mathcal{E}_a\rangle + c_b |b\rangle |\mathcal{E}_b\rangle.\tag{14.42}$$

Матрица плотности соответствующая (14.42) имеет вид

$$\begin{aligned}\hat{\rho}_{mix} &= |\phi\rangle_{mix} \langle \phi|_{mix} = \\ &= |c_a|^2 |a\rangle \langle a| \otimes |\mathcal{E}_a\rangle \langle \mathcal{E}_a| + |c_b|^2 |b\rangle \langle b| \otimes |\mathcal{E}_b\rangle \langle \mathcal{E}_b| + \\ &\quad + c_a c_b^* |a\rangle \langle b| \otimes |\mathcal{E}_a\rangle \langle \mathcal{E}_b| + c_b c_a^* |b\rangle \langle a| \otimes |\mathcal{E}_b\rangle \langle \mathcal{E}_a|.\end{aligned}\tag{14.43}$$

Если теперь применить к выражению (14.43) усреднение по переменным окружения, то получим

$$\begin{aligned}\langle \hat{\rho}_{mix} \rangle_{\mathcal{E}} &= Sp_{\mathcal{E}} (\hat{\rho}) = \\ &= \langle \mathcal{E}_a | \hat{\rho}_{mix} | \mathcal{E}_a \rangle + \langle \mathcal{E}_b | \hat{\rho}_{mix} | \mathcal{E}_b \rangle = \\ &= |c_a|^2 |a\rangle \langle a| + |c_b|^2 |b\rangle \langle b|. \end{aligned} \quad (14.44)$$

Выражение (14.44) получено в предположении ортонормированного базиса  $\{|\mathcal{E}_a\rangle, |\mathcal{E}_b\rangle\}$ :

$$\begin{aligned}\langle \mathcal{E}_a | \mathcal{E}_a \rangle &= \langle \mathcal{E}_b | \mathcal{E}_b \rangle = 1, \\ \langle \mathcal{E}_a | \mathcal{E}_b \rangle &= \langle \mathcal{E}_b | \mathcal{E}_a \rangle = 0. \end{aligned} \quad (14.45)$$

Условия (14.45) являются ключевыми для понимания того почему рассматриваемый базис атомной системы является выделенным и почему например в случае смешанных состояний не рассматривают другие базисы такие как базис полученный преобразованием Адамара по отношению к исходному :

$$\begin{aligned}|\mathcal{A}\rangle &= \frac{|a\rangle + |b\rangle}{\sqrt{2}}, \\ |\mathcal{B}\rangle &= \frac{|a\rangle - |b\rangle}{\sqrt{2}}. \end{aligned} \quad (14.46)$$

Состояния окружения соответствующие базису (14.46) не являются ортогональными откуда следует невозможность использования (14.46) в качестве базисных векторов для смешанных состояний.

Процесс декогеренции, т. е. перехода от (14.41) к (14.42) может быть описан с помощью уравнения Шредингера, и следовательно теоретически является обратимым. Единственное требование - ортогональность различных состояний окружения:  $\langle \mathcal{E}_a | \mathcal{E}_b \rangle = 0$ . Это требование всегда выполняется для макроскопических систем, где состояние зависит от очень большого числа переменных. При этом в случае макроскопических систем стоит отметить, что существует большое число возможных вариантов конечных состояний  $|\mathcal{E}_{a,b}\rangle$  в силу чего обратный процесс становится практически не реализуемым, так как необходимо контролировать большое число возможных переменных которыми описывается состояние окружения. В этом смысле процесс декогеренции имеет такую же природу как и второй закон термодинамики (возрастания энтропии), который описывает необратимые процессы.<sup>4</sup>

---

<sup>4</sup>Здесь надо быть немного аккуратным поскольку второй закон термодинамики применим к закрытым системам, а сами процессы декогеренции происходят в открытых системах





Рис. 14.3: Процесс измерения. Показание прибора соответствует одному из собственных чисел оператора  $\hat{L}$ :  $\{l_k\}$

Процесс декогеренции является очень быстрым, в частности [29] дает следующую оценку: для систем массой 1 г. при разделении  $\Delta x = 1$  см. и температуре  $T = 300$  К, времени релаксации равной времени жизни Вселенной  $\tau_R = 10^{17}$  с. процесс декогеренции занимает  $10^{-23}$  с.

### 14.2.3 Редукция волновой функции. Измерение в квантовой механике

Процесс выбора (результата измерения) один из самых сложных в квантовой механике. В отличие от детерминистского изменения волновой функции, описываемого уравнением Шрёдингера (14.30), процесс измерения носит случайный характер и для его описания следует применять другие уравнения.

Рассмотрим вначале чистые состояния и предположим, что производится измерение физической наблюдаемой, описываемой оператором  $\hat{L}$ . Собственные числа и собственные функции этого оператора  $\{l_k\}$  и  $\{|l_k\rangle\}$  соответственно. В момент измерения показания прибора могут принимать значения соответствующие собственным числам измеряемого оператора (см. рис. 14.3). Допустим, что показание прибора -  $l_n$  в этом случае волновая функция должна быть  $|l_n\rangle$ , т. о. произошло следующее изменение волновой функции:

$$|\phi\rangle \rightarrow |l_n\rangle,$$

которое может быть описано действием оператора проецирования  $\hat{P}_n = |l_n\rangle \langle l_n|$

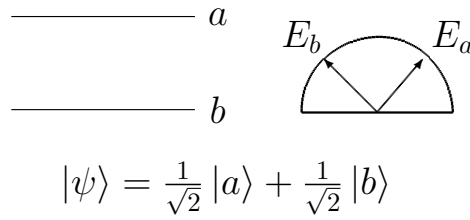


Рис. 14.4: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии  $|\psi\rangle = \frac{1}{\sqrt{2}} |a\rangle + \frac{1}{\sqrt{2}} |b\rangle$ . Прибором регистрируется значение энергии  $E_a$  или  $E_b$ .

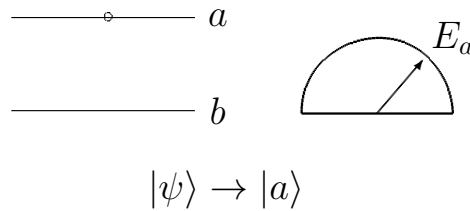


Рис. 14.5: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии  $|\psi\rangle = \frac{1}{\sqrt{2}} |a\rangle + \frac{1}{\sqrt{2}} |b\rangle$ . Прибором регистрируется значение энергии  $E_a$ . При измерении происходит следующая редукция  $|\psi\rangle \rightarrow |a\rangle$

(14.18):

$$\hat{P}_n |\phi\rangle = c_n |l_n\rangle.$$

**Пример 14.2.1** (Измерение энергии двухуровневого атома). Рассмотрим двухуровневый атом находящийся в чистом состоянии (см. рис. 14.4)  $|\psi\rangle = \frac{1}{\sqrt{2}} |a\rangle + \frac{1}{\sqrt{2}} |b\rangle$ .

Наш прибор измеряет энергию этого атома и оператор Гамильтона имеет 2 собственные функции  $|a, b\rangle$ , которым соответствуют собственные числа  $E_a, E_b$ . Таким образом возможные показания прибора принадлежат множеству  $\{E_a, E_b\}$ .

В том случае когда стрелка прибора показывает  $E_a$  происходит следующая редукция (см. рис. 14.5)

$$|\psi\rangle \rightarrow |a\rangle.$$

Аналогично в случае  $E_b$  происходит следующая редукция (см. рис. 14.6)

$$|\psi\rangle \rightarrow |b\rangle.$$

Не существует способа предсказать результат который будет получен в результате единичного измерения. Вместе с тем можно сказать с какой вероятностью будет получен тот или иной результат.



Рис. 14.6: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии  $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$ . Прибором регистрируется значение энергии  $E_b$ . При измерении происходит следующая редукция  $|\psi\rangle \rightarrow |b\rangle$

Действительно в случае смешанного состояния

$$\hat{\rho} = \sum_n |c_n|^2 |l_n\rangle \langle l_n|$$

коэффициенты  $P_n = |c_n|^2$  задают вероятности обнаружить систему в состоянии  $|l_n\rangle$ .

Для чистого состояния

$$|\phi\rangle = \sum_n c_n |l_n\rangle$$

мы также имеем, что вероятность обнаружить систему в состоянии  $|l_n\rangle$  задается числом  $P_n = |c_n|^2$ .

Основное отличие чистых и смешанных состояний с точки зрения измерения заключается в том, что в первом случае (чистое состояние) в процессе измерения меняется волновая функция, т. е. само состояние. При этом если в процессе измерения было получено некоторое конечное состояние  $|l_i\rangle$ , то нельзя сказать, что оно было таким же и до измерения. Смешанные состояния ведут себя подобно классическим объектам, т. е. если в процессе измерения было получено состояние  $|l_i\rangle$ , то можно утверждать, что оно было таким же и до измерения, а само измерение представляет собой выбор одного состояния из многих возможных.

**Пример 14.2.2.** Выбор из урны с шарами двух цветов *Допустим у нас имеется урна с 4 шарами. С вероятностью  $\frac{1}{2}$  будет извлечен либо белый либо черный шар. Допустим что в результате эксперимента был получен черный шар. Если рассматриваемая система является квантовой и находится в смешанном состоянии (см. рис. 14.7), то состояние извлеченного шара (цвет) не изменилось в результате эксперимента.*

*Если рассматриваемая система является чистой (см. рис. 14.8), то состояние каждого шара описывается суперпозицией двух цветов - черного и*



Рис. 14.7: Пример смешанного состояния. Цвет шара не меняется в результате “измерения”



Рис. 14.8: Пример чистого состояния. Цвет шара меняется в результате “измерения”

белого. Таким образом в результате эксперимента эта суперпозиция разрушается и шар приобретает определенный цвет (черный в нашем случае), т. е. можно сказать что цвет шара меняется.

## 14.3 Измеримость физических величин

### 14.3.1 Принцип неопределенности Гейзенберга

Допустим два оператора  $\hat{A}$  и  $\hat{B}$  не коммутируют друг с другом, т.е.

$$[\hat{A}\hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} = i\hat{C} \neq 0,$$

где  $\hat{C}$  некоторый эрмитовый оператор.

Допустим система находится в состоянии  $|\psi\rangle$ . Тогда средние значения операторов выражаются следующими соотношениями:

$$\langle\psi|\hat{A}|\psi\rangle = \langle\hat{A}\rangle,$$

$$\langle\psi|\hat{B}|\psi\rangle = \langle\hat{B}\rangle.$$

Определим неопределённость измерения величин  $A$  и  $B$  как их дисперсии

следующим образом

$$\Delta A = \sqrt{\langle \psi | \hat{\mathcal{A}}^2 | \psi \rangle},$$

$$\Delta B = \sqrt{\langle \psi | \hat{\mathcal{B}}^2 | \psi \rangle},$$

где

$$\hat{\mathcal{A}} = \hat{A} - \langle \hat{A} \rangle,$$

$$\hat{\mathcal{B}} = \hat{B} - \langle \hat{B} \rangle.$$

Введем оператор  $\hat{D}$  следующим образом

$$\hat{D} = \hat{\mathcal{A}} + i\lambda\hat{\mathcal{B}}.$$

Рассмотрим оператор  $\hat{D}^\dagger \hat{D}$ , который является эрмитовым. Его среднее в состоянии  $|\psi\rangle$ :

$$\langle \psi | \hat{D}^\dagger \hat{D} | \psi \rangle = \langle \phi | \phi \rangle \geq 0,$$

где  $|\phi\rangle = \hat{D} |\psi\rangle$ . С другой стороны

$$\begin{aligned} \langle \psi | \hat{D}^\dagger \hat{D} | \psi \rangle &= \langle \psi | \left( \hat{\mathcal{A}} - i\lambda\hat{\mathcal{B}} \right) \left( \hat{\mathcal{A}} + i\lambda\hat{\mathcal{B}} \right) | \psi \rangle = \\ &= \langle \psi | \hat{\mathcal{A}}^2 | \psi \rangle + \lambda^2 \langle \psi | \hat{\mathcal{B}}^2 | \psi \rangle + i\lambda \langle \psi | [\hat{\mathcal{A}}, \hat{\mathcal{B}}] | \psi \rangle = \\ &= (\Delta A)^2 + \lambda^2 (\Delta B)^2 + i\lambda \langle \psi | [\hat{A}, \hat{B}] | \psi \rangle = \\ &= \lambda^2 (\Delta B)^2 - \lambda \langle C \rangle + (\Delta A)^2 \geq 0. \end{aligned}$$

Рассмотрим многочлен

$$f(\lambda) = \lambda^2 (\Delta B)^2 - \lambda \langle C \rangle + (\Delta A)^2.$$

Имеем  $f(\pm\infty) > 0$  т.о.  $f(\lambda) \geq 0$  если этот многочлен имеет не больше одного вещественного корня, т.е.

$$\langle C \rangle^2 - 4(\Delta A)^2 (\Delta B)^2 \leq 0$$

или

$$\Delta A \Delta B \geq \frac{|\langle C \rangle|}{2}, \quad (14.47)$$

что представляет собой неравенство Гейзенберга.

### 14.3.2 Соотношение неопределенности энергия-время

Время в квантовой механике не имеет соответствующего оператора и поэтому для оценки времени следует использовать некоторую отдельную наблюдаемую  $\hat{O}$ . С помощью (14.47) можно получить следующее соотношение

$$\Delta E \Delta O \geq \frac{|\langle C \rangle|}{2},$$

где, с учетом (14.37),

$$\frac{d\hat{O}}{dt} = \frac{i}{\hbar} [\hat{\mathcal{H}}, \hat{O}]$$

и следовательно

$$C = \frac{1}{i} [\hat{\mathcal{H}}, \hat{O}] = -\hbar \frac{d\hat{O}}{dt}.$$

Таким образом

$$\Delta E \Delta O \geq \frac{|\langle C \rangle|}{2} = \frac{\hbar}{2} \left| \left\langle \frac{d\hat{O}}{dt} \right\rangle \right|.$$

Обозначив  $\Delta t = \frac{\Delta O}{\left| \left\langle \frac{d\hat{O}}{dt} \right\rangle \right|}$ <sup>5</sup> окончательно получим

$$\Delta E \Delta t \geq \frac{\hbar}{2}. \quad (14.48)$$

Стоит отметить, что состояния с определенной энергией не противоречат соотношению (14.48) поскольку несмотря на то что  $\delta E = 0$ , мы имеем для любой наблюдаемой  $\left\langle \frac{d\hat{O}}{dt} \right\rangle = 0$  и следовательно,  $\Delta t = \infty$ .

### 14.3.3 Одновременная измеримость физических величин

Вопрос об одновременной измеримости двух физических величин имеет большой смысл, особенно при исследовании квантово-механических парадоксов, таких как парадокс ЭПР (см. [разд. 10.1](#)).

Допустим у нас имеется две наблюдаемых  $\hat{A}$ ,  $\hat{B}$ , каждой из которых соответствует набор собственных функций  $|a_i\rangle$ ,  $|b_i\rangle$  и значений  $\{a_i\}$ ,  $\{b_i\}$ , т. е.

$$\begin{aligned} \hat{A} |a_i\rangle &= a_i |a_i\rangle, \\ \hat{B} |b_i\rangle &= b_i |b_i\rangle. \end{aligned}$$

---

<sup>5</sup> Мы можем считать, что при малых временах наблюдаемая  $\hat{O}$  меняется линейно, т.е.  $\left\langle \frac{d\hat{O}}{dt} \right\rangle = \frac{\Delta O}{\Delta t}$ . Т. о.  $\Delta t$  это время значимого изменения наблюдаемой  $O$ .

Если в какой-то момент времени мы сможем измерить значения этих величин одновременно, то полученные значения можно описать числами  $a$  и  $b$ , при этом очевидно что  $a \in \{a_i\}, b \in \{b_i\}$  и

$$\begin{aligned}\hat{A}|a\rangle &= a|a\rangle, \\ \hat{B}|b\rangle &= b|b\rangle.\end{aligned}$$

С учетом того, что измерение величин проводилось одновременно, в силу редукции волновой функции (см. [разд. 14.2.3](#)) имеем

$$|a\rangle = |b\rangle,$$

т. е. операторы  $\hat{A}$  и  $\hat{B}$  имеют общие собственные функции. При этом обязательно чтобы все собственные вектора этих операторов совпадали, достаточно совпадения единственного вектора.

Стоит отметить, что если операторы коммутируют, то наборы собственных векторов операторов совпадают, что находится в соответствии с неравенством Гейзенберга которое в данном случае запишется в виде

$$\Delta a \Delta b \geq 0.$$

Действительно если

$$\hat{A}|a\rangle = a|a\rangle,$$

то, с учетом  $\hat{A}\hat{B} = \hat{B}\hat{A}$

$$\hat{A}\hat{B}|a\rangle = \hat{B}\hat{A}|a\rangle = a\hat{B}|a\rangle.$$

Обозначив  $|b\rangle = \hat{B}|a\rangle$  имеем

$$\hat{A}|b\rangle = a|b\rangle,$$

т. е.  $|b\rangle = |a\rangle$  и данный вектор является собственным для обеих операторов  $\hat{A}$  и  $\hat{B}$ . Т. о. если операторы коммутируют то они обладают общим базисом (набором собственных векторов). Обратное тоже верно см. [\[34\]](#).

## 14.4 Процедура квантования

Как мы уже выяснили физическим величинам в квантовой механике соответствуют самосопряженные операторы. Если нам известна волновая функция (например с помощью уравнения Шредингера), то зная выражение для оператора интересующей нас физической величины можно производить практические расчеты, например средних значений.

Процедура вывода соотношений которым подчиняются операторы называется квантованием.

Ниже приведена информация о связи классической механики с процедурой квантования, а так же приведен пример квантования оператора углового момента.

### 14.4.1 Обобщенные координаты и импульсы

Для полного описания механической системы необходимо задать ее координаты и импульсы. Не всегда координата представляет собой классическую координату, например позиции в декартовой системе координат  $(x, y, z)$ . Иногда для описания рассматриваемой системы удобно пользоваться особыми координатами, такими как например угол в полярной системе координат. В этом случае встает вопрос что же считать импульсом соответствующим такой координате. Для ответа на этот вопрос следует рассмотреть лагранжиан который определяется как разность кинетической и потенциальной энергий:

$$\mathcal{L} = T - U.$$

Если мы имеем совокупность обобщенных координат  $q_n$ , то лагранжиан  $\mathcal{L}$  может быть представлен как функция этих переменных и их производных по времени:

$$\mathcal{L} = \mathcal{L}(q_1, q_2, \dots, \dot{q}_1, \dot{q}_2, \dots).$$

Мы можем определить обобщенный импульс  $p_i$  соответствующий обобщенной координате  $q_i$  как

$$p_i = \frac{\partial \mathcal{L}}{\partial \dot{q}_i}$$

Для квантовой механики особую роль играют уравнения движения в Гамильтоновой форме:

$$\begin{aligned} \dot{q}_i &= \frac{\partial \mathcal{H}}{\partial p_i}, \\ \dot{p}_i &= -\frac{\partial \mathcal{H}}{\partial q_i}, \end{aligned} \quad (14.49)$$

где  $\mathcal{H}$  - гамильтониан (полная энергия) системы как функция обобщенных координат и импульсов.

**Пример 14.4.1** (Прямолинейное движение материальной точки). Допустим у нас имеется материальная точка которая движется вдоль оси  $x$  под действием силы  $F = -\frac{dU}{dx}$ , где  $U$  - потенциальная энергия. В этом случае

$$\mathcal{L} = T - U = \frac{m\dot{x}^2}{2} - U(x).$$



Обобщенный импульс  $p$ , соответствующий координате  $x$

$$p = \frac{\partial \mathcal{L}}{\partial \dot{x}} = m\dot{x},$$

что совпадает с классическим определением импульса.

Гамильтониан

$$\mathcal{H}(x, p) = T + U(x) = \frac{p^2}{2m} + U(x)$$

Уравнения движения:

$$\begin{aligned}\dot{x} &= \frac{\partial \mathcal{H}}{\partial p} = \frac{p}{m}, \\ \dot{p} &= -\frac{\partial \mathcal{H}}{\partial x} = -\frac{dU}{dx} = F\end{aligned}$$

где первое уравнение совпадает с определением импульса, а второе представляет собой известный закон Ньютона

$$F = m\ddot{x}.$$

## 14.4.2 Квантование углового момента

### Классика

Рассматриваемая система состоит из материальной частицы движущейся по кругу. Обобщенными координатами, описывающими частицу являются угол  $\theta$  и радиус окружности  $r$ , который считается постоянным:  $r = \text{const}|_t$  (см. [рис. 14.9](#)).

Гамильтониан системы имеет следующий вид

$$\begin{aligned}\mathcal{H} = T + U &= \frac{mv^2}{2} + U(r) = \\ &= \frac{mr^2\dot{\theta}^2}{2} + U(r),\end{aligned}$$

где  $T = \frac{mv^2}{2}$  - кинетическая энергия частицы, а  $U$  - потенциальная энергия, которая в силу симметрии задачи, не зависит от угла  $\theta$  и зависит только от расстояния  $r$ .

Лангранжин системы

$$\mathcal{L} = T - U = \frac{mr^2\dot{\theta}^2}{2} - U(r)$$

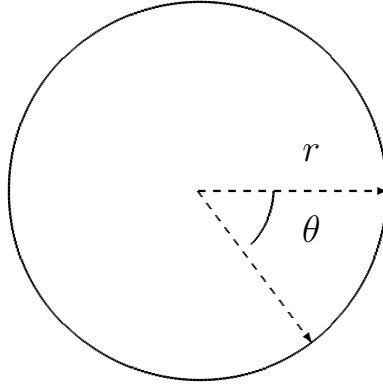


Рис. 14.9: Квантование углового момента. Положение частицы определяется двумя обобщенными координатами:  $r$  и углом  $\theta$ .

Угловой момент (обобщенный импульс соответствующий обобщенной координате  $\theta$ ) определяется как

$$l = \frac{d\mathcal{L}}{d\dot{\theta}} = mr^2\dot{\theta} = I\dot{\theta}, \quad (14.50)$$

где через  $I$  обозначено  $I = mr^2$  - момент инерции (moment of inertia).

Уравнения движения для координаты  $r$ :

$$\frac{\partial \mathcal{L}}{\partial r} = \frac{d}{dt} \frac{\partial \mathcal{L}}{\partial \dot{r}}$$

откуда

$$\begin{aligned} \frac{\partial \mathcal{L}}{\partial r} &= 0, \\ \frac{\partial T}{\partial r} - \frac{\partial U}{\partial r} &= 0, \\ \frac{\partial U}{\partial r} &= mr\dot{\theta}^2, \end{aligned}$$

или же

$$U = \frac{mr^2\dot{\theta}^2}{2} = \frac{l^2}{2I}$$

Таким образом гамильтониан рассматриваемой системы

$$\begin{aligned}\mathcal{H} &= \frac{mr^2\dot{\theta}^2}{2} + \frac{l^2}{2I} = \\ &= \frac{l^2}{2I} + \frac{l^2}{2I} = \frac{l^2}{I}\end{aligned}\quad (14.51)$$

## Квантование

Пусть  $|\psi\rangle$  - собственная функция оператора углового момента  $\hat{L}$  отвечающая собственному числу  $l$ :

$$\hat{L}|\psi\rangle = l|\psi\rangle. \quad (14.52)$$

Эта же волновая функция должна удовлетворять уравнению Шредингера

$$i\hbar\frac{\partial|\psi\rangle}{\partial t} = \hat{\mathcal{H}}|\psi\rangle$$

Из (14.51) имеем

$$\hat{\mathcal{H}} = \frac{\hat{L}^2}{I}$$

откуда с учетом (14.52)

$$i\hbar\frac{\partial|\psi\rangle}{\partial t} = \frac{1}{I}\hat{L}\hat{L}|\psi\rangle = \frac{l^2}{I}|\psi\rangle,$$

или же

$$\frac{\partial|\psi\rangle}{\partial t} = \frac{-il^2}{\hbar I}|\psi\rangle$$

Таким образом

$$|\psi(t)\rangle = C \cdot \exp\left\{\frac{-il^2}{\hbar I}t\right\}$$

Волновая функция должна удовлетворять условию периодичности

$$|\psi(t)\rangle = |\psi(t+T)\rangle$$

где  $T$  - период колебаний. Его можно найти из (14.50):

$$\begin{aligned}\dot{\theta} &= \frac{l}{I}, \\ \theta &= \theta_0 + \frac{l \cdot t}{I}, \\ 2\pi &= \frac{l \cdot T}{I}, \\ T &= \frac{2\pi I}{l}\end{aligned}$$

таким образом

$$2i\pi n = \frac{-il^2}{\hbar I} T = \frac{2\pi I}{l} \frac{-il^2}{\hbar I}$$

откуда

$$l = -\hbar n$$

## 14.5 Составные системы

Системы состоящие из нескольких частей ведут себе принципиально различным образом для случая классических и квантовых систем.

В качестве примера рассмотрим систему из двух частиц. Положение первой из них описывается 3 координатами, которые представляют собой точку в некотором линейном пространстве  $L_1$ :  $(x_1, y_1, z_1) \in L_1$ . Для второй допустим имеем 2 координаты в пространстве  $L_2$  полностью задающие расположение:  $(x_2, y_2) \in L_2$ . Очевидно что для полного описания положения двух частиц нам необходимо 5 координат:  $(x_1, y_1, z_1, x_2, y_2) \in L_1 \times L_2$ . Таким образом составные системы, в классическом случае, описываются точками в пространстве  $L^{classical}$ , которое является декартовым произведением исходных:  $L = L_1 \times L_2$ . Отличительной особенностью декартова произведения является то, что размерности соответствующих пространств складываются:

$$\dim L^{classical} = \dim L_1 + \dim L_2.$$

В квантовом случае составная система описывается векторами (точками) в пространстве которое является тензорным произведением исходных:

$$L^{quantum} = L_1 \otimes L_2.$$

В этом пространстве имеется 6 базисных векторов, и соответственно, для описание положения системы необходимо 6 чисел:  $(x_1 \cdot x_2, y_1 \cdot x_2, z_1 \cdot x_2, x_1 \cdot y_2, y_1 \cdot y_2, z_1 \cdot y_2) \in L^{quantum}$ . Соответствующим образом размерности перемножаются:

$$\dim L^{quantum} = \dim L_1 \cdot \dim L_2.$$

Таким образом если у нас имеется две независимых квантовых системы с волновыми функциями  $|\psi_1\rangle$  и  $|\psi_2\rangle$  то составная система будет иметь следующую волновую функцию

$$|\psi_{12}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

при этом очевидно имеют место следующие равенства

$$\begin{aligned} |\psi_1\rangle &= Sp_2 |\psi_{12}\rangle, \\ |\psi_2\rangle &= Sp_1 |\psi_{12}\rangle \end{aligned} \tag{14.53}$$

т.е. для того чтобы получить состояние подсистемы 1 надо взять след по состояниям системы 2 от общей волновой функции.

У составных систем есть интересное свойство, когда несмотря на то что части этой системы представляют собой смешанные состояния, вся система как целая является чистой. В качестве примера рассмотрим так называемые перепутанные состояния :

$$|\psi\rangle = \frac{|0_1\rangle |1_2\rangle - |1_1\rangle |0_2\rangle}{\sqrt{2}}$$

которое является чистым. При этом для первой частицы имеем

$$\begin{aligned}\rho_1 &= Sp_2 |\psi\rangle \otimes \langle\psi| = \\ &= \langle 0_2|\psi\rangle \langle\psi|0_2\rangle + \langle 1_2|\psi\rangle \langle\psi|1_2\rangle = \\ &= \frac{|1_1\rangle \langle 1_1| + |0_1\rangle \langle 0_1|}{2}\end{aligned}$$

т.е. состояние первой частицы является смешанным.

## 14.6 Координатное представление когерентного состояния

Начнем с вакуумного состояния, которое удовлетворяет уравнению

$$\hat{a} |0\rangle = 0. \quad (14.54)$$

В координатном представлении  $\hat{q} = q$ ,  $\hat{p} = -i\frac{\partial}{\partial q}$ , тогда

$$\begin{aligned}\hat{a} &= \frac{1}{\sqrt{2\hbar\omega}} \left( \omega q + \hbar \frac{\partial}{\partial q} \right), \\ \hat{a}^\dagger &= \frac{1}{\sqrt{2\hbar\omega}} \left( \omega q - \hbar \frac{\partial}{\partial q} \right).\end{aligned} \quad (14.55)$$

Подставляя (14.55) в (14.54) получим уравнение для волновой функции вакуумного состояния моды в когерентном представлении:

$$\left( \omega q + \hbar \frac{\partial}{\partial q} \right) \Phi_0(q) = 0, \quad (14.56)$$

где  $\Phi_0(q) = \langle q|0\rangle$ . Нормированное решение этого уравнения равно

$$\Phi_0(q) = \left( \frac{\omega}{\pi\hbar} \right)^{\frac{1}{4}} e^{-\frac{\omega q^2}{2\hbar}}.$$

Неопределенность этого решения  $\Delta q \Delta p = \frac{\hbar}{2}$  - минимальна. Плотность вероятности обнаружить определенную координату  $q$  (в нашем случае определенную напряженность электрического поля) равна:

$$\Phi_0(q) \Phi_0^*(q) = \left(\frac{\omega}{\pi \hbar}\right)^{\frac{1}{2}} e^{-\frac{\omega q^2}{\hbar}}. \quad (14.57)$$

Для когерентного состояния справедливо уравнение

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle,$$

которое в координатном представлении будет иметь вид

$$\left(\omega q + \hbar \frac{\partial}{\partial q}\right) \Phi_\alpha(q) = \alpha \Phi_\alpha(q), \quad (14.58)$$

где

$$\Phi_\alpha(q) = \langle q | \alpha \rangle.$$

Сравнивая (14.56) и (14.58), легко увидеть, что решение уравнения (14.58) отличается от (14.57) сдвигом на величину  $\alpha \sqrt{\frac{2\hbar}{\omega}}$ . Действительно, уравнение (14.58) можно записать в виде

$$\left(\omega \left(q - \frac{\alpha}{\omega}\right) + \hbar \frac{\partial}{\partial q}\right) \Phi_\alpha(q) = 0.$$

Решением этого уравнения будет:

$$\Phi_\alpha(q) = \left(\frac{\omega}{\pi \hbar}\right)^{\frac{1}{4}} e^{-\frac{\omega}{2\hbar} \left(q - \sqrt{\frac{2\hbar}{\omega}} \alpha\right)^2}. \quad (14.59)$$

Когерентное состояние не является стационарным состоянием. Оно должно удовлетворять нестационарному уравнению Шредингера. От времени зависит  $\alpha = \alpha(t)$ . Подставляя (14.59) в уравнение Шредингера, эту зависимость можно определить, но и без этого ясно, что  $\alpha(t)$  должно колебаться по гармоническому закону на частоте моды. Примем

$$\alpha(t) = |\alpha| e^{-i\omega t}.$$

Тогда плотность вероятности будет иметь вид

$$\Phi_\alpha(q) \Phi_\alpha^*(q) = N e^{-\frac{\omega}{2\hbar} \left[ \left(q - \sqrt{\frac{2\hbar}{\omega}} \alpha\right)^2 + \left(q - \sqrt{\frac{2\hbar}{\omega}} \alpha^*\right)^2 \right]}.$$

Преобразуем выражение показателя экспоненты

$$\begin{aligned}
& \left[ \left( q - \sqrt{\frac{2\hbar}{\omega}} \alpha \right)^2 + \left( q - \sqrt{\frac{2\hbar}{\omega}} \alpha^* \right)^2 \right] = \\
& = q^2 + \frac{2\hbar}{\omega} \alpha^2 - 2q\alpha \sqrt{\frac{2\hbar}{\omega}} + q^2 + \frac{2\hbar}{\omega} \alpha^{*2} - 2q\alpha^* \sqrt{\frac{2\hbar}{\omega}} = \\
& = 2 \left[ q^2 + \frac{2\hbar}{\omega} \frac{\alpha^2 + \alpha^{*2}}{2} - 2q \sqrt{\frac{2\hbar}{\omega}} \frac{\alpha + \alpha^*}{2} + \frac{2\hbar}{\omega} (\alpha\alpha^*) - \frac{2\hbar}{\omega} (\alpha\alpha^*) \right] = \\
& = 2 \left[ q^2 + \frac{4\hbar}{\omega} \left( \frac{\alpha + \alpha^*}{2} \right)^2 - 2q \sqrt{\frac{2\hbar}{\omega}} \frac{\alpha + \alpha^*}{2} - \frac{2\hbar}{\omega} (\alpha\alpha^*) \right] = \\
& = 2 \left[ q - \sqrt{\frac{2\hbar}{\omega}} \frac{\alpha + \alpha^*}{2} \right]^2 + const = \\
& = 2 \left[ q - \sqrt{\frac{2\hbar}{\omega}} |\alpha| \cos \omega t \right]^2 + const.
\end{aligned}$$

Константа перейдет в нормирующий множитель, в результате мы получим:

$$\Phi_\alpha(q, t) \Phi_\alpha^*(q, t) = N e^{-\frac{\omega}{\hbar} \left[ q - \sqrt{\frac{2\hbar}{\omega}} |\alpha| \cos \omega t \right]^2}. \quad (14.60)$$

Из выражения (14.60) видно, что плотность вероятности для  $q$  (в нашем случае для напряженности электрического поля) для фиксированного времени такая же, как для вакуумного состояния, но смещена на величину  $\sqrt{\frac{2\hbar}{\omega}} \alpha(t)$ . Во времени центр распределения перемещается по гармоническому закону, как это изображено на [рис. 14.10](#)

Поскольку ширина распределения не зависит от амплитуды, относительная неопределенность с ростом амплитуды будет уменьшаться. Следовательно состояние будет стремиться к классическому.

## 14.7 Адиабатическая теорема

**Теорема 14.7.1** (Адиабатическая теорема). *Физическая система остается в своем мгновенном собственном состоянии, если возмущение действует достаточно медленно и если это состояние отделено энергетической щелью от остального спектра Гамильтониана.*

*Доказательство.* TBD

□



Рис. 14.10: Эволюция функции распределения когерентного состояния  $|\Phi_\alpha(q, t)|^2$  во времени.

## 14.8 Бозоны и фермионы

Рассмотрим ансамбль тождественных частиц. Состояние системы состоящей из  $n$  тождественных частиц может быть записано в следующем виде

$$|\psi\rangle = |x_1, x_2, \dots, x_k, \dots, x_j, \dots, x_n\rangle. \quad (14.61)$$

Для каждой из частиц в выражении (14.61) нас интересует некоторая физическая характеристика (например координата) которая обозначена через  $x$ .

Очевидно, что с точки зрения классики не должно быть никакой разницы если мы поменяем местами две частицы. При этом волновая функция которая определена с точностью до фазы может измениться. Таким образом обозначив через  $\hat{S}_{k,j}$  оператор который меняет местами две частицы с индексами  $k$  и  $j$  получим

$$\begin{aligned} \hat{S}_{k,j} |\psi\rangle &= |x_1, x_2, \dots, x_j, \dots, x_k, \dots, x_n\rangle = \\ &= e^{i\phi} |x_1, x_2, \dots, x_k, \dots, x_j, \dots, x_n\rangle = e^{i\phi} |\psi\rangle \end{aligned}$$

Если оператор  $\hat{S}_{k,j}$  применить два раза то очевидно что система будет приведена полностью в исходное состояние, т.е.

$$\hat{S}_{k,j}^2 |\psi\rangle = e^{2i\phi} |\psi\rangle = |\psi\rangle$$

откуда следует, что  $\phi$  может принимать два значения 0 и  $\pi$ . Таким образом мы можем разделить все частицы на два класса. Для первого из них волновая



функция не меняется при перестановке двух частиц ( $\psi = 0$ ), а для второго меняет знак ( $\psi = \pi$ ).

**Пример 14.8.1.** Рассмотрим систему состоящую из двух частиц. Допустим что 1-ая частица может находиться в одном из двух состояний  $|\psi_1^{(1)}\rangle$  или  $|\psi_2^{(1)}\rangle$ . Аналогично 2-ая частица может находиться в одном из двух состояний  $|\psi_1^{(2)}\rangle$  или  $|\psi_2^{(2)}\rangle$ .

Предположим общая волновая функция  $|\psi^{(12)}\rangle$  двух частиц представима в виде суперпозиции волновых функций одиночных частиц, т.е.

$$|\psi^{(12)}\rangle = |\psi_{1,2}^{(1)}\rangle \pm |\psi_{1,2}^{(2)}\rangle$$

Случай симметричной (при перестановке частиц) волновой функции будет иметь вид

$$|\psi^{(12)}\rangle = |\psi_{1,2}^{(1)}\rangle + |\psi_{1,2}^{(2)}\rangle$$

при этом обе частицы могут находиться в одном и том же состоянии, т. е. иметь одну и ту же волновую функцию

$$|\psi\rangle = |\psi_1^{(1)}\rangle = |\psi_1^{(2)}\rangle. \quad (14.62)$$

В этом случае

$$|\psi^{(12)}\rangle = 2|\psi\rangle,$$

т. е. частицы могут одновременно находиться в одном и том же состоянии.

Для случая антисимметричной волновой функции имеем

$$|\psi^{(12)}\rangle = |\psi_{1,2}^{(1)}\rangle - |\psi_{1,2}^{(2)}\rangle$$

и если обе частицы находятся в одном и том же состоянии (14.62), то для  $\psi^{(12)}$  получим

$$|\psi^{(12)}\rangle = |\psi\rangle - |\psi\rangle = 0,$$

т. е. в этом случае частицы не могут одновременно находиться в одном и том же состоянии.

Имея в виду пр. 14.8.1, можно рассмотреть общий случай ансамбля тождественных частиц, каждая из которых находится в одном и том же состоянии

или по другому имеют одну и ту же волновую функцию. В этом случае при перемене частиц реальный вид волновой функции ансамбля не меняется:

$$|\psi^{(12)}\rangle = |\psi^{(21)}\rangle.$$

Т. е. в антисимметричном случае

$$|\psi^{(12)}\rangle = -|\psi^{(21)}\rangle = -|\psi^{(12)}\rangle = 0.$$

Таким образом мы можем сказать, что частицы состояния ансамбля которых симметричны могут находиться одновременно в одном и том же состоянии. Такие частицы называются бозонами.

Для антисимметричного случая будем предполагать, что такие частицы не могут одновременно находиться в одном и том же состоянии. Такие частицы называются фермионами.

Рассмотрим состояние с определенным числом частиц  $n$   $|\psi\rangle = |n\rangle$ . В случае бозонов мы будем иметь

$$|\psi_b\rangle = |n\rangle_b. \quad (14.63)$$

Операторы рождения  $\hat{a}_b^\dagger$  и уничтожения  $\hat{a}_b$  действуют на состояние (14.63) следующим образом

$$\begin{aligned} \hat{a}_b^\dagger |n\rangle_b &= \sqrt{n+1} |n+1\rangle_b, \\ \hat{a}_b |n\rangle_b &= \sqrt{n} |n-1\rangle_b \end{aligned}$$

Для фермионов возможны два состояния:  $|0\rangle_f$  и  $|1\rangle_f$  при этом соответствующие операторы рождения  $\hat{a}_f^\dagger$  и уничтожения  $\hat{a}_f$  действуют следующим образом

$$\begin{aligned} \hat{a}_f^\dagger |0\rangle_f &= |1\rangle_f, \\ \hat{a}_f^\dagger |1\rangle_f &= 0, \\ \hat{a}_f |0\rangle_f &= 0, \\ \hat{a}_f |1\rangle_f &= |0\rangle_f. \end{aligned}$$

## 14.9 Золотое правило Ферми

Золотое правило Ферми позволяет, используя временную теорию возмущений вычислить вероятность перехода между двумя состояниями квантовой системы.

**Теорема 14.9.1** (Золотое правило Ферми). *Допустим, что квантовая система находится изначально в состоянии  $|i\rangle$  и мы хотим оценить вероятность перехода в состояние  $|f\rangle$ . Гамильтониан рассматриваемой системы состоит из двух частей: стационарного гамильтониана  $\hat{H}_0$  и слабого возмущения  $\hat{V}$ :*

$$\hat{H} = \hat{H}_0 + \hat{V}$$

*В этом случае искомая вероятность задается*

$$W_{i \rightarrow f} = \frac{2\pi}{\hbar} \left| \langle f | \hat{V} | i \rangle \right|^2 \rho,$$

*где  $\rho$  является плотностью конечных состояний.*

*Доказательство.* Допустим, что существует состояния  $\{|n\rangle\}$  образуют полный набор собственных векторов гамильтониана  $\hat{H}_0$ , т.е.

$$\hat{H}_0 |n\rangle = E_n |n\rangle,$$

при этом, рассматриваемое начальное состояние  $|i\rangle$  и конечное состояние  $|f\rangle$  принадлежат этой системе векторов, т. е.

$$|i\rangle, |f\rangle \in \{|n\rangle\}.$$

В некоторый момент времени система оказывается в состоянии  $|\psi\rangle$ , которое удовлетворяет уравнению Шредингера:

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{H} |\psi\rangle. \quad (14.64)$$

Наша задача заключается в вычислении вероятности того что при наблюдении система окажется в состоянии  $|f\rangle$ , при том что начальное условие для (14.64) имеет следующий вид

$$|\psi\rangle|_{t=0} = |i\rangle. \quad (14.65)$$

В силу полноты системы  $\{|n\rangle\}$  состояние  $|\psi\rangle$  может быть представлено в виде

$$|\psi\rangle = \sum_n a_n(t) |n\rangle e^{\frac{-iE_n t}{\hbar}} \quad (14.66)$$

Подставив (14.66) в уравнение Шредингера (14.64) получим

$$i\hbar \sum_n \frac{\partial a_n(t)}{\partial t} |n\rangle e^{\frac{-iE_n t}{\hbar}} + \sum_n a_n(t) |n\rangle i\hbar \frac{\partial e^{\frac{-iE_n t}{\hbar}}}{\partial t} = \quad (14.67)$$

$$\begin{aligned} &= i\hbar \sum_n e^{\frac{-iE_n t}{\hbar}} |n\rangle \left( \frac{\partial a_n(t)}{\partial t} - \frac{iE_n}{\hbar} a_n(t) \right) = \\ &= i\hbar \sum_n e^{\frac{-iE_n t}{\hbar}} \frac{\partial a_n(t)}{\partial t} |n\rangle + \sum_n E_n a_n(t) |n\rangle e^{\frac{-iE_n t}{\hbar}} = \\ &= i\hbar \sum_n e^{\frac{-iE_n t}{\hbar}} \frac{\partial a_n(t)}{\partial t} |n\rangle + \sum_n E_n a_n(t) |n\rangle e^{\frac{-iE_n t}{\hbar}}. \end{aligned} \quad (14.68)$$

С другой стороны выражение (14.68) должно равняться

$$\hat{H} |\psi\rangle = \sum_n E_n a_n(t) |n\rangle e^{\frac{-iE_n t}{\hbar}} + \sum_n a_n(t) e^{\frac{-iE_n t}{\hbar}} \hat{V} |n\rangle,$$

т. е.

$$i\hbar \sum_n e^{\frac{-iE_n t}{\hbar}} \frac{\partial a_n(t)}{\partial t} |n\rangle = \sum_n a_n(t) e^{\frac{-iE_n t}{\hbar}} \hat{V} |n\rangle. \quad (14.69)$$

Выражение (14.69) будем решать методом теории возмущений, т.е.

$$a_n(t) = a_n^{(0)}(t) + a_n^{(1)}(t) + \dots,$$

при этом будем полагать, что

$$a_n^{(0)}(t) = \text{const}|_t = a_n^{(0)}(0),$$

откуда с учетом начального условия (14.65)

$$a_n^{(0)}(t) = \delta_{ni}.$$

Таким образом для первого порядка теории возмущений из (14.69) получим

$$i\hbar \sum_n e^{\frac{-iE_n t}{\hbar}} \frac{\partial a_n^{(1)}(t)}{\partial t} |n\rangle = \sum_n \delta_{ni} e^{\frac{-iE_n t}{\hbar}} \hat{V} |n\rangle = e^{\frac{-iE_i t}{\hbar}} \hat{V} |i\rangle. \quad (14.70)$$

Следовательно из (14.70) имеем

$$\frac{\partial a_n^{(1)}(t)}{\partial t} = -\frac{i}{\hbar} e^{\frac{-i(E_i - E_n)t}{\hbar}} \langle n | \hat{V} | i \rangle,$$

обозначив  $E_i - E_n = \hbar\omega_{in}$ , где  $\omega_{in}$  - частота перехода между состояниями  $|i\rangle$  и  $|n\rangle$ , после интегрирования получим

$$a_n^{(1)}(t) = -\frac{i}{\hbar} \int_0^t e^{-i\omega_{in}t'} \langle n | \hat{V} | i \rangle dt',$$

т.е.

$$\begin{aligned} a_n^{(1)}(t) &= \frac{1}{\hbar\omega_{in}} \langle n | \hat{V} | i \rangle (e^{-i\omega_{in}t} - 1) = \\ &= \frac{1}{\hbar\omega_{in}} \langle n | \hat{V} | i \rangle e^{\frac{-i\omega_{in}t}{2}} \left( e^{\frac{-i\omega_{in}t}{2}} - e^{\frac{i\omega_{in}t}{2}} \right) = \\ &= -\frac{2i}{\hbar\omega_{in}} \langle n | \hat{V} | i \rangle e^{\frac{-i\omega_{in}t}{2}} \sin\left(\frac{\omega_{in}t}{2}\right) \end{aligned} \quad (14.71)$$

Нас интересует скорость  $W_{i \rightarrow f}$  перехода в состояние  $|f\rangle$ , которая задается выражением

$$W_{i \rightarrow f} = \frac{|a_f^{(1)}(t)|^2}{t}.$$

Или же

$$W_{i \rightarrow f} = \frac{t}{\hbar^2} \left| \langle f | \hat{V} | i \rangle \right|^2 \frac{\sin^2\left(\frac{\omega_{if}t}{2}\right)}{\left(\frac{\omega_{if}t}{2}\right)^2}. \quad (14.72)$$

В случае если финальное состояние  $|f\rangle$  представляет собой некоторый непрерывный спектр вблизи энергии  $E_f$ , то выражение (14.72) должно быть просуммировано для всех финальных состояний у которых  $\omega_{nf} \approx 0$ . Введем понятие плотности состояний  $\rho(E) = \frac{dn}{dE}$ , так что число состояний  $dn$  приходящееся на бесконечно малый интервал энергий  $dE$  может быть представлено в виде  $dn = \rho dE$ . Следовательно скорость перехода может быть переставлена в виде:

$$W_{i \rightarrow f} = \sum_{n: E_n \approx E_f} \rho(E_n) W_{i \rightarrow f}(E_n),$$

т.е. предполагая для рассматриваемого интервала энергий  $\rho(E_n) \approx \rho(E_f)$ ,

$$\left| \langle n | \hat{V} | i \rangle \right|^2 \approx \left| \langle f | \hat{V} | i \rangle \right|^2$$

и заменяя суммирование интегрированием, получим

$$\begin{aligned}
 W_{i \rightarrow f} &\approx \int_{E_n \approx E_f} \rho(E_n) dE_n \frac{t}{\hbar^2} \left| \langle n | \hat{V} | i \rangle \right|^2 \frac{\sin^2 \left( \frac{\omega_{in} t}{2} \right)}{\left( \frac{\omega_{in} t}{2} \right)^2} = \\
 &= \int_{\omega_{in} \approx \omega_{if}} \rho(E_n) dE_n \frac{t}{\hbar^2} \left| \langle n | \hat{V} | i \rangle \right|^2 \frac{\sin^2 \left( \frac{\omega_{in} t}{2} \right)}{\left( \frac{\omega_{in} t}{2} \right)^2} \approx \\
 &\approx \frac{2}{\hbar} \left| \langle f | \hat{V} | i \rangle \right|^2 \rho \int_{-\infty}^{\infty} d \left( \frac{\omega t}{2} \right) \frac{\sin^2 \left( \frac{\omega t}{2} \right)}{\left( \frac{\omega t}{2} \right)^2} = \frac{2\pi}{\hbar} \left| \langle f | \hat{V} | i \rangle \right|^2 \rho,
 \end{aligned} \tag{14.73}$$

что совпадает с доказываемым выражением.

□

## Глава 15

# Теория вероятностей

Когда говорят о квантовой механике, то очень часто ее считают прикладной частью классической теории вероятности. Такое допущение верно лишь отчасти, вероятности лежащие в основе таких эффектов как перепутанные состояния и неклассический свет имеют принципиально неклассическую природу, т.е. не описываются классической Колмогоровской теорией вероятности. Материал в этом разделе в основном опирается на монографии [32] и [33] в которых делается сравнение между классической и квантовой теорией вероятности.

### 15.1 Алгебра множеств и базовые понятия теории вероятностей

**Определение 15.1.1** ( $\sigma$ -алгебра). Допустим, что  $\Omega$  некоторое множество, тогда семейство  $\mathcal{F}$  подмножеств множества  $\Omega$  называется  $\sigma$ -алгеброй если выполнены следующие условия

- $\mathcal{F}$  содержит  $\Omega$ :  $\Omega \in \mathcal{F}$
- если  $\Upsilon \in \mathcal{F}$  тогда  $\Omega \setminus \Upsilon \in \mathcal{F}$
- объединение или пересечение счетного подсемейства  $\mathcal{F}$  принадлежит  $\mathcal{F}$

**Определение 15.1.2** (Мера). Если  $\mathcal{F}$  некоторая  $\sigma$ -алгебра тогда следующая функция

$$\mu : \mathcal{F} \rightarrow [0, \infty]$$

называется мерой если

- $\mu(\emptyset) = 0$
- $\forall A, B \in \mathcal{F}, A \cap B = \emptyset$  мы имеем  $\mu(A \cup B) = \mu(A) + \mu(B)$

## 15.2 Классическая Колмогоровская теория вероятностей

### 15.2.1 Базовые понятия и аксиомы теории вероятности

Классическая теория вероятностей имеет дело с теорией множеств и базируется на нескольких простых аксиомах. Данная аксиоматика была предложена в 30-х годах XX века Колмогоровым А. Н. [31].

Прежде всего несколько определений объектов с которыми мы будем иметь дело.

**Определение 15.2.1** (Пространство событий).  $\mathcal{F}$  некоторая  $\sigma$ -алгебра заданная на некотором множестве  $\Omega$  называется пространством событий.

**Комментарий 15.2.1** (Пространство событий). В силу свойств  $\sigma$ -алгебра имеем следующие факты: если  $\Omega \subset \Omega$ ,  $\emptyset \subset \Omega$  и для любых  $A, B \subset \Omega$  имеет место  $A \cup B \subset \Omega$ ,  $A \cap B \subset \Omega$  и  $A \setminus B \subset \Omega$ . Элемент множества  $\omega \in \Omega$  называется элементарным событием. Подмножество  $A \subset \Omega$  или же  $A \in \mathcal{F}$  называется событием.

**Определение 15.2.2** (Вероятность  $P$ ). Конечная мера заданная на  $\mathcal{F}$  над множеством  $\Omega$  называется вероятностью если  $P(\Omega) = 1$ .

**Пример 15.2.1** (Пространство событий). На [рис. 15.1](#) изображено множество  $\Omega$  которое мы называем пространством событий. Элементы множества  $\omega_i \in \Omega$  (черные точки на [рис. 15.1](#)) - элементарные события. Подмножество  $A \subset \Omega$  - событие.

Теперь собственно говоря аксиомы.

**Аксиома 15.2.1** (Не-отрицательность). Вероятность события  $A \subset \Omega$  есть неотрицательное вещественное число, т. е.  $P() \geq 0$

**Аксиома 15.2.2** (Нормировка). Вероятность пространства событий  $\Omega$  есть 1, т. е.  $P(\Omega) = 1$

**Аксиома 15.2.3** (Аддитивность). Если  $A_i \cap A_j = \emptyset$  тогда  $P(A_i \cup A_j) = P(A_i) + P(A_j)$

**Пример 15.2.2** (Аксиомы Колмогоровской теории вероятностей). Каждому элементарному событию  $\omega_i \in \Omega$  на [рис. 15.2](#) поставим в соответствие неотрицательное число  $P(\omega_i) = \frac{1}{12}$ . Вероятность события  $A$  -  $P(A) = \frac{5}{13}$



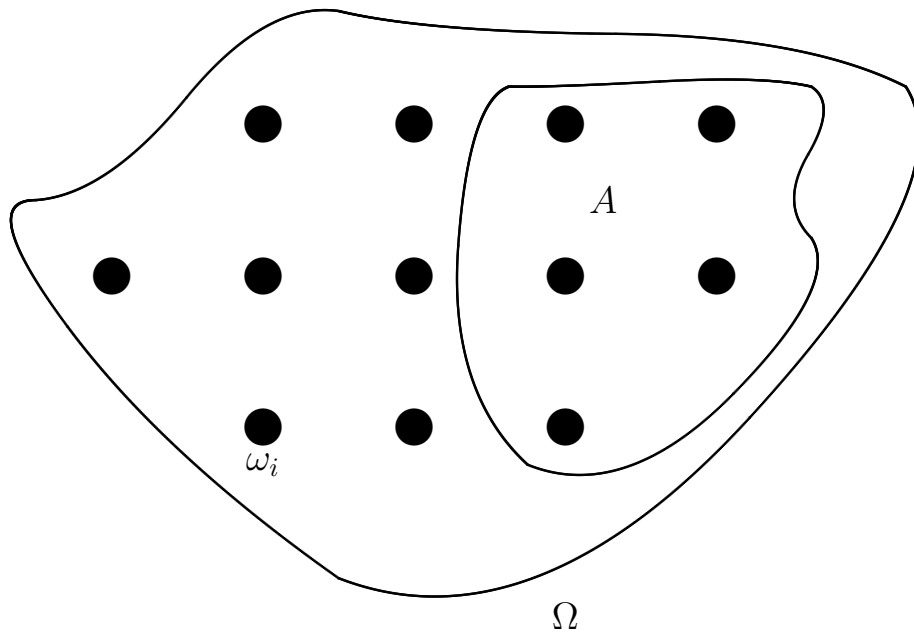


Рис. 15.1: Пространство событий  $\Omega$  представляет собой множество, которое состоит из 12 элементов (элементарных событий)  $\omega_i \in \Omega$ . Подмножество  $A \subset \Omega$  (событие) содержит 5 элементов (элементарных событий) множества  $\Omega$

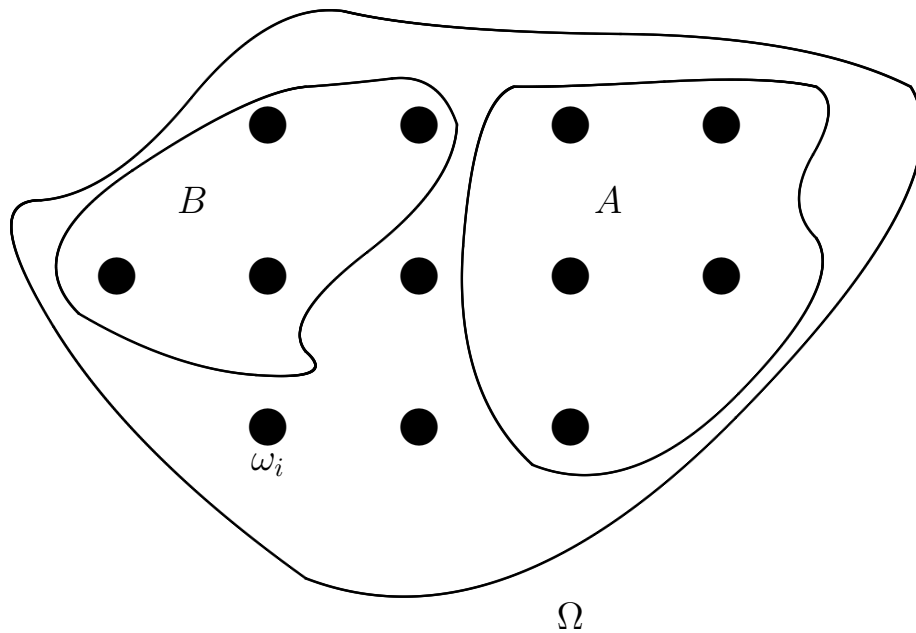
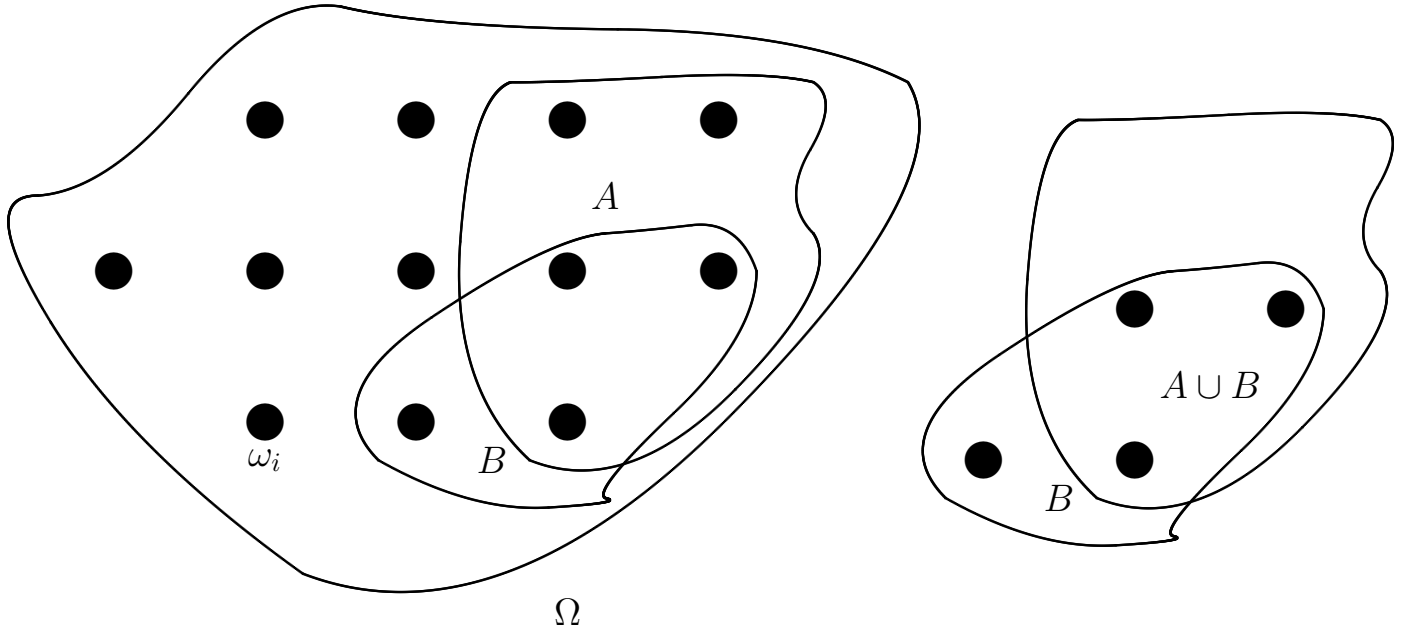


Рис. 15.2: Пространство событий  $\Omega$ , элементарное событие  $\omega \in \Omega$ , события  $A \subset \Omega$  и  $B \subset \Omega$ .  $P(\omega) = \frac{1}{12}$ ,  $P(\Omega) = \frac{12}{12} = 1$ ,  $P(A) = \frac{5}{12}$ ,  $P(B) = \frac{4}{12}$ ,  $P(A \cup B) = P(A) + P(B) = \frac{5}{12} + \frac{4}{12} = \frac{9}{12} = \frac{3}{4}$

Рис. 15.3: Условная вероятность  $P(A|B)$ 

для события  $B$  имеем  $P(B) = \frac{4}{13}$ . Таким образом в силу того, что  $A \cap B = \emptyset$ , используя аксиому 15.2.3 получим:

$$P(A \cup B) = P(A) + P(B) = \frac{5}{12} + \frac{4}{12} = \frac{3}{4}.$$

Для события  $\Omega$  в силу аксиомы 15.2.2 имеем  $P(\Omega) = 1$ . С другой стороны  $\Omega = \cup_i \omega_i$  т.е.

$$P(\Omega) = \sum_i P(\omega_i) = 12 \cdot \frac{1}{12} = 1.$$

Все известные факты теории вероятности выводятся из этих трех аксиом.  
TBD

## 15.2.2 Случайная величина. Функции распределения

**Определение 15.2.3** (Случайная величина). Если  $\Omega$  - пространство событий (см. определение 15.2.1), то отображение  $X : \Omega \rightarrow \mathbb{R}$  называется случайной величиной.

Стоит отметить что если случайную величину записывают с помощью большой буквы  $X$ , то конкретную реализацию с помощью строчной буквы  $x$ , т.е. если  $\omega \in \Omega$ , то  $x = X(\omega)$ . В частности для дискретных случайных

величин каждой реализации  $x = X(\omega)$  можно поставить в соответствие некоторую вероятность  $P(x) = P(\omega)$ . В противном случае используют функции распределения.

**Определение 15.2.4** (Функция распределения случайной величины). Функция распределения  $F_X$  случайной величины  $X$  называется функция  $F_X : \mathbb{R} \rightarrow [0, 1]$ , которая задается формулой

$$F_X(x) = P(X \leq x),$$

т.о. функция распределения от аргумента  $x$  равна вероятности тех событий  $\omega \in \Omega$  для которых  $X(\omega) \leq x$ .

**Определение 15.2.5** (Плотность распределения случайной величины). Случае непрерывных случайных величин имеет смысл говорить о плотности распределения  $f_X(x)$ , которая определяется следующим выражением

$$f_X(x) = \frac{dF_X(x)}{dx}$$

**Определение 15.2.6** (Среднее случайной величины). Для дискретной случайной величины, т.е. если множество элементарных событий счетно, то среднее  $E(X)$  случайной величины  $X$  определяется следующим соотношением

$$E(X) = \sum_{\omega} p_{\omega} \cdot X(\omega) = \sum_x p_x \cdot x,$$

где суммирование производится по всем возможным элементарным исходам  $\omega$ ,  $x = X(\omega)$ ,  $p_{\omega} = p_{X(\omega)} = p_x$ . Для непрерывных случайных величин это соотношение трансформируется в

$$E(X) = \int_{-\infty}^{\infty} x \cdot f_X(x) dx.$$

TBD

### 15.2.3 Распределение Пуассона

Распределение Пуассона играет очень важную роль в квантовой оптике и поэтому на нем стоит остановиться подробнее.

**Определение 15.2.7** (Распределение Пуассона).

TBD

### 15.2.4 Случайные процессы

Для полного описания некоторого случайного процесса  $x(t)$  необходимо знать все функции плотности совместной вероятности

$$p_n(\{x\}_n, \{t\}_n) = p_n(x_1, x_2, \dots, x_n, t_1, t_2, \dots, t_n).$$

Например при помощи  $p_1 = p_1(x, t)$  можно подсчитать среднее значение случайной величины

$$\langle x(t) \rangle = \int x p_1(x, t) dx, \quad (15.1)$$

а при помощи  $p_2 = p_2(x_1, x_2, t_1, t_2)$  - так называемую двухвременную автокорреляционную функцию

$$r(t_1, t_2) = \langle x^*(t_1) x(t_2) \rangle = \int \int x_1 x_2 p_2(x_2, t_2, x_1, t_1) dx_1 dx_2. \quad (15.2)$$

В том случае, когда среднее случайной величины (15.1) не зависит от  $t$ :

$$\langle x(t) \rangle = \text{const}_t, \quad (15.3)$$

а автокорреляционная функция (15.2) зависит только от разности  $t_1 - t_2 = \tau$ :

$$r(t_1, t_2) = r(t_1 - t_2) = r(\tau), \quad (15.4)$$

то случайный процесс называется стационарным в широком смысле. Очевидно, что для таких процессов справедливо следующее тождество

$$r(-\tau) = r^*(\tau), \quad (15.5)$$

действительно, из (15.4) имеем

$$r(-\tau) = r(t_2 - t_1) = r(t_2, t_1) = r^*(t_1, t_2) = r^*(\tau).$$

Для стационарных в широком смысле случайных процессов справедлива следующая теорема,

**Теорема 15.2.1** (Хинчин-Винер). Автокорреляционная функция стационарных в широком смысле случайных процессов и их спектральная плотность связаны прямым и обратным преобразованием Фурье.

*Доказательство.* Доказательство будет не строгим и является попыткой объяснить смысл этой теоремы, для чего рассмотрим следующий интеграл

$$\tilde{x}(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} x(t) e^{i\omega t} dt, \quad (15.6)$$

который можно трактовать как Фурье образ (см. [разд. 18.1](#)) случайного процесса  $x(t)$ . Для стационарных случайных процессов очевидно, что интеграл (15.6) в общем случае не существует. Действительно в случае существования этого интеграла было бы справедливо соотношение Парсеваля

$$\int_{-\infty}^{\infty} |\tilde{x}(\omega)|^2 d\omega = \int_{-\infty}^{\infty} |x(t)|^2 dt, \quad (15.7)$$

которое очевидным образом расходится в случае стационарного случайного процесса. При этом в силу (15.7)  $S(\omega) = |\tilde{x}(\omega)|^2$  представляет собой распределение энергии по оси частот для конкретной реализации процесса, а усредненное значение  $\langle S(\omega) \rangle$  представляет некоторую характеристику случайного процесса, которая описывает распределение энергии по частотам.

Не смотря на то что интеграл (15.7) расходится для рассматриваемых случайных процессов, как показали Хинчин и Винер, существует интеграл

$$\langle \tilde{x}^*(\omega) \tilde{x}(\omega') \rangle = \frac{1}{(2\pi)^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \langle x^*(t) x(t') \rangle e^{i(\omega't' - \omega t)} dt dt', \quad (15.8)$$

который можно трактовать как спектральную плотность мощности  $S(\omega, \omega')$  рассматриваемого случайного процесса. Таким образом, с учетом стационарности

$$\langle x^*(t) x(t') \rangle = r(t' - t) = r(\tau),$$

получим

$$\begin{aligned} S(\omega, \omega') &= \langle \tilde{x}^*(\omega) \tilde{x}(\omega') \rangle = \\ &= \frac{1}{(2\pi)^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \langle x^*(t) x(t') \rangle e^{i(\omega't' - \omega t)} dt dt' = \\ &= \frac{1}{(2\pi)^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} r(\tau) e^{i(\omega' - \omega)t} e^{i\omega'(t' - t)} dt d\tau = \\ &= \frac{1}{(2\pi)^2} \int_{-\infty}^{\infty} e^{i(\omega' - \omega)t} dt \int_{-\infty}^{\infty} r(\tau) e^{i\omega'\tau} d\tau = \\ &= \tilde{r}(\omega') \delta(\omega' - \omega), \end{aligned} \quad (15.9)$$

где использовано интегральное представление дельта-функции (18.3).

Таким образом из (15.9) следует, что Фурье образ автокорреляционной функции  $\tilde{r}(\omega)$  может рассматриваться как спектральная плотность случайного процесса (15.8).  $\square$

### 15.3 Квантовая теория вероятностей

Говоря о квантовой теории вероятности, мы будем опираться на классическую (Колмогоровскую), при этом мы постараемся выбрать такой вариант формулировки который будет применим к обоим случаям. В качестве модельной будем рассматривать систему с  $n$  возможными исходами, т.е. ту в которой классическое распределение вероятностей задается следующим распределением:

$$p = \{p_1, p_2, \dots, p_n\} \quad (15.10)$$

Квантовое состояние полностью описывается в общем случае (как чистых так и смешанных состояний) с помощью матрицы плотности

$$\hat{\rho} = \begin{bmatrix} \rho_{11} & \rho_{12} & \cdots & \rho_{1n} \\ \rho_{21} & \rho_{22} & \cdots & \rho_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n1} & \rho_{n2} & \cdots & \rho_{nn} \end{bmatrix}.$$

В классическом случае этому объекту соответствует распределение вероятностей (15.10), которое также можно представить в виде некоторой матрицы

$$\hat{p} = \begin{bmatrix} p_1 & 0 & \cdots & 0 \\ 0 & p_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_n \end{bmatrix}.$$

Стоит отметить, что для обоих случаев выполняется равенство

$$Sp(\hat{\rho}) = Sp(\hat{p}) = 1,$$

которое представляет собой переписанный вариант аксиомы 15.2.2.

Наблюдаемой  $\hat{x}$  соответствует некоторая матрица

$$\hat{x} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix}, \quad (15.11)$$

которая в классическом случае является диагональной

$$\hat{x} = \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x_n \end{bmatrix}. \quad (15.12)$$

При этом стоит отметить, что вычисление среднего при этом приобретает знакомый классический вид

$$\bar{x} = Sp(\hat{p}\hat{x}) = \sum_{i=1}^n p_i x_i.$$

**Комментарий 15.3.1.** *Стоит отметить, что для любой наблюдаемой  $\hat{X}$ , в силу самосопряженности  $\hat{X} = \hat{X}^\dagger$ , можно подобрать базис в котором соответствующая матрица будет диагональной и на диагонали будут стоять собственные числа. При этом если две наблюдаемые  $\hat{X}$  и  $\hat{Y}$  коммутируют:*

$$\hat{X}\hat{Y} = \hat{Y}\hat{X},$$

*то они диагонализуются в общем базисе.*

Отличие квантовой теории вероятностей от классической может быть показано несколькими способами [32, 33], один из которых основан на некоммутативности квантового описания. Действительно можно отметить, что в общем случае квантовые наблюдаемые представляемые матрицами вида (15.11) не коммутируют друг с другом. При этом классические наблюдаемые, записываемые в виде диагональных матриц (15.12) всегда коммутируют друг с другом. Из этого выводится много фактов TBD





## Глава 16

# Абстрактная алгебра

Здесь можно найти определения и базовые свойства групп, колец и полей.

### 16.1 Введение в теорию групп

**Определение 16.1.1.** Группой  $(\mathcal{G}, \circ)$  называется множество элементов  $g \in \mathcal{G}$  для которого определена некоторая бинарная операция  $\circ$  (часто ее называют умножением, либо сложением):

$$\begin{aligned} \forall g_1, g_2 \in \mathcal{G}, \\ g_1 \circ g_2 \in \mathcal{G}. \end{aligned} \tag{16.1}$$

Операция определенная посредством (16.1) обладает свойством ассоциативности:

$$g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3.$$

Рассматриваемое множество должно содержать элемент  $e_{\mathcal{G}}$  обладающий следующим свойством, справедливым для любого элемента множества  $g$ :

$$g \circ e_{\mathcal{G}} = e_{\mathcal{G}} \circ g = g.$$

Для каждого элемента группы  $g$  должен существовать обратный элемент  $g^{-1} \in \mathcal{G}$ , обладающий следующим свойством

$$g \circ g^{-1} = g^{-1} \circ g = e_{\mathcal{G}}$$

**Определение 16.1.2** (Моноид). Если для некоторого множества элементов  $\mathcal{G}$  у нас не выполнено последнее свойств группы (существование обратного элемента), то данное множество называется моноидом (monoid) или полугруппой.

**Определение 16.1.3** (Абелева группа). Группа  $(\mathcal{A}, \circ)$  называется абелевой, или коммутативной если  $\forall a_1, a_2 \in \mathcal{A}: a_1 \circ a_2 = a_2 \circ a_1$ .

**Пример 16.1.1.** Группа  $(\mathbb{Z}, +)$  Множество целых чисел  $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$  представляет собой группу относительно операции сложения.

**Определение 16.1.4** (Циклическая группа). Циклическая группа  $G$  - это группа которая порождена единственным элементом  $g : G = \langle g \rangle$ , т.е. все ее элементы являются степенями  $g$ . Элемент  $g$  называется порождающим элементом, или генератором, группы  $G$ .

**Определение 16.1.5** (Мультипликативная группа кольца вычетов). Рассмотрим набор целых чисел взаимно простых с  $n$  и меньших  $n$ , который обозначим через  $(\mathbb{Z}/n\mathbb{Z})^\times$ . В качестве операции умножения двух элементов  $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$  примем

$$a \circ b = a \cdot b \pmod n.$$

Единичным элементом  $e_{(\mathbb{Z}/n\mathbb{Z})^\times}$  является 1. Кроме того можно показать, что для каждого  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$  существует  $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$  такой что  $a \circ a^{-1} = 1$ . Таким образом  $(\mathbb{Z}/n\mathbb{Z})^\times$  является группой.

**Теорема 16.1.1** (О порядке  $(\mathbb{Z}/n\mathbb{Z})^\times$ ). Порядок группы  $(\mathbb{Z}/n\mathbb{Z})^\times$  определяется следующим соотношением

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n),$$

где  $\phi(n)$  - функция Эйлера (19.3.1). При этом если  $n = p$  - простое число, то

$$|(\mathbb{Z}/p\mathbb{Z})^\times| = \phi(p),$$

и если  $a \in (\mathbb{Z}/p\mathbb{Z})^\times, a \neq 1$ , то  $a$  - генератор рассматриваемой группы, т.е.

$$a^{p-1} = 1.$$

*Доказательство.* TBD □

**Теорема 16.1.2** (Лагранж). Для любой конечной группы  $\mathcal{G}$  порядок (число элементов) любой подгруппы  $\mathcal{H}$  делит порядок  $\mathcal{G}$ :

$$|\mathcal{G}| = h |\mathcal{H}|,$$

где целое число  $h$  называется кофактором подгруппы.

## 16.2 Поля

**Определение 16.2.1** (Поле (алгебра)). Пусть задана Абелева группа (см. определение 16.1.3)  $(\mathcal{F}, +)$ . Единичный элемент этой группы  $e_{\mathcal{F}}$  - 0. Пусть также  $(\mathcal{F} \setminus \{0\}, \cdot)$  - некоторая другая группа (также Абелева) с единичным элементом 1. Кроме того операции  $+$ ,  $\cdot$  удовлетворяют свойству дистрибутивности, т.е.  $\forall a, b, c \in \mathcal{F}$ :

$$\begin{aligned} c \cdot (a + b) &= c \cdot a + c \cdot b, \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned}$$

В этом случае  $(\mathcal{F}, +, \cdot)$  называется полем.

**Пример 16.2.1** (Поле  $\mathbb{Q}$ ). Заметим, что  $\mathbb{Z}$  не является полем, поскольку не для любого целого определен обратный элемент относительно операции умножения. Вместе с тем следующее множество будет полем:  $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$ . При этом обратный по отношению к  $a/b \in (\mathbb{Q} \setminus \{0\}, \cdot)$  будет  $b/a$ .

**Пример 16.2.2** (Поле  $\mathbb{R}$ ). Вещественные числа образуют поле.

**Пример 16.2.3** (Поле  $\mathbb{C}$ ). Комплексные числа образуют поле.



## Глава 17

# Линейная алгебра

### 17.1 Линейное пространство

**Определение 17.1.1** (Линейное пространство). TBD

#### 17.1.1 Прямая сумма линейных пространств и тензорное произведение

Допустим у нас имеется два линейных пространства  $\mathbb{A}$  и  $\mathbb{B}$  с базисами  $\{a_i\} \subset \mathbb{A}$  и  $\{b_j\} \subset \mathbb{B}$  соответственно.

**Определение 17.1.2** (Тензорное произведение линейных пространств). Линейное пространство  $\mathbb{L} = \mathbb{A} \otimes \mathbb{B}$  с базисом  $l_{ij} = a_i \otimes b_j$  называется тензорным произведением линейных пространства  $\mathbb{A}$  и  $\mathbb{B}$ .

**Определение 17.1.3** (Тензорное (внешнее) произведение линейных операторов). Рассмотрим два линейных оператора  $\hat{A} : \mathbb{A} \rightarrow \mathbb{A}$  и  $\hat{B} : \mathbb{B} \rightarrow \mathbb{B}$  тогда оператор  $\hat{L} = \hat{A} \otimes \hat{B} : \mathbb{L} \rightarrow \mathbb{L}$  действующий на базис по правилу

$$\hat{L}l_{ij} = \hat{L}a_i \otimes b_j = \hat{A}a_i \otimes \hat{B}b_j$$

называется тензорным произведением операторов.

#### 17.1.2 Теорема об операторном разложении

**Теорема 17.1.1** (Об операторном тождестве).

$$e^{\hat{A}}\hat{B}e^{-\hat{A}} = \hat{B} + [\hat{A}, \hat{B}] + \frac{1}{2!} [\hat{A}, [\hat{A}, \hat{B}]] + \dots \quad (17.1)$$

*Доказательство.* Для доказательства введем следующую вспомогательную функцию:

$$f(\alpha) = e^{\alpha \hat{A}} \hat{B} e^{-\alpha \hat{A}}, \quad (17.2)$$

которая совпадает с искомым выражением при  $\alpha = 1$ . Разложим (17.2) в ряд Тейлора:

$$f(\alpha) = f(0) + \frac{\alpha}{1!} f'(0) + \frac{\alpha^2}{2!} f''(0) + \dots + \frac{\alpha^k}{k!} f^{(k)}(0) + \dots \quad (17.3)$$

Справедливо следующее рекуррентное соотношение:

$$\begin{aligned} f^{(k)}(\alpha) &= [\hat{A}, f^{(k-1)}(\alpha)] = \\ &= \underbrace{[\hat{A}[\dots[\hat{A}, f^{(0)}(\alpha)]\dots]}_{k \text{ раз}}, \end{aligned} \quad (17.4)$$

где

$$f^{(0)}(\alpha) = f(\alpha).$$

Действительно по индукции имеем для первой производной:

$$\begin{aligned} f^{(1)}(\alpha) &= \hat{A} e^{\alpha \hat{A}} \hat{B} e^{-\alpha \hat{A}} - e^{\alpha \hat{A}} \hat{B} \hat{A} e^{-\alpha \hat{A}} = \\ &= \hat{A} e^{\alpha \hat{A}} \hat{B} e^{-\alpha \hat{A}} - e^{\alpha \hat{A}} \hat{B} e^{-\alpha \hat{A}} \hat{A} = \\ &= [\hat{A}, e^{\alpha \hat{A}} \hat{B} e^{-\alpha \hat{A}}] = [\hat{A}, f(\alpha)] = [\hat{A}, f^{(0)}(\alpha)], \end{aligned} \quad (17.5)$$

т. е. (17.4) справедливо при  $k = 1$ . При выводе (17.5) мы учитывали тот факт, что

$$\hat{A} e^{-\alpha \hat{A}} = e^{-\alpha \hat{A}} \hat{A}.$$

Для  $k + 1$  производной получим:

$$\begin{aligned} f^{(k+1)}(\alpha) &= \frac{\partial f^{(k)}(\alpha)}{\partial \alpha} = \\ &= \frac{\partial}{\partial \alpha} \left( \underbrace{[\hat{A}[\dots[\hat{A}, f^{(0)}(\alpha)]\dots]}_k \right) = \underbrace{[\hat{A}[\dots[\hat{A}, \frac{\partial}{\partial \alpha} f^{(0)}(\alpha)]\dots]}_k = \\ &= \underbrace{[\hat{A}[\dots[\hat{A}, f^{(1)}(\alpha)]\dots]}_k = \underbrace{[\hat{A}[\dots[\hat{A}, [\hat{A}, f^{(0)}(\alpha)]]\dots]}_k = \\ &= \underbrace{[\hat{A}[\dots[\hat{A}, f^{(0)}(\alpha)]\dots]}_{k+1}, \end{aligned}$$

что вместе с (17.5) доказывает справедливость (17.4).

С учетом того, что

$$f^{(0)}(\alpha) = \hat{B},$$

можно получить из (17.3) искомое тождество (17.1) при  $\alpha = 1$ . □

## 17.2 Гильбертово пространство

Гильбертово пространство это обобщение евклидова пространства допускающее бесконечную размерность.

**Определение 17.2.1** (Гильбертово пространство). TBD

### 17.2.1 Теорема Стоуна

**Теорема 17.2.1** (Стоун). TBD





## Глава 18

# Преобразование Фурье

### 18.1 Преобразование Фурье

В этом курсе мы будем использовать следующую форму записи для преобразования Фурье <sup>1</sup>

$$\tilde{x}(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} x(t) e^{i\omega t} dt, \quad (18.1)$$

при этом обратное преобразование Фурье выглядит следующим образом

$$x(t) = \int_{-\infty}^{\infty} \tilde{x}(\omega) e^{-i\omega t} d\omega, \quad (18.2)$$

Следующая таблица содержит важные формулы обращения

| Функция $x(t)$ | Образ $\tilde{x}(\omega)$ |
|----------------|---------------------------|
| 1              | $\delta(\omega)$          |
| $\delta(t)$    | $\frac{1}{2\pi}$          |

Таблица 18.1: Преобразование Фурье

Из табл. 18.1 следует важная формула (интегральное представление дельта-функции) [40]

$$\delta(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{i\omega t} dt \quad (18.3)$$

---

<sup>1</sup> Чаще всего используется следующее определение Фурье образа

$$\tilde{x}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x(t) e^{-i\omega t} dt.$$

Вместе с тем в соответствии с [41] существуют альтернативные определения отличающиеся знаком перед частотой и коэффициентом перед интегралом.

## 18.2 Дискретное преобразование Фурье

Преобразование Фурье играет важную роль в обработке цифровых сигналов, в частности для анализа периодических последовательностей.

### 18.2.1 Определение

**Определение 18.2.1.** Допустим имеется  $M$  отсчетов  $x_0, x_1, \dots, x_{M-1}$  тогда дискретное преобразование Фурье задается следующим соотношением

$$\tilde{X}_k = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} x_m e^{-\frac{2\pi i}{M} k \cdot m}, \quad (18.4)$$

которое так же записывается в виде

$$\{x_m\} \longleftrightarrow \{\tilde{X}_k\}.$$

Обратное преобразование Фурье может быть получено с помощью аналогичного соотношения

$$x_k = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} \tilde{X}_m e^{\frac{2\pi i}{M} k \cdot m},$$

На [рис. 18.1](#) приведен график некоторой периодической функции и ее преобразования Фурье.

Выражение (18.4) может быть также переписано в матричной форме

$$\vec{\tilde{X}} = \hat{F} \vec{x},$$

где

$$\vec{x} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{M-1} \end{pmatrix}, \quad \vec{\tilde{X}} = \begin{pmatrix} \tilde{X}_0 \\ \tilde{X}_1 \\ \vdots \\ \tilde{X}_{M-1} \end{pmatrix},$$

а матрица  $\hat{F}$  имеет вид

$$\hat{F} = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & e^{-i\omega} & e^{-2i\omega} & \dots & e^{-(M-1)i\omega} \\ 1 & e^{-2i\omega} & e^{-4i\omega} & \dots & e^{-2(M-1)i\omega} \\ 1 & e^{-3i\omega} & e^{-6i\omega} & \dots & e^{-3(M-1)i\omega} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{-(M-1)i\omega} & e^{-2(M-1)i\omega} & \dots & e^{-(M-1)(M-1)i\omega} \end{pmatrix}, \quad (18.5)$$

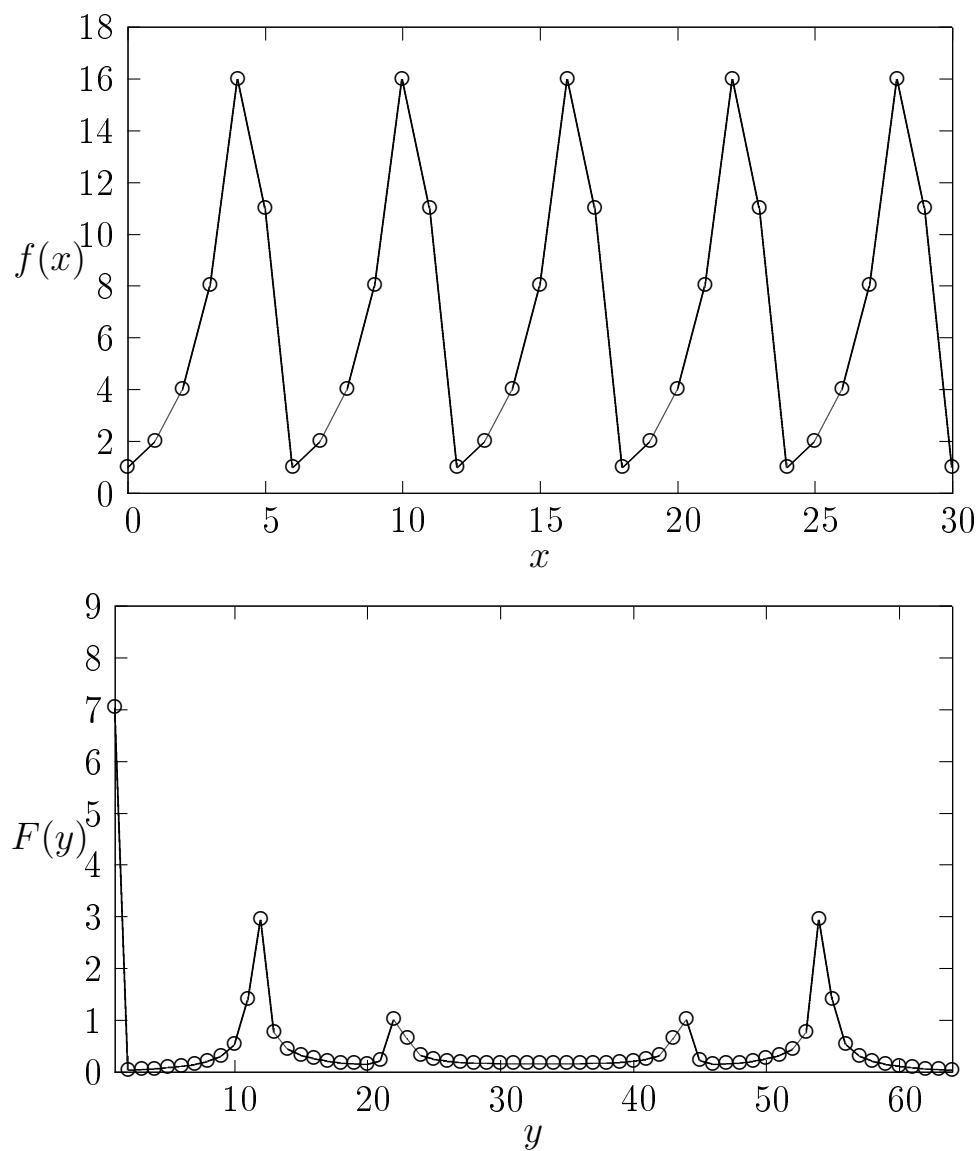


Рис. 18.1: Периодическая функция  $f(x, a) = a^x \bmod N$  при  $a = 2$ ,  $N = 21$  (верхний график) и ее дискретное преобразование Фурье (нижний график). Период исходной функции  $r = 6$ . Число отсчетов  $M = 64$ , видны локальные максимумы с периодом  $T \approx \frac{M}{r} \approx 10.67$

где

$$\omega = \frac{2\pi}{M}.$$

Для матричного элемента матрицы (18.5) можно записать

$$F_{nm} = \frac{1}{\sqrt{M}} e^{-i\omega nm}, \quad (18.6)$$

где  $n, m \in \{0, 1, \dots, M-1\}$ .

## 18.2.2 Свойства дискретного преобразования Фурье

Следует отметить следующие свойства преобразования Фурье, которые играют основную роль в алгоритме Шора:

**Лемма 18.2.1.** (Сдвиг) Если  $\{x_n\} \longleftrightarrow \{\tilde{X}_k\}$  то  $\{x_{(n-m) \bmod M}\} \longleftrightarrow \{e^{-i\omega mk} \tilde{X}_k\}$

*Доказательство.* Для последовательности  $\{x_{(n-m) \bmod M}\}$  можно записать

$$\{x_{(n-m) \bmod M}\} = \begin{pmatrix} x_{-m \bmod M} \\ x_{-m+1 \bmod M} \\ \vdots \\ x_{-1 \bmod M} \\ x_0 \\ x_1 \\ \vdots \\ x_{M-m-1} \end{pmatrix} = \begin{pmatrix} x_{M-m} \\ x_{M-m+1} \\ \vdots \\ x_{M-1} \\ x_0 \\ x_1 \\ \vdots \\ x_{M-m-1} \end{pmatrix},$$

при этом

$$\begin{aligned}
& \hat{F} \{x_{(n-m) \bmod M}\} = \\
& = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & e^{-i\omega} & e^{-2i\omega} & \dots & e^{-(M-1)i\omega} \\ 1 & e^{-2i\omega} & e^{-4i\omega} & \dots & e^{-2(M-1)i\omega} \\ 1 & e^{-3i\omega} & e^{-6i\omega} & \dots & e^{-3(M-1)i\omega} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{-(M-1)i\omega} & e^{-2(M-1)i\omega} & \dots & e^{-(M-1)(M-1)i\omega} \end{pmatrix} \begin{pmatrix} x_{M-m} \\ x_{M-m+1} \\ \vdots \\ x_0 \\ \vdots \\ x_{M-m-1} \end{pmatrix} = \\
& = \begin{pmatrix} \frac{x_{M-m}}{\sqrt{M}} + \frac{x_{M-m+1}}{\sqrt{M}} + \dots + \frac{x_0}{\sqrt{M}} + \dots + \frac{x_{M-m-1}}{\sqrt{M}} \\ \frac{x_{M-m}}{\sqrt{M}} + \frac{e^{-i\omega} x_{M-m+1}}{\sqrt{M}} + \dots + \frac{e^{-i\omega m} x_0}{\sqrt{M}} + \dots + \frac{e^{-i\omega(M-1)} x_{M-m-1}}{\sqrt{M}} \\ \frac{x_{M-m}}{\sqrt{M}} + \frac{e^{-2i\omega} x_{M-m+1}}{\sqrt{M}} + \dots + \frac{e^{-2i\omega m} x_0}{\sqrt{M}} + \dots + \frac{e^{-2i\omega(M-1)} x_{M-m-1}}{\sqrt{M}} \\ \vdots \\ \frac{x_{M-m}}{\sqrt{M}} + \frac{e^{-mi\omega} x_{M-m+1}}{\sqrt{M}} + \dots + \frac{e^{-mi\omega m} x_0}{\sqrt{M}} + \dots + \frac{e^{-mi\omega(M-1)} x_{M-m-1}}{\sqrt{M}} \\ \vdots \end{pmatrix}. \quad (18.7)
\end{aligned}$$

С учетом соотношения

$$e^{-i\omega k M} = 1, k \in \{0, 1, \dots\},$$

выражение (18.7) может быть переписано в следующем виде

$$\begin{aligned}
& \hat{F} \{x_{(n-m) \bmod M}\} = \\
& = \frac{1}{\sqrt{M}} \begin{pmatrix} x_{M-m} + \dots + x_{M-m-1} \\ e^{-i\omega m} e^{-i\omega(M-m)} x_{M-m} + \dots + e^{-i\omega 2m} e^{-i2\omega(M-m-1)} \\ e^{-i\omega 2m} e^{-i2\omega(M-m)} x_{M-m} + \dots + e^{-i\omega 2m} e^{-i2\omega(M-m-1)} \\ \vdots \end{pmatrix} = \\
& = \begin{pmatrix} \tilde{X}_0 \\ e^{-i\omega m} \tilde{X}_1 \\ e^{-i\omega 2m} \tilde{X}_2 \\ \vdots \end{pmatrix}.
\end{aligned}$$

□

**Лемма 18.2.2.** (Периодичность) Если последовательность  $\{x_n\}$  имеет период  $r$ :  $x_n = x_{n+r}$ , а число отсчетов  $M$  кратно  $r$ , то не нулевые члены преобразования Фурье следуют с периодом  $\frac{M}{r}$ .

*Доказательство.* Действительно если  $M \bmod r = 0$  и  $kr \bmod M \neq 0$ , то

$$1 - e^{-i\omega kr} \neq 0,$$

откуда

$$\begin{aligned} \tilde{X}_k &= \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} e^{-i\omega kn} x_n = \\ &= \frac{1}{\sqrt{M}} \left( \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega k(n+r)} x_{n+r} + \right. \\ &\quad \left. + \sum_{n=0}^{r-1} e^{-i\omega k(n+2r)} x_{n+2r} + \dots \right) = \\ &= \frac{1}{\sqrt{M}} \left( \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega k(n+r)} x_n + \sum_{n=0}^{r-1} e^{-i\omega k(n+2r)} x_n + \dots \right) = \\ &= \frac{1}{\sqrt{M}} \left( \sum_{n=0}^{r-1} x_n e^{-i\omega kn} \sum_{l=0}^{\frac{M}{r}-1} e^{-i\omega klr} = \sum_{n=0}^{r-1} x_n e^{-i\omega kn} \frac{1 - e^{-i\omega k \frac{M}{r} r}}{1 - e^{-i\omega kr}} \right) = \\ &= \frac{1}{\sqrt{M}} \frac{1 - e^{-i\omega kM}}{1 - e^{-i\omega kr}} \sum_{n=0}^{r-1} x_n e^{-i\omega kn} = 0. \quad (18.8) \end{aligned}$$

Если  $M \bmod r = 0$  и  $kr \bmod M = 0$ , то

$$e^{-i\omega kr} = e^{-i\frac{2\pi}{M}kr} = 1,$$

откуда

$$\begin{aligned} \tilde{X}_k &= \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} e^{-i\omega kn} x_n = \\ &= \frac{1}{\sqrt{M}} \left( \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega kn} x_{n+r} + \sum_{n=0}^{r-1} e^{-i\omega kn} x_{n+2r} + \dots \right) = \\ &= \frac{1}{\sqrt{M}} \left( \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \dots \right) = \\ &= \frac{1}{\sqrt{M}} \frac{M}{r} \sum_{n=0}^{r-1} e^{-i\omega kn} x_n \neq 0. \quad (18.9) \end{aligned}$$

Таким образом из выражений (18.8) и (18.9) следует что ненулевые члены следуют с периодом  $T = \frac{M}{r}$ .  $\square$

**Комментарий 18.2.1.** (Периодичность максимумов) Стоит отметить, что выражение (18.8) (в случае когда период не кратен числу отсчетов:  $M \bmod r \neq 0$ ) будет приближенно равно 0 для тех значений  $k$  которые сильно отличаются от значений кратных  $\frac{M}{r}$ , т. е. локальные максимумы преобразования Фурье будут повторяться с периодом  $\frac{M}{r}$ .

### 18.2.3 Быстрое преобразование Фурье

Вычисления по формуле (18.4) имеют сложность порядка  $O(M^2)$ , где  $M$  - число элементов (отсчетов)<sup>2</sup>.

Существует алгоритм быстрого расчета по формуле (18.4) который имеет сложность  $O(M \log M)$ .

Воспользовавшись парадигмой “разделяй и властвуй” (см. разд. 20.2) можно обратить внимание на форму записи (18.6) и заметить, что выражение (18.4) может быть переписано в виде

$$\tilde{X}_k = \sum_{m=0}^{M-1} F_{km}^M x_m,$$

где запись  $F_{km}^M$  обозначает, что используется матрица (18.6) размера  $M \times M$ . Если  $M$  чётно, то

$$\tilde{X}_k = \sum_{m=0}^{M-1} F_{k,m}^M x_m = \sum_{m=0}^{\frac{M}{2}-1} F_{k,2m}^M x_{2m} + \sum_{m=0}^{\frac{M}{2}-1} F_{k,2m+1}^M x_{2m+1},$$

где

$$F_{k,2m}^M = e^{-i\omega k 2m} = e^{-ikm \frac{2\pi}{M}} = F_{k,m}^{\frac{M}{2}},$$

$$F_{k,2m+1}^M = e^{-i\omega k (2m+1)} = e^{-i\omega k} e^{-ikm \frac{2\pi}{M}} = e^{-2\pi i \frac{k}{M}} F_{k,m}^{\frac{M}{2}},$$

т. е.

$$\tilde{X}_k = \sum_{m=0}^{\frac{M}{2}-1} F_{k,m}^{\frac{M}{2}} x_{2m} + \exp\left\{\left(-2\pi i \frac{k}{M}\right)\right\} \sum_{m=0}^{\frac{M}{2}-1} F_{k,m}^{\frac{M}{2}} x_{2m+1}. \quad (18.10)$$

Сложность вычислений по формуле (18.10) определяется следующим соотношением

$$T(M) = 2T\left(\frac{M}{2}\right) + O(M). \quad (18.11)$$

---

<sup>2</sup> Действительно необходимо получить  $M$  элементов, для подсчета каждого из которых требуется  $M$  операций умножения

В справедливости (18.11) можно убедиться если заметить что вычисления сложности  $T(M)$  в (18.10) распадаются на две подзадачи по вычислениям сложности  $T(\frac{M}{2})$ .

Используя основную теорему о рекуррентных соотношениях (случай 2) (Теорема 20.1.1) получаем

$$T(M) = O(M \log M).$$

## 18.3 Двумерное преобразование Фурье

### 18.3.1 Определение

**Определение 18.3.1** (Двумерное преобразование Фурье). Допустим у нас имеется двумерный сигнал  $x(k_1, k_2)$ , где  $k_1, k_2 \in \{0, \dots, M-1\}$ . Двумерным преобразованием Фурье называется двумерная функция

$$\tilde{X}(j_1, j_2), j_1, j_2 \in \{0, \dots, M-1\}$$

такая, что

$$\tilde{X}(j_1, j_2) = \frac{1}{M} \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1} x(k_1, k_2) e^{-i\omega(k_1 j_1 + k_2 j_2)},$$

где

$$\omega = \frac{2\pi}{M}.$$



## Глава 19

# Дискретная математика

### 19.1 Наибольший общий делитель. Алгоритм Евклида

**Определение 19.1.1.** Наибольшим общим делителем чисел  $a$  и  $b$  ( $\text{НОД}(a, b)$ ) называется максимальный из их общих делителей.

**Теорема 19.1.1** (Теорема об общих делителях). *Допустим, что выполняются следующие неравенства  $a > b > 0$ , а число  $r$  является остатком от деления  $a$  на  $b$ . Т. о. можно записать*

$$a = x \cdot b + r, \quad (19.1)$$

где  $x \geq 1$ ,  $b > r \geq 0$ . Если  $r = 0$ , то  $b$  является максимальным числом на которое делятся без остатка и  $a$  и  $b$ . В случае, если  $r > 0$ , то

$$\text{НОД}(a, b) = \text{НОД}(b, r). \quad (19.2)$$

*Доказательство.* Для доказательства (19.2) покажем, что любой делитель пары чисел  $(a, b)$  является делителем пары чисел  $(b, r)$ . Пусть  $d$  некоторый общий делитель чисел  $a$  и  $b$ , т. е.  $a = d \cdot x_1$ ,  $b = d \cdot x_2$ . Т. о. из (19.1) следует

$$r = a - x \cdot b = d \cdot (x_1 - x \cdot x_2),$$

т. е.  $d$  является делителем числа  $r$ .

Теперь докажем, что любой общий делитель чисел  $b$  и  $r$  будет являться общим делителем чисел  $a$  и  $b$ , действительно пусть  $d$  - общий делитель чисел  $b$  и  $r$ , т. е.  $b = y_1 \cdot d$  и  $r = y_2 \cdot d$ , т. о. (19.1) переписывается в виде

$$a = x \cdot y_1 \cdot d + y_2 \cdot d = d \cdot (x \cdot y_1 + y_2),$$

т. е.  $d$  является делителем числа  $a$ .

Таким образом пары чисел  $(a, b)$  и  $(b, r)$  имеют общие делители, в том числе и максимальный делитель для одной пары будет являться таковым и для второй.  $\square$

Соотношение (19.2) приводит к следующему алгоритму вычисления наибольшего общего делителя

---

**Алгоритм 3** Алгоритм Евклида

---

```

 $a > b$ 
if  $b = 0$  then
    return  $a$ 
end if
 $a \Leftarrow 0$ 
 $r \Leftarrow b$ 
 $b \Leftarrow a$ 
repeat
     $a \Leftarrow b$ 
     $b \Leftarrow r$ 
     $r \Leftarrow$  остаток от деления  $a$  на  $b$ 
until  $(r \neq 0)$ 
return  $b$ 

```

---

Для оценки сложности алгоритма 3 запишем его в следующем виде

$$\begin{aligned}
 f_k &= x_k \cdot f_{k+1} + f_{k+2}, \\
 f_0 &= a, \quad f_1 = b, \\
 x_k &\geq 1, \quad f_k > f_{k+1} > f_{k+2},
 \end{aligned}$$

т. о.  $f_k > 2 \cdot f_{k+2}$ , или же  $f_0 > 2 \cdot f_2 > \dots > 2^n f_{2n}$  т. е. алгоритм остановится при  $n = \log_2(f_0) = \log_2(a)$ <sup>1</sup>. Число шагов алгоритма при этом очевидно равно  $2n$  или же  $2 \cdot \log_2(a)$ . Т. о. алгоритмическая сложность алгоритма Евклида может быть записана как  $O(\log(a))$ .

---

<sup>1</sup>Дальнейшие выкладки сделаны в предположении, что  $\log_2(a)$  - целое число

**Пример 19.1.1.** (НОД(2345, 1456))

$$\begin{aligned}
 2345 &= 1456 + 889, \\
 1456 &= 889 + 567, \\
 889 &= 567 + 322, \\
 567 &= 322 + 245, \\
 322 &= 245 + 77, \\
 245 &= 3 \cdot 77 + 14, \\
 77 &= 5 \cdot 14 + 7, \\
 14 &= 2 \cdot 7.
 \end{aligned}$$

*т. о. НОД(2345, 1456) = 7. Число шагов алгоритма  $8 < 2 \cdot \log_2 2345 \approx 2 \cdot 11.2 = 22.4$ .*

### 19.1.1 Соотношение Безу

**Теорема 19.1.2** (Безу). *Если числа  $a$  и  $b$  взаимно просты, то уравнение*

$$ax + by = 1$$

*имеет целочисленные решения.*

*Доказательство.* Используем алгоритм Евклида 3 для нахождения НОД( $a, b$ ). Допустим  $a > b$ , тогда

$$\begin{aligned}
 r_1 &= a - bq_0, \\
 r_2 &= b - r_1q_1 = b - (a - bq_0)q_1 = b(1 + q_1q_0) - aq_1, \\
 r_3 &= r_1 - r_2q_2 = a - bq_0 - (b(1 + q_1q_0) - aq_1)q_2 = \\
 &= a(1 + q_1q_2) - b(q_0 + q_2 + q_0q_1q_2), \\
 &\quad \dots \\
 \text{НОД}(a, b) &= r_n = r_{n-2} - r_{n-1}q_{n-1} = \dots = ax + by,
 \end{aligned} \tag{19.3}$$

что доказывает наше утверждение. □

**Комментарий 19.1.1** (О сложности вычисления соотношения Безу). *Вычисления по (19.3) эквивалентны шагам в алгоритме 3. Число этих шагов  $O(\log_2(a))$ , таким образом алгоритм описанный уравнениями (19.3) достаточно эффективный и имеет сложность  $O(\log_2(a))$ .*

**Пример 19.1.2** (Соотношение Безу). Допустим  $a = 25, b = 14$ . Формулы алгоритма Евклида имеют вид

$$\begin{aligned} 11 &= 25 - 14 \cdot 1, \\ 3 &= 14 - 11 \cdot 1, \\ 2 &= 11 - 3 \cdot 3, \\ 1 &= 3 - 2 \cdot 1. \end{aligned}$$

Из этих формул получаем

$$\begin{aligned} 11 &= 25 - 14 \cdot 1, \\ 3 &= 14 - 25 + 14 = 2 \cdot 14 - 25, \\ 2 &= 11 - 3 \cdot 3 = 25 - 14 - 3 \cdot (2 \cdot 14 - 25) = 4 \cdot 25 - 7 \cdot 14, \\ 1 &= 3 - 2 \cdot 1 = 9 \cdot 14 - 5 \cdot 25. \end{aligned}$$

Т. о.

$$25 \cdot (-5) + 14 \cdot 9 = 1.$$

## 19.2 Сравнение по модулю

**Определение 19.2.1.** Запись

$$a \equiv b \pmod{c} \tag{19.4}$$

означает, что  $a$  и  $b$  имеют одинаковые остатки при делении на  $c$  или  $a$  и  $b$  сравнимы по модулю натурального числа  $c$ . При этом число  $c$  называется модулем сравнения.

Определение 19.4 может также трактоваться как то, что разность  $a - b$  делится на  $c$ .

**Пример 19.2.1.** Сравнение по модулю  $30 \equiv 8 \pmod{11}$ , потому что,  $30 = 2 \cdot 11 + 8$ .

**Определение 19.2.2** (Отрицательный элемент). Если  $a < n$ , то  $n - a$  будет называться отрицательным по отношению к  $a$  элементом и обозначаться  $-a \pmod{n}$ .

**Пример 19.2.2.** Отрицательный элемент

$$-5 \equiv 6 \pmod{11},$$

поскольку  $5 < 11, 6 = 11 - 5$ .

### 19.2.1 Арифметические операции

**Лемма 19.2.1** (О сложении по модулю). *Если  $a_1 \equiv a_2 \pmod{n}$ ,  $b_1 \equiv b_2 \pmod{n}$ , то*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$$

*Доказательство.* Можно записать  $a_1 = k_1n + r_a$ ,  $a_2 = k_2n + r_a$ ,  $b_1 = l_1n + r_b$ ,  $b_2 = l_2n + r_b$  откуда

$$a_1 + b_1 = (k_1 + l_1)n + r_a + r_b \equiv r_a + r_b \pmod{n}$$

и

$$a_2 + b_2 = (k_2 + l_2)n + r_a + r_b \equiv r_a + r_b \pmod{n}$$

откуда

$$a_1 + b_1 \equiv a_2 + b_2 \equiv r_a + r_b \pmod{n}$$

□

**Лемма 19.2.2** (Об умножении по модулю). *Если  $a_1 \equiv a_2 \pmod{n}$ ,  $b_1 \equiv b_2 \pmod{n}$ , то*

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$$

*Доказательство.* Если  $a_1 \equiv a_2 \pmod{n}$ ,  $b_1 \equiv b_2 \pmod{n}$ , то

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$$

Можно записать  $a_1 = k_1n + r_a$ ,  $a_2 = k_2n + r_a$ ,  $b_1 = l_1n + r_b$ ,  $b_2 = l_2n + r_b$  откуда

$$a_1 \cdot b_1 = k_1l_1n + l_1nr_a + k_1nr_b + r_ar_b \equiv r_ar_b \pmod{n}$$

и

$$a_2 \cdot b_2 = k_2l_2n + l_2nr_a + k_2nr_b + r_ar_b \equiv r_ar_b \pmod{n}$$

откуда

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \equiv r_ar_b \pmod{n}$$

□

### 19.2.2 Решение уравнений

Очень часто в криптографии имеют дело с уравнениями вида

$$ax \equiv b \pmod{n}, \quad (19.5)$$

где  $a, b, n$  известные целые числа, а  $x$  неизвестный параметр, подлежащий определению.

Очевидно, что если мы найдем такое целое число  $a^{-1}$ , что

$$aa^{-1} \equiv 1 \pmod{n},$$

то

$$x \equiv ba^{-1} \pmod{n}.$$

Если  $\text{НОД}(a, n) = 1$ , то в соответствии с соотношением Безу (см. теорему Безу (Теорема 19.1.2))  $\exists x, y : ax + ny = 1$ , т.е.

$$x \equiv a^{-1} \pmod{n}.$$

При этом, в соответствии с комментарием 19.1.1,  $a^{-1}$ , и решение уравнения (19.5), может быть найдено достаточно эффективно.

### 19.2.3 Поле $\mathbb{F}_p$

Как мы видели в модульной арифметике можно складывать, вычитать, умножать и даже, если сравнение ведется по модулю простого числа, делить. При этом операции сложения и умножения коммутативны и удовлетворяют условию дистрибутивности. Таким образом остатки при делении образуют поле (см. определение 16.2.1) которое называется полем Галуа и обозначается через  $\mathbb{F}_p$ .

## 19.3 Функция Эйлера

### 19.3.1 Определение

**Определение 19.3.1** (Функция Эйлера). Функция Эйлера  $\phi(n)$  показывает сколько чисел  $k \in \{1, \dots, n-1\}$  взаимно просты с  $n$ , т.е.  $\text{НОД}(k, n) = 1$ .

**Пример 19.3.1** (Функция Эйлера). Если взять число  $n = 15$  то имеется 8 чисел взаимно простых с 15: 1, 2, 4, 7, 8, 11, 13, 14. Оставшиеся 7 чисел не являются взаимно простыми с  $n$  поскольку имеют наибольший общий делитель отличный от 1, например  $\text{НОД}(6, 15) = 3$ . Таким образом,  $\phi(15) = 8$ .

### 19.3.2 Свойства

**Свойство 19.3.1** (Функция Эйлера простого числа). Если  $p$  - простое число, то  $\phi(p) = p - 1$

*Доказательство.* Следует из определения 19.3.1. □

**Свойство 19.3.2** (Функция Эйлера произведения (обобщенная мультипликативность)). Если  $\text{НОД}(n, m) = 1$ , то  $\phi(n \cdot m) = \phi(n) \phi(m)$

*Доказательство.* TBD □

**Комментарий 19.3.1** (О сложности вычисления функции Эйлера). Вычисление функции Эйлера больших чисел является очень сложной задачей. Чаще всего для вычисления используется свойство 19.3.1 в комбинации с 19.3.2. Применений этих свойств для произвольного числа требует его факторизации, поэтому сложность вычисления функции Эйлера сравнима со сложностью задачи факторизации.

## 19.4 Малая теорема Ферма

**Теорема 19.4.1** (Малая теорема Ферма). Если  $p$  простое число, и  $a$  не делится на  $p$ , то

$$a^{p-1} \equiv 1 \pmod{p} \quad (19.6)$$

*Доказательство.* Рассмотрим следующее соотношение

$$a \cdot k_i \pmod{p},$$

где  $k_i \in \{1, \dots, p-1\}$ .

Очевидно, что

$$a \cdot k_i \equiv k_j \pmod{p}. \quad (19.7)$$

Действительно

$$a \cdot k_i \pmod{p} \subset \{1, \dots, p-1\},$$

т. к. любой остаток от деления на  $p$  принимает значения  $0, 1, \dots, p-1$ . Нулевой остаток невозможен т. к.  $a$  и  $p$  взаимно просты.

Кроме этого каждый из остатков  $a \cdot k_i \pmod{p}$  встречается только один раз, действительно допустим что  $a \cdot k_i \pmod{p} = a \cdot k_j \pmod{p}$  или же  $a \cdot (k_i - k_j) \equiv 0 \pmod{p}$ , т. е.  $a$  делится на  $p$ , что противоречит условию взаимной простоты.

Перемножив все выражения [выр. 19.7](#) получим

$$a \cdot 2a \cdot 3a \cdot \dots \cdot a(p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}.$$

или же

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p},$$

откуда получаем требуемое равенство в силу взаимной простоты  $p$  и  $(p-1)!$ :

$$a^{p-1} \equiv 1 \pmod{p}$$

□

### 19.4.1 Псевдопростые числа

Обобщение малой теоремы Ферма не верно, т. е. если  $a$  и  $p$  взаимно простые числа которые удовлетворяют соотношению [выр. 19.6](#) то  $p$  может быть не простым. Например

$$2^{341-1} \equiv 1 \pmod{341},$$

при том, что  $341 = 11 \cdot 31$ .

Числа  $p$  удовлетворяющие соотношению [выр. 19.6](#), но при этом не являющиеся простыми называется псевдопростыми числами по основанию  $a$ . Например 341 - первое псевдопростое число по основанию 2.

## 19.5 Китайская теорема об остатках

**Теорема 19.5.1.** *Если имеются взаимно простые целые числа  $n_1, n_2, \dots, n_k$ , тогда для любого набора целых чисел  $a_1, a_2, \dots, a_k$   $\exists x$  такой что*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}, \end{aligned} \tag{19.8}$$

*При этом для любых  $x_1, x_2$  удовлетворяющих этому соотношению имеет место равенство*

$$x_1 \equiv x_2 \pmod{N},$$

*где  $N = n_1 \cdot n_2 \cdot \dots \cdot n_k$ .*

## 19.6 Алгоритм RSA

Алгоритм RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) - несимметричный алгоритм шифрования <sup>2</sup>, основанный на сложности разложения числа на простые множители.

### 19.6.1 Генерация ключей

Состоит из нескольких шагов

- Выбираются два простых числа  $p$  и  $q$

---

<sup>2</sup>Несимметричным (с открытым ключом) называется такой алгоритм шифрования, в котором используются два различных ключа: один для шифрования, а второй для де-шифрования



- Вычисляется произведение выбранных простых чисел  $n = p \cdot q$
- Вычисляется функция Эйлера (19.3.1) (см. свойства 19.3.1 и 19.3.2)  
 $\phi(n) = (p - 1)(q - 1)$
- Выбирается целое число  $e$  такое что  $1 < e < \phi(n)$  и  $e$  и  $\phi(n)$  взаимно просты, т. е.  $\text{НОД}(e, \phi(n)) = 1$ .
- вычисляем  $d \equiv e^{-1} \pmod{\phi(n)}$ , т. е.  $d \cdot e \equiv 1 \pmod{\phi(n)}$ .

Открытый ключ состоит из двух чисел: модуля  $n$  и открытой экспоненты  $e$ . Именно эти два числа используются для шифрования исходного сообщения.

Закрытый ключ состоит тоже из двух чисел: модуля  $n$  и закрытой экспоненты  $d$ .

Исходные числа  $p$  и  $q$  держатся в секрете, так как с их помощью вычисление  $\phi(n)$  становится тривиальным.

При этом стоит отметить, что для получения закрытого ключа по открытому необходимо вычислить  $\phi(n)$  при известном  $n$ . Эта задача является сложной (если не известны  $p$  и  $q$ ), как это отмечено в комментарии 19.3.1.

**Пример 19.6.1.** (RSA. Генерация ключей) *Выбираем два простых числа  $p = 3$  и  $q = 7$ . Произведение этих чисел  $n = 21$ . Функция Эйлера (19.3.1)  $\phi(n) = (p - 1)(q - 1) = 2 \cdot 6 = 12$ .*

*Выбираем число  $e$  (открытая экспонента), таким образом, что  $1 < e < 12$  и  $\text{НОД}(e, 12) = 1$ . Очевидно  $e = 5$  удовлетворяет заявленным условиям.*

*Вычисляем закрытую экспоненту  $d \equiv 5^{-1} \pmod{12}$ , т. е.  $d = 5$ . Действительно  $5 \cdot 5 = 25 = 2 \cdot 12 + 1$ , т. е.  $5 \cdot 5 \equiv 1 \pmod{12}$ .*

*Т. о. получаем*

- Открытый ключ ( $n = 21, e = 5$ )
- Закрытый ключ ( $n = 21, d = 5$ )

## 19.6.2 Шифрование

Допустим надо зашифровать некоторое сообщение  $M$ . Вначале оно переводится в целое число(числа)  $m$  такое, что  $0 < m < \phi(n)$ . Далее вычисляется за зашифрованный текст  $c$ :

$$c \equiv m^e \pmod{n} \quad (19.9)$$

**Пример 19.6.2.** (RSA. Шифрование) Допустим у нас есть открытый ключ  $(n = 21, e = 5)$  (см. прим. 19.6.1) и мы хотим зашифровать следующее сообщение  $m = 1101_2 = 11_{10}$ . Шифротекст вычисляется по формуле (19.9)  $c \equiv 11^5 \pmod{21} = 2$ .

### 19.6.3 Де-шифрование

$m$  может быть восстановлено из  $c$  по следующей формуле:

$$m \equiv c^d \pmod{n}. \quad (19.10)$$

Имея  $m$  можно восстановить исходное сообщение  $M$ .

**Пример 19.6.3.** (RSA. Де-шифрование) Допустим у нас есть закрытый ключ  $(n = 21, d = 5)$  (см. прим. 19.6.1) и шифротекст  $c = 2$  из примера 19.6.2.

Исходный текст вычисляется по формуле (19.10)  $m \equiv 2^5 \pmod{21} = 11 = 1101_2$ .

### 19.6.4 Доказательство

Хотим доказать что

$$(m^e)^d \equiv m \pmod{p \cdot q}$$

для любых положительных чисел  $m$  когда  $p$  и  $q$  простые числа, а  $e$  и  $d$  удовлетворяют выражению

$$d \cdot e \equiv 1 \pmod{\phi(p \cdot q)},$$

которое мы можем переписать в виде

$$d \cdot e - 1 = h(p-1)(q-1).$$

Таким образом

$$m^{e \cdot d} = m m^{h(p-1)(q-1)}.$$

Далее возможны два случая: когда  $m$  делится на  $p$  и когда  $m$  и  $p$  взаимно просты.

В первом случае

$$m^{e \cdot d} \equiv m \equiv 0 \pmod{p}$$

Во втором случае используем малую теорему Ферма (Теорема 19.4.1) :

$$m m^{h(p-1)(q-1)} = m (m^{p-1})^{h(q-1)} \equiv m \cdot 1^{h(q-1)} \equiv m \pmod{p}.$$

Аналогично имеем либо

$$m^{e \cdot d} \equiv m \equiv 0 \pmod{q}$$

либо в силу малой теоремы Ферма

$$mm^{h(p-1)(q-1)} = m(m^{q-1})^{h(p-1)} \equiv m \cdot 1^{h(p-1)} \equiv m \pmod{q}.$$

Таким образом мы имеем следующие два типа соотношений: тривиальное равенство

$$\begin{aligned} x_1 &= m \equiv m \pmod{p}, \\ x_1 &= m \equiv m \pmod{q}, \end{aligned}$$

и только, что полученные соотношения

$$\begin{aligned} x_2 &= m^{ed} \equiv m \pmod{p}, \\ x_2 &= m^{ed} \equiv m \pmod{q}, \end{aligned}$$

откуда в силу китайской теоремы об остатках ([Теорема 19.5.1](#))

$$x_1 \equiv x_2 \pmod{p \cdot q}$$

т.е.

$$m^{e \cdot d} \equiv m \pmod{n}$$

## 19.7 Дискретный логарифм

**Определение 19.7.1** (Дискретный логарифм). Рассмотрим некоторую абелеву мультипликативную группу  $G$  и уравнение

$$g^x = a \tag{19.11}$$

Решение этого уравнения, т.е. целое неотрицательное число  $x$  удовлетворяющее равенству ([19.11](#)) называется дискретным логарифмом.

Уравнение ([19.11](#)) в общем случае имеет решение не для любых значений  $a$ . Но в том случае, если  $g$  - порождающий элемент  $G$ , т.е.  $G = \langle g \rangle$ , то решение всегда существует и оно единственно. В дальнейшем говоря о дискретном логарифме мы будем предполагать, что  $g$  выбрано таким образом, что  $G = \langle g \rangle$ .

В прикладной криптографии часто имеют дело с особой разновидностью дискретного логарифма в кольце вычетов по модулю  $p$ :

**Определение 19.7.2** (Дискретный логарифм в кольце вычетов по модулю  $p$ ). Дискретным логарифмом  $\text{ind}_g(a) \bmod p$ <sup>3</sup> называется минимальное число  $x$ , которое удовлетворяет следующему уравнению (если такое число существует):

$$g^x \equiv a \pmod{p} \quad (19.12)$$

**Пример 19.7.1.** ( $\text{ind}_3 14 \bmod 17$ ) Решим задачу методом перебора [25]:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{17}, 3^2 \equiv 9 \pmod{17}, 3^3 \equiv 10 \pmod{17}, 3^4 \equiv 13 \pmod{17}, \\ 3^5 &\equiv 5 \pmod{17}, 3^6 \equiv 15 \pmod{17}, 3^7 \equiv 11 \pmod{17}, 3^8 \equiv 16 \pmod{17}, \\ 3^9 &\equiv 14 \pmod{17}, 3^{10} \equiv 8 \pmod{17}, 3^{11} \equiv 7 \pmod{17}, 3^{12} \equiv 4 \pmod{17}, \\ 3^{13} &\equiv 12 \pmod{17}, 3^{14} \equiv 2 \pmod{17}, 3^{15} \equiv 6 \pmod{17}, 3^{16} \equiv 1 \pmod{17}, \end{aligned}$$

т. о. можно видеть, что  $\text{ind}_3 14 \bmod 17 = 9$ , т. к.  $3^9 \equiv 14 \pmod{17}$ .

Задача о нахождении дискретного логарифма является сложной задачей. Самый быстрый из известных алгоритмов [8] решает ее за время порядка  $O\left(c \cdot \exp\left(\log p^{\frac{1}{3}} \log \log p^{\frac{2}{3}}\right)\right)$ , где  $c$  - некоторая константа, что обуславливает широкое применение алгоритмов использующих дискретный логарифм в криптографии.

## 19.8 Протокол Диффи-Хеллмана (Diffie-Hellman, DH)

Предположим существуют два абонента Алиса и Боб. Им известны два числа  $g$  и  $p$ , которые не являются секретными.

Алиса выбирает случайное число  $a$  и пересылает Бобу следующее значение

$$A \equiv g^a \pmod{p}. \quad (19.13)$$

Боб вычисляет следующее число (с помощью секретной случайной величины  $b$ )

$$B \equiv g^b \pmod{p}. \quad (19.14)$$

Алиса, с помощью только ей известного числа  $a$  вычисляет ключ

$$K \equiv B^a \pmod{p} \equiv g^{ab} \pmod{p}. \quad (19.15)$$

Боб может получить то же самое значение ключа с помощью своего секретного числа  $b$ :

$$K \equiv A^b \pmod{p} \equiv g^{ab} \pmod{p}. \quad (19.16)$$

---

<sup>3</sup>От слова **index** - альтернативного названия для дискретного логарифма

Таким образом Алиса и Боб получают один и тот же ключ, который в дальнейшем может быть использован для передачи сообщения с помощью симметричных алгоритмов шифрования (например AES).

**Пример 19.8.1.** (Диффи-Хеллман) *Исходные данные (открытая информация):  $g = 2$ ,  $p = 23$ . Алиса выбирает случайное число  $a = 6$  и вычисляет по формуле (19.13) число  $A = 18$  и отправляет его Бобу. Боб выбирает случайное число  $b = 9$  и, с помощью формулы (19.14), получает  $B = 6$  и отправляет и отправляет это число Алисе.*

*Алиса вычисляет ключ  $K = 12$  по формуле (19.15). Боб может получить тоже значение ключа  $K = 12$  используя (19.16)*

Злоумышленнику Еве известны числа  $g$ ,  $p$ ,  $A$  и  $B$ . Для получения ключа  $K$  Еве необходимо получить одно из секретных чисел  $a$  или  $b$ :

$$a \equiv \text{ind}_g(A) \pmod{p},$$

откуда с помощью (19.15) получается искомое значение  $K$ .

## 19.9 Схема Эль-Гамала (Elgamal)

Одной из вариаций протокола Диффи-Хелмана является схема Эль Гамала. Следует различать алгоритм шифрования и алгоритм цифровой подписи Эль-Гамала. Цифровая подпись Эль-Гамала лежит в основе стандартов цифровой подписи США (DSA) и России (ГОСТ Р 34.10-94).

Ниже мы рассмотрим алгоритм в режиме шифрования.

### 19.9.1 Генерация ключей

- Генерируется простое число  $p$ .
- Выбирается целое число  $g$
- Выбирается случайное целое число  $x : 1 < x < p$ .
- Вычисляется  $y = g^x \pmod{p}$

Открытым ключом является тройка  $p, g, y$ . Закрытым ключом является число  $x$ .

**Пример 19.9.1** (Генерация ключей (Elgamal)). *Выбираем  $p = 21$ ,  $g = 10$ ,  $x = 3$ .  $y = 10^3 \pmod{21} = 13$ .*

### 19.9.2 Шифрование

Шифруемое сообщение  $M$  должно удовлетворять критерию  $0 < M < p$ .

- Выбирается сессионный ключ - случайное число  $k : 1 < k < p - 1$ .
- Вычисляется  $a = g^k \mod p$
- Вычисляется  $b = y^k M \mod p$

Пара чисел  $(a, b)$  считается шифротекстом.

**Пример 19.9.2** (Шифрование (Elgamal)). Допустим мы хотим зашифровать  $M = 6$ . Выбираем  $k = 7$ .  $a = 10^7 \mod 21 = 10$ ,  $b = 13^7 \cdot 6 \mod 21 = 15$ .

### 19.9.3 Дешифрование

Зная закрытый ключ  $x$  мы можем восстановить исходное сообщение с помощью

$$M = b \cdot (a^x)^{-1} \mod p, \quad (19.17)$$

действительно в силу того что

$$(a^x)^{-1} = g^{-kx} \mod p$$

имеем

$$b \cdot (a^x)^{-1} = y^k M g^{-kx} = g^{kx} M g^{-kx} = M \mod p.$$

**Пример 19.9.3** (Дешифрование (Elgamal)). Зашифрованное сообщение из прим. 19.9.3  $C = (a = 10, b = 15)$ . Используя (19.17) имеем

$$M = 15 \cdot 13 \mod 21 = 6$$

где было использовано

$$(10^3)^{-1} \equiv 13 \mod 21,$$

т.к.  $13 \cdot 10^3 = 1 \mod 21$ . Таким образом мы восстановили зашифрованное в прим. 19.9.3 сообщение  $M = 6$ .

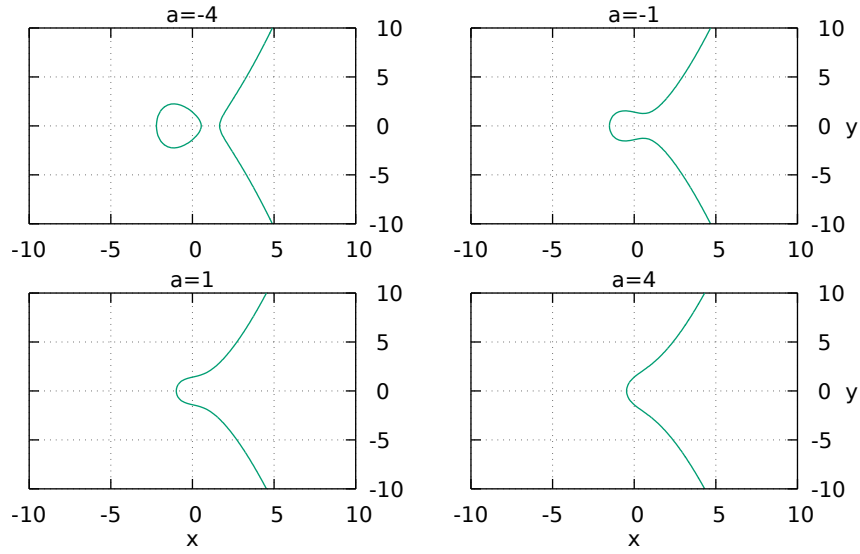


Рис. 19.1: Эллиптическая кривая  $y^2 = x^3 + ax + 2$  над полем вещественных чисел  $\mathbb{R}$  при различных значениях параметра  $a$

## 19.10 Эллиптическая криптография

### 19.10.1 Эллиптические кривые над полем $\mathbb{R}$

В эллиптической криптографии рассматривают определенные наборы объектов которые образуют группу (см. [разд. 16.1](#)). В качестве такого набора мы будем рассматривать точки принадлежащие некоторой кривой (см. [рис. 19.1](#)):

$$E : y^2 = x^3 + ax + b,$$

где коэффициенты  $a, b$  должны удовлетворять следующему соотношению

$$4a^3 + 27b^2 \neq 0,$$

в этом случае кубическое уравнение  $x^3 + ax + b = 0$  будет иметь 3 различных действительных корня [\[24\]](#).

В соответствии с определением [16.1.1](#) для точек на кривой задана некоторая бинарная операция которая двум точкам  $p, q$  с координатами  $(p_x, p_y)$  и  $(q_x, q_y)$ , соответственно, сопоставляет третью точку  $r$  с координатами  $(r_x, r_y)$ , данную операцию мы будем называть сложением:

$$p + q = r.$$

Существует простая геометрическая интерпретация операции сложения (см. [рис. 19.2](#)). Допустим имеется 2 точки на кривой которые мы хотим сложить:

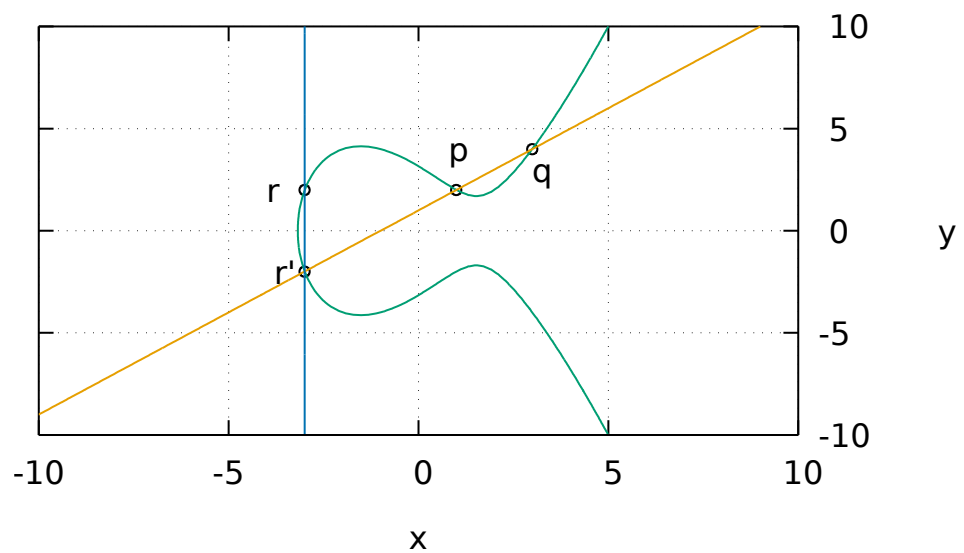


Рис. 19.2: Эллиптическая кривая  $y^2 = x^3 - 7x + 10$  над полем вещественных чисел  $\mathbb{R}$ . Сложение двух точек  $p(1, 2)$  и  $q(3, 4)$ . Прямая проходящая через эти точки пересекает кривую еще в третьей точке  $r'(-3, -2)$ . Симметричная  $r'$  относительно кривой точка  $r(-3, 2)$  является суммой исходных двух:  $p+q = r$



$p$  и  $q$  с координатами  $(x_p, y_p), (x_q, y_q)$  соответственно. Если  $x_p \neq x_q$ , то через эти точки можно провести прямую, которая имеет наклон

$$m = \frac{y_p - y_q}{x_p - x_q}.$$

и пересекает кривую в точке  $r'$ . Если эта точка имеет координаты  $(x_{r'}, y_{r'})$ , то в силу того, что она лежит на прямой с наклоном  $m$ :

$$m = \frac{y_{r'} - y_p}{x_{r'} - x_p},$$

следовательно

$$y_{r'} = y_p + m(x_{r'} - x_p).$$

Эта точка должна принадлежать кривой, т.е.

$$y_{r'}^2 = (y_p + m(x_{r'} - x_p))^2 = x_{r'}^3 + ax_{r'} + b$$

которое можно переписать

$$x_{r'}^3 - m^2 x_{r'}^2 + \dots = 0.$$

Уравнение  $x^3 - m^2 x^2 + \dots = 0$  имеет 3 корня:  $x_p, x_q, x_{r'}$ , т.е. его можно также переписать в виде

$$(x - x_{r'})(x - x_p)(x - x_q) = x^3 - (x_{r'} + x_p + x_q)x^2 + \dots = 0.$$

Т.о.

$$x_{r'} + x_p + x_q = m^2.$$

Следовательно

$$\begin{aligned} x_{r'} &= m^2 - x_p - x_q, \\ y_{r'} &= y_p + m(x_{r'} - x_p), \end{aligned}$$

Отразив эту точку относительно оси  $X$  мы получим финальную точку  $r$  которую будем называть суммой исходных точек (см. [рис. 19.2](#)). Координаты этой точки  $x_r, y_r$  могут быть получены по следующим формулам

$$\begin{aligned} x_r &= m^2 - x_p - x_q, \\ y_r &= -y_p + m(x_p - x_r). \end{aligned} \tag{19.18}$$

В случае  $x_p = x_q$  возможны два варианта:

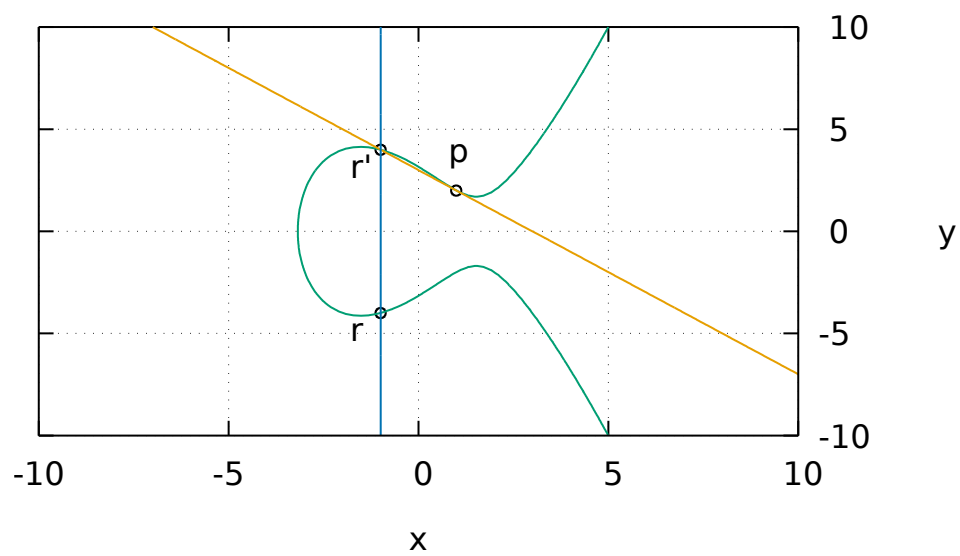


Рис. 19.3: Эллиптическая кривая  $y^2 = x^3 - 7x + 10$  над полем вещественных чисел  $\mathbb{R}$ . Сложение двух точек с одинаковыми координатами  $p(1, 2)$ :  $2p = r(-1, -4)$



Рис. 19.4: Эллиптическая кривая  $y^2 = x^3 - 7x + 10$  над полем вещественных чисел  $\mathbb{R}$ . Сложение двух точек  $p(1, 2)$  и  $q(1, -2)$ . Прямая проходящая через эти точки не пересекает кривую. Результат сложения - нулевой элемент:  $p + q = 0$ , т.е.  $q = -p$

1.  $y_p = y_q$  (см. рис. 19.3). В случае когда точки на кривой приближаются друг к другу, прямая линия, проведенная через них, стремиться к касательной. Коэффициент  $m$  может быть найден по следующей формуле:  $m = \frac{dy}{dx}$ . С учетом  $2ydy = 3x^2dx + adx$  имеем  $m = \frac{dy}{dx} = \frac{3x^2+a}{2y}$ . дальнейший расчет ведется по формулам (19.18).
2.  $y_p \neq y_q$  (см. рис. 19.4). В этом случае, в силу симметрии кривой относительно оси  $X$  возможен только один вариант:  $y_p = y_q$  и кривая проходящая через эти две точки не пересекает кривую в третьей точке. Для этого случая вводят еще одну точку  $0$  в которую уходит прямая линия проведенная через две точки. Таким образом, в этом случае мы имеем  $p + q = 0, q = -p$ .

Таким образом мы можем определить эллиптическую кривую над полем вещественных чисел  $\mathbb{R}$  как следующее множество точек

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b, \} \cup \{0\}. \quad (19.19)$$

где  $a, b \in \mathbb{R}$ .

Для данных точек определена бинарная операция, которую мы называли сложением. На множестве есть нулевой элемент, так же для каждого элемента можно определить обратный элемент. Можно доказать, что введенная операция является ассоциативной:  $(a + b) + c = a + (b + c)$  [24]. Таким образом множество  $E(\mathbb{R})$  образует группу относительно операции сложения. С учетом очевидного равенства  $p + q = q + p$ , данная группа будет являться коммутативной, т.е. Абелевой (см. определение 16.1.3).

**Комментарий 19.10.1** (Об операции сложения). Введенная операция сложения для точек на эллиптической кривой выглядит на первый взгляд неестественно, почему бы не использовать более очевидные операции сложения точек на плоскости, например правила сложения векторов. В этом случае, если  $p, q \in E(\mathbb{R})$ , то вполне может быть что  $p + q \notin E(\mathbb{R})$  и, следовательно, будет нарушено основное свойство группы - связанность (closure). Вместе с тем для определенной нами бинарной операции (19.18) справедливы все свойства групп, и соответственно, все вытекающие из этого свойства, такие например как теорема Лагранжа (см. теор. 16.1.2), которые могут быть применены к введенным нам объектам.

## 19.10.2 Эллиптические кривые над полем $\mathbb{F}_p$

Множество (19.19) вместе с операцией сложения (19.18) может определено над произвольным полем (см. определение 16.2.1), т.е. не только над



Рис. 19.5: Эллиптическая кривая  $y^2 = x^3 - 7x + 10$  над полем  $\mathbb{F}_{19}$

$\mathbb{R}$ . С точки зрения криптографии особый интерес представляет поле  $\mathbb{F}_p$  (см. [разд. 19.2.3](#)). Можно определить множество элементов эллиптической кривой над полем  $\mathbb{F}_p$  аналогично выражению (19.2.3):

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 \equiv x^3 + ax + b, \} \cup \{0\}. \quad (19.20)$$

где  $a, b \in \mathbb{F}_p$ .

На [рис. 19.5](#) изображено такое множество для поля  $\mathbb{F}_{19}$ , т.е.  $p = 19$ . Уравнение кривой  $y^2 \equiv x^3 - 7x + 10 \pmod{19}$ .

Для каждой точки  $a$  с координатами  $x_a, y_a$  определен обратный элемент  $-a$  с координатами  $x_{-a} = x_a, y_{-a} \equiv -y_a \pmod{p}$ .

Для точек на данной кривой задан следующий закон сложения  $a + b = c, b \neq -a$

$$\begin{aligned} x_c &\equiv m^2 - x_a - x_b \pmod{p}, \\ y_c &\equiv -y_a + m(x_a - x_c) \pmod{p}, \end{aligned} \quad (19.21)$$

где  $(x_{a,b,c}, y_{a,b,c})$  - координаты точек  $a, b$  и  $c$  соответственно. Для коэффициента  $m$  используются следующие соотношения:

$$\begin{aligned} m &= (y_a - y_b)(x_a - x_b)^{-1} \pmod{p}, \text{ если } x_a \neq x_b \\ m &= (3x_a^2 + a)(2y_a)^{-1} \pmod{p}, \text{ если } x_a = x_b. \end{aligned}$$

Очевидно что если  $b = -a$ , то  $a + b = a + (-a) = 0$ .

### 19.10.3 Скалярное умножение и дискретный логарифм

Допустим  $n$  некоторое натуральное число  $n \in \mathbb{N}$  и  $a \in E(\mathbb{F}_p)$ . Определим скалярное произведение следующим образом

$$n \cdot a = a + a + \dots a = \sum_{k=1}^n a$$

Наивная реализация требует  $O(n)$  операций сложения, но с помощью парадигмы “разделяй и властвуй” (см. [разд. 20.2](#)) может быть сведено к  $O(\log n)$  операций сложения.

**Пример 19.10.1** (Скалярное произведение). Рассмотрим эллиптическую кривую

$$E(\mathbb{F}_{19}) = \{(x, y) \in \mathbb{F}_{19} \times \mathbb{F}_{19} : y^2 \equiv x^3 - 7x + 10\} \cup \{0\},$$

изображенную на [рис. 19.5](#). Выберем в качестве точки  $p = (13, 8)$ , тогда

$$\begin{aligned} 0 \cdot p &= 0, \\ 1 \cdot p &= p = (13, 8), \\ 2 \cdot p &= p + p = (16, 7), \\ 3 \cdot p &= 2 \cdot p + p = (18, 5), \\ 4 \cdot p &= 3 \cdot p + p = (12, 1), \\ 5 \cdot p &= 4 \cdot p + p = (5, 10), \\ 6 \cdot p &= 5 \cdot p + p = (7, 0), \\ 7 \cdot p &= 6 \cdot p + p = (5, 9), \\ 8 \cdot p &= 7 \cdot p + p = (12, 18), \\ 9 \cdot p &= 8 \cdot p + p = (18, 4), \\ 10 \cdot p &= 9 \cdot p + p = (16, 2), \\ 11 \cdot p &= 10 \cdot p + p = (13, 11), \\ 12 \cdot p &= 11 \cdot p + p = 0 \end{aligned}$$

Как видно из прим. [19.10.1](#) каждый элемент эллиптической кривой является генератором некоторой циклической подгруппы. Вместе с тем вся группа точек на эллиптической кривой не обязательно является циклической (TBD). С другой стороны для формирования задачи дискретного логарифма нам требуется именно циклическая группа. Таким образом для заданной эллиптической кривой вначале вычисляют ее порядок, для этого существует эффективный алгоритм Шуфа [\[18\]](#). После этого находится простой делитель

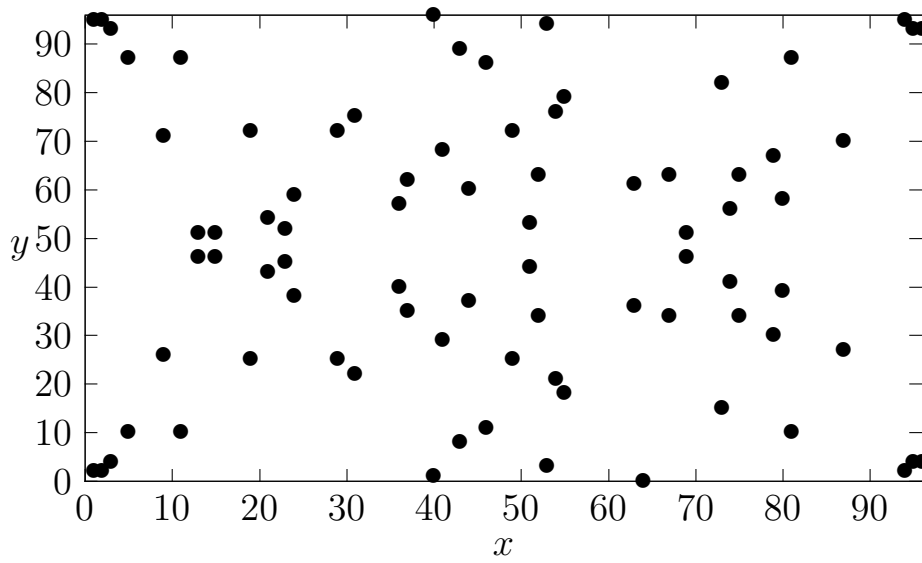


Рис. 19.6: Эллиптическая кривая  $y^2 = x^3 - 7x + 10$  над полем  $\mathbb{F}_{97}$

найденного порядка и ищется точка которая является генератором подгруппы выбранного порядка. Для того чтобы это сделать используется следующий факт. Для любой точки  $g \in E$  имеет место соотношение

$$Ng = 0,$$

где  $N = |E|$  -порядок (число точек) эллиптической кривой. Допустим  $p$  - некоторый простой делитель числа  $N$ :

$$N = hp$$

тогда

$$Ng = p(hg) = 0.$$

Т. о. если  $hg \neq 0$ , то точка  $g' = hg$  будет генератором циклической подгруппы порядка  $p$ .

**Комментарий 19.10.2.** *Имеет смысл в качестве порядка подгруппы выбирать именно простое число, поскольку если порядок группы простой то по теореме Лагранжа (см. теор. 16.1.2) у нее есть только тривиальные подгруппы - сама группа и группа состоящая из единичного элемента. Т. о. в силу  $hg \neq 0$  остается только сама группа, которая является циклической с порядком  $p$ .*

**Пример 19.10.2** (Выбор базовой точки). *Рассмотрим эллиптическую кривую*

$$E = E(\mathbb{F}_{97}) = \{(x, y) \in \mathbb{F}_{97} \times \mathbb{F}_{97} : y^2 \equiv x^3 - 7x + 10\} \cup \{0\},$$

изображенную на [рис. 19.6](#). Порядок этой кривой:

$$N = |E| = 82.$$

Число 82 имеет 2 делителя: 41 и 2. Т. о. существует циклическая подгруппа порядка 41, т.е.  $h = 2$ .

Возьмем точку  $g = (1, 2) \in E$  ее порядок:  $|\langle g \rangle| = 82$ , т.е. эта точка не подходит. Рассчитываем

$$g' = hg = 2g = (96, 93) \neq 0.$$

При этом  $|\langle g' \rangle| = 41$ , т.е. мы нашли требуемую базовую точку.

Если имеется две точки на кривой  $a, b \in E(\mathbb{F}_p)$  то имеет смысл вопрос о существовании такого  $x \in \mathbb{N}$ :

$$x \cdot a = b$$

данная задача называется дискретным логарифмом на эллиптических кривых.

## 19.11 Алгоритм ECDH

Алгоритм ECDH является модификацией алгоритма Диффи-Хеллмана (см. [разд. 19.8](#)) для эллиптических кривых. Протокол Диффи-Хеллмана является протоколом обмена ключей. В нашем случае публикуются следующие параметры эллиптической кривой:  $(p, a, b, g, n, h)$ , где  $p, a, b$  задают кривую

$$E(\mathbb{F}_p) = \{(x, y) : y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{0\},$$

$g$  - базовая точка порядка  $n$ :  $|\langle g \rangle| = n$ ,  $h$  - кофактор группы  $\langle g \rangle$ , т.е.  $n = nh$ .

Алиса выбирает закрытый ключ  $d_a \in \{1, \dots, n-1\}$  и формирует открытый ключ  $A = d_a g$ . Боб также формирует закрытый  $d_b \in \{1, \dots, n-1\}$  и открытый  $B = d_b g$  ключи. Алиса и Боб обмениваются этими ключами. Далее каждый из них вычисляет реальный ключ по правилу  $K = d_a B = d_b A$ .

**Пример 19.11.1** (Алгоритм ECDH). Возьмем кривую и базовую точку из [прим. 19.10.2](#). Т.о.

$$(p, a, b, g, n, h) = (97, -7, 10, (96, 93), 41, 2)$$

Алиса выбирает  $d_a = 5$ , т.е.  $A = (37, 35)$ . Боб выбирает  $d_b = 15$ , т.о.  $B = (15, 51)$ . Ключ у Алисы  $K = d_a B = (46, 11)$  и ключ у Боба  $K = d_b A = (46, 11)$  совпадают.



## Глава 20

# Теория алгоритмов

### 20.1 Основная теорема о рекуррентных соотношениях

**Теорема 20.1.1** (Основная теорема о рекуррентных соотношениях). *Если имеется следующее рекуррентное соотношение для сложности некоторого алгоритма*

$$T(n) = aT\left(\frac{n}{b}\right) + f(n),$$

*то возможно определить асимптотическое поведение функции  $T(n)$  в следующих случаях*

1. *Если  $f(n) = O(n^{\log_b a - \epsilon})$ , при некоторых  $\epsilon > 0$ , то  $T(n) = \Theta(n^{\log_b a})$*
2. *Если  $f(n) = \Theta(n^{\log_b a} \log^k n)$ , то  $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$*
3. *Если  $f(n) = \Omega(n^{\log_b a + \epsilon})$ , при некоторых  $\epsilon > 0$  и  $af\left(\frac{n}{b}\right) \leq cf(n)$  для некоторой константы  $c < 1$  и больших  $n$ , то  $T(n) = \Theta(f(n))$*

### 20.2 Разделяй и властвуй

“Разделяй и властвуй” (divide and conquer) - важная парадигма в решении алгоритмических задач, которая заключается в разделении исходной задачи на более простые.

### 20.3 Булева логика. Булевы формулы КНФ

**Определение 20.3.1** (Конъюнкция (логическое “И”)). Для логической операции “И” ( $a \& b$ ) справедлива следующая таблица истинности [20.1](#).

| $a$ | $b$ | $a \& b$ |
|-----|-----|----------|
| 0   | 0   | 0        |
| 0   | 1   | 0        |
| 1   | 0   | 0        |
| 1   | 1   | 1        |

Таблица 20.1: Конъюнкция  $a \& b$ 

| $a$ | $b$ | $a \parallel b$ |
|-----|-----|-----------------|
| 0   | 0   | 0               |
| 0   | 1   | 1               |
| 1   | 0   | 1               |
| 1   | 1   | 1               |

Таблица 20.2: Дизъюнкция  $a \parallel b$ 

**Определение 20.3.2** (Дизъюнкция (логическое “ИЛИ”)). Для логической операции “ИЛИ” ( $a \parallel b$ ) справедлива следующая таблица истинности [20.2](#).

**Определение 20.3.3** (Булева формула). Булевой формулой называется совокупность булевых литералов объединённых логическими операциями.

**Определение 20.3.4** (КНФ - Конъюнктивная нормальная форма (SAT)). Конъюнктивной нормальной формой в булевой логике называют такую булеву формулу которая имеет вид конъюнкции дизъюнкций литералов.

**Пример 20.3.1.** Задача SAT *Задачей SAT называют задачу о разрешимости КНФ. Допустим задана следующая булева формула в форме КНФ:*

$$(x_1 \parallel x_2 \parallel \bar{x}_3) \& (x_1 \parallel \bar{x}_2 \parallel x_3)$$

*Она является разрешимой, достаточно принять  $x_1 = 1$ , значения  $x_{2,3}$  могут быть любыми.*

*Вместе с тем следующая формула является неразрешимой:*

$$(x_1 \parallel x_2 \parallel \bar{x}_3) \& (\bar{x}_1 \parallel \bar{x}_2 \parallel x_3).$$

**Теорема 20.3.1** (Приводимость к КНФ). *Любая булева формула может быть приведена к КНФ.*

*Доказательство.* Для доказательства можно использовать: закон двойного отрицания, закон де Моргана, дистрибутивность. □

**Теорема 20.3.2** (Приводимость к 3-КНФ (3-SAT)). *Любая булева формула конъюнктивной нормальной форме может быть приведена к 3-КНФ.*

*Доказательство.* TBD □

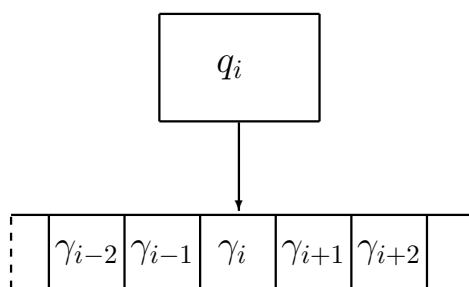


Рис. 20.1: Машина Тьюринга. Текущее состояние машины описывается двумя числами  $(q_i, \gamma_i)$ , где  $q_i \in Q$  - состояние управляющего устройства, которое указывает на элемент ленты  $\gamma_i \in \Gamma$ .

## 20.4 Машина Тьюринга

Машина Тьюринга  $TM$  - математический объект состоящий из управляющего устройства (head) и бесконечной ленты разделенной на ячейки в каждой из которых может быть записан один символ.

Управляющее устройство  $TM$  может находиться в одном из состояний  $q_i \in Q$ , где  $Q$  - множество различных состояний. Состояние в котором  $TM$  находилась в начальный момент времени  $q_0 \in Q$  называется начальным состоянием.

Среди элементов множества  $Q$  выбрано подмножество  $F \subset Q$  финальных состояний. Если  $TM$  оказалась в состоянии  $f \in F \subset Q$ , то говорят что машина Тьюринга завершила (terminate) свою работу.

Символы записанные на ленту образуют некоторое множество (алфавит)  $\Gamma = \{\gamma_i\}$ .

Входным алфавитом  $\Sigma$  машины Тьюринга называется называется подмножество элементов  $\Gamma$  которыми оперирует управляющее устройство  $TM$ , т. е. те символы, которые она может распознать на ленте. Те символы, которые управляющее устройство не может распознать мы будем обозначать символом  $\beta$  (blank).

В процессе работы  $TM$  она выполняет следующие действия:

- считывает элемент на который указывает управляющее устройство (см. [рис. 20.1](#))
- изменяет (или оставляет неизменным) этот символ на элемент  $\sigma \in \Sigma \subset \Gamma$
- изменяет положение управляющего устройства на одну ячейку вправо ( $R$ ), влево ( $L$ ) или не меняет его ( $S$ )

Изменение состояния  $TM$  описывается таблицей переходов  $\Delta$ . Элемент таблицы переходов записывается в следующем виде:  $\delta_j(q_{old}, \gamma_{old})$  где  $q_{old} \in Q$

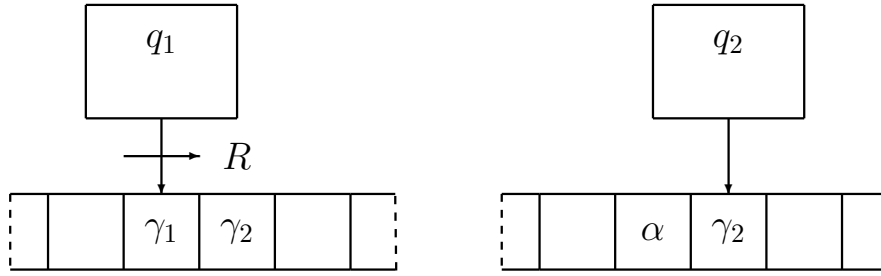


Рис. 20.2: Переход машины Тьюринга из состояния  $(q_1, \gamma_1)$  в состояние  $(q_2, \gamma_2)$ . Соответствующий элемент таблицы переходов  $\delta : \{q_1, \gamma_1\} \rightarrow \{q_2, \alpha, R\}$ . Т. е. элемент ленты на который изначально указывало управляющее устройство ( $\gamma_1$ ) изменяет свое значение на  $\alpha$ , управляющее устройство изменяет свое положение на одну ячейку вправо ( $R$ ).

текущее состояние,  $\gamma_{old} \in \Gamma$  - выбранный элемент на ленте. Значение перехода может быть не определено или записано в виде  $\{q_{new}, \gamma_{new}, d\}$  (см. [рис. 20.2](#)), где  $q_{new} \in Q$  - новое состояние машины Тьюринга,  $\gamma_{new} \in \Gamma$  - новое значение элемента на ленте на который указывало управляющее устройство, т. е.  $\gamma_{old}$  заменяется на  $\gamma_{new}$ .  $d \in D = \{L, R, S\}$  - направление движения управляющего устройства ( $L$  налево,  $R$  направо,  $S$  оставаться на том же самом месте). В случае неопределенного перехода говорят, что машина Тьюринга зависла (halt) в состоянии  $q_{old}$ .

**Определение 20.4.1** (Язык машины Тьюринга  $L(M)$ ). Исходные символы на ленте могут трактоваться как некоторая строка  $x$  которая поступает на вход машины Тьюринга  $M$ . Все те строки которые приводят машину  $M$  в некоторое финальное состояние  $f \in F$  называются языком  $L(M)$  машины  $M$

**Определение 20.4.2** (Детерминированная машина Тьюринга). Если в таблице переходов отображение  $(q_{old}, \gamma_{old}) \rightarrow \{q_{new}, \gamma_{new}, d\}$  является биекцией<sup>1</sup>, то соответствующая машина Тьюринга называется детерминированной машиной Тьюринга

**Определение 20.4.3** (Не-детерминированная машина Тьюринга). Если в таблице переходов отображение  $(q_{old}, \gamma_{old}) \rightarrow \{q_{new}, \gamma_{new}, d\}$  не является биекцией, т. е. состоянию  $(q_{old}, \gamma_{old})$  может соответствовать несколько элементов таблицы переходов  $\{q_{new}, \gamma_{new}, d\}$ , то соответствующая машина Тьюринга называется не-детерминированной машиной Тьюринга

<sup>1</sup>Биекция - взаимно однозначное отображение, т. е. в нашем случае каждому состоянию  $(q_{old}, \gamma_{old})$  соответствует только один элемент таблицы переходов  $\{q_{new}, \gamma_{new}, d\}$



Рис. 20.3: Машина Тьюринга  $M$  как функция  $t(x)$ . На входе имеется некоторая последовательность исходных данных  $x$  (начальные символы на ленте). На выходе  $M$  может оказаться в некотором финальном состоянии (1 - принять  $x$ ), зависнуть (0 - отклонить  $x$ ) - т. е. оказаться в состоянии из которого нет дальнейших переходов. Машина также может войти в бесконечный цикл и никогда не завершить свою работу

## 20.5 Теория вычислимости

Машина Тьюринга  $M$  (см. [рис. 20.3](#)) может трактоваться как некоторая функция  $t$  в качестве аргумента которой является набор символов представляющий собой начальное состояние ленты  $x$ . В результате обработки  $x$  машина  $M$  может завершить свою работу, т. е. оказаться в некотором финальном состоянии  $f \in F \subset Q$ . В этом случае говорят, что  $M$  принимает  $x$ . В этом случае значение соответствующей функции  $t(x) = 1$ .

При этом вычисление функции  $t(x)$  может трактоваться как некоторая задача.

**Определение 20.5.1** (Задача). Будем называть задачей относительно машины Тьюринга ответ да/нет на вопрос об некотором множестве возможных объектов

**Пример 20.5.1** (Гамильтонов граф). *Задача о гамильтоновом графе - для заданного графа существует или нет путь (цепь) содержащий каждую вершину этого графа только один раз.*

В случае зависания (halt)  $M$ , т. е. когда  $M$  оказывается в состоянии дальнейший переход из которого не определен, говорят, что  $M$  отвергает  $x$ . В этом случае значение соответствующей функции  $t(x) = 0$ .

Так же машина  $M$  на входе  $x$  может никогда не завершить свою работу. В этом случае значение функции  $t(x)$  не определено.

**Определение 20.5.2** (Рекурсивный язык (Recursive language)). Множество строк  $L$ <sup>2</sup> называется рекурсивным языком если существует машина Тьюринга  $M$  такая, что  $\forall x \in L$  соответствующая функция  $t(x) = 1$ , а  $\forall x \notin L$  соответствующая функция  $t(x) = 0$ .

<sup>2</sup>множество начальных состояний ленты некоторой машины Тьюринга

Т. о.  $M$  соответствующая рекурсивному языку  $L(M)$  останавливается на любых исходных данных. Множество рекурсивных языков обозначается  $R$ .

**Определение 20.5.3** (Рекурсивно перечислимый язык (Recursively enumerable language)). Множество строк  $L$  называется рекурсивно перечислимым языком если существует машина Тьюринга  $M$  такая, что  $\forall x \in L$   $M$  завершает свою работу в некотором финальном состоянии, т. е. соответствующая функция  $m(x) = 1$ .

Т. о.  $M$  соответствующая рекурсивно перечислимому языку  $L(M)$  останавливается на любых исходных данных принадлежащих языку, но при этом может никогда не завершить свою работу при исходных данных не принадлежащих языку  $L(M)$ . Множество рекурсивно перечислимых языков обозначается  $RE$ . Очевидно  $R \subset RE$ .

Машина Тьюринга задает класс функций для которых можно определить такое понятие как вычислимость.

**Определение 20.5.4** (Вычислимая функция). <sup>3</sup> Функция  $m$  называется вычислимой, а соответствующая ей задача - разрешимой, если для нее существует некоторая машина Тьюринга  $M$ , а соответствующий этой машине язык является рекурсивным  $L(M) \in R$ . В противном случае соответствующая задача называется не разрешимой.

**Теорема 20.5.1** (О мощности множества машин Тьюринга). *Множество машин Тьюринга счетно.*

*Доказательство.* Множество называется счетным [55] если каждому его элементу можно поставить в соответствие некоторое натуральное число. Машина Тьюринга взаимно однозначно определяется следующей группой элементов

- Множество состояний  $Q$
- Начальное состояние  $q_0$
- Множество финальных состояний  $F \subset Q$
- Алфавит  $\Sigma$
- Таблица переходов  $\Delta$

---

<sup>3</sup> На самом деле понятие вычислимости не может быть определено строго математически и дается здесь в формулировке тезиса Чёрча - Тьюринга

В силу того, что каждый из перечисленных элементов машины Тьюринга принимает ограниченное число значений, то каждому элементу, а следовательно и всей машине Тьюринга, можно поставить некоторое уникальное (для соответствующей машины) число <sup>4</sup>, что доказывает счетность множества всех машин Тьюринга.  $\square$

После введения понятия вычислимой функции ставит вопрос о вычислимости произвольной функции. Допустим у нас имеются некоторые исходные данные (аргумент функции)  $x$  существует ли такая машина Тьюринга  $M$  которая принимает эти данные, т. е.  $M$  завершит свою работу в некотором финальном состоянии. Ответ на этот вопрос дает следующая теорема

**Теорема 20.5.2** (О невычислимости). *Существует такой язык  $L_d$  который не принимает ни одна машина Тьюринга, т. е. соответствующая  $L_d$  задача является принципиально неразрешимой (не вычислимой)*

Язык  $L_d$  часто называют диагональным языком (diagonalization language), потому что если составить матрицу [11] индексы строк которой будут задавать номера исходных данных машин Тьюринга, а номера столбцов будут соответствовать номер машин Тьюринга. Значение этой матрицы  $a_{ij}$  будет равно 1 если  $M_j$  содержит  $x_i$  и 0 в противном случае. Инвертированные <sup>5</sup> числа на диагонали будут определять язык  $L_d$ .

*Доказательство.* В силу теоремы **О мощности множества машин Тьюринга** (Теорема 20.5.1) можно говорить о  $i$ -ой машине Тьюринга  $M_i$ , где  $i$  - некоторое натуральное число. Допустим  $x_i$  строка которая не распознается  $M_i$ , т. е.  $x_i \notin L(M_i)$ . Строки  $x_i$  образуют некоторый язык  $L_d$ . В силу определения языка  $L_d$  не существует машины Тьюринга, которая бы принимала все строки этого языка.  $\square$

**Определение 20.5.5** (Универсальная машина Тьюринга). Универсальная машина Тьюринга  $M_u$  это такая машина, которая получив на входе строку  $x$  и код для некоторой машины Тьюринга  $M$  вычисляет результат применения  $x$  на  $M$ .

Множество пар строк  $(x, M)$  образуют некоторый язык  $L_U$  машины  $M_U$ .

---

<sup>4</sup> Например можно закодировать каждую машину уникальной последовательностью чисел 0 и 1. Полученная последовательность будет конечной в силу конечности множества элементов из которых состоит машина Тьюринга. Любой конечной последовательности чисел 0 и 1 соответствует уникальное натуральное число, для которого рассматриваемая последовательность является двоичной записью.

<sup>5</sup> 0 заменен на 1, а 1 на 0

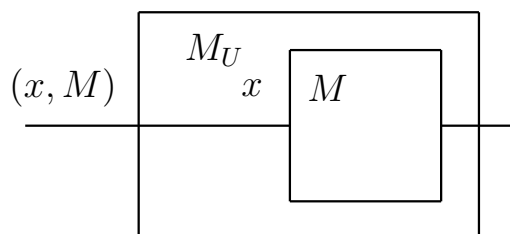


Рис. 20.4: Универсальная машина Тьюринга  $M_U$ .  $M_U$  получает на вход пару строк  $(x, M)$ , где  $M$  представляет собой код некоторой машины Тьюринга на которой должны быть выполнены исходные данные  $x$

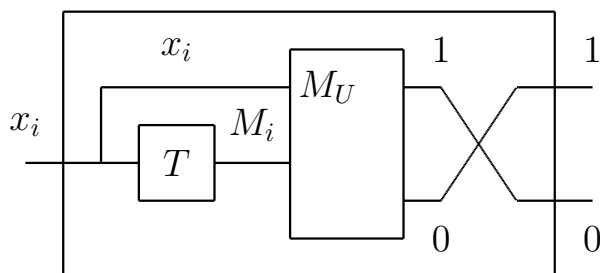


Рис. 20.5: Доказательство  $L_U \notin R$ . Если  $L_U \in R$ , то универсальная машина Тьюринга  $M_U$  может быть построена для машины Тьюринга  $M_d$ , которая принимает все строки языка  $L_d$ , что невозможно в силу теоремы 20.5.2.  $T$  специальное устройство которое по строке  $x_i$  создает код для машины Тьюринга  $M_i$ , которая не принимает  $x_i$ .



**Теорема 20.5.3** (О языке универсальной машины Тьюринга). *Язык универсальной машины Тьюринга является рекурсивно перечислимым и не является рекурсивным, т. е.  $L_U \in RE$  и  $L_U \notin R$ . Таким образом задача распознавания языка универсальной машины Тьюринга является не разрешимой.*

*Доказательство.* Утверждение  $L_U \in RE$  прямо вытекает из определения универсальной машины Тьюринга: если  $M$  принимает  $x$  то и  $M_U$  принимает пару строк  $(x, M)$ .

Утверждения  $L_U \notin R$  докажем от противного, т. е. допустим, что  $L_U \in R$ . Построим с помощью такой машины  $M_U$  машину Тьюринга  $M_d$  которая будет принимать все строки языка  $L_d$ . Для каждой строчки  $x_i \in L_d$  можно поставить в соответствие некоторую машину Тьюринга  $M_i$  которая не принимает эту строчку, т. е.  $x_i \notin L(M_i)$ . Пара значений  $(x_i, M_i)$  может быть подана на вход универсальной машины Тьюринга как это показано на [рис. 20.5](#). Если  $L_U \in R$  то машина  $M_U$  может решить принимает  $M_i$  исходные данные  $x_i$  или нет. Если  $M_i$  не принимает  $x_i$ , то машина  $M_d$  должна принять эти данные. Таким образом построена машина Тьюринга  $M_d$  которая принимает все строки  $x_i \in L_d$  и отвергает все строки  $x_i \notin L_d$ , что невозможно в силу теоремы [О невычислимости](#) (Теорема 20.5.2)  $\square$

Каждая машина Тьюринга  $M$  имеет некоторый код который может быть интерпретирован как исходные данные для другой машины Тьюринга  $M_R$ . Машина может как принять так и отвергнуть этот код. В силу взаимной однозначности соответствия между машиной Тьюринга  $M$  и языком  $L(M)$ , можно говорить о машине Тьюринга которая принимает либо отвергает языки  $L$ . Если машина  $M_R$  принимает некоторое множество языков, то говорят, что эти языки обладают некоторым свойством  $P$ .

**Определение 20.5.6** (Нетривиальное свойство языка машины Тьюринга). Свойство языка называется нетривиальным если среди всех языков можно выделить как те которые удовлетворяют данному свойству так и те которые ему не удовлетворяют.

**Теорема 20.5.4** (Райс). *Задача об определении любого нетривиального свойства языка  $L(M)$  машины Тьюринга  $M$  является неразрешимой задачей*

*Доказательство.* Допустим, что мы имеем машину  $M_R$  которая может определять некоторое нетривиальное свойство языков  $P$ , т. е. она может распределить языки всех машин Тьюринга в два множества (каждое из которых является непустым). Первое из этих множеств содержит все языки удовлетворяющие  $P$  ( $M_R$  принимает языки из этого множества), а второе - все языки которые не удовлетворяют свойству  $P$ .



Рис. 20.6: Теорема Райса. Машина Тьюринга  $M_P$  распознающая нетривиальное свойство языка  $P$  используется для построения универсальной машины Тьюринга  $M_U$  которая может как принимать так и отвергать пары строк  $(x, M)$ . Адаптер  $T$  используется для преобразования пары строк  $(x, M)$  в код для машины Тьюринга  $M'$  которая удовлетворяет свойству  $P$  тогда и только тогда когда  $M$  принимает  $x$ .

Попробуем построить на базе  $M_P$  универсальную машину Тьюринга  $M_U$ , которая принимает (или отвергает) пары  $(x, M)$  (см. [рис. 20.6](#)).

Допустим мы имеем машину  $M_L$  которая принимает строки  $l$  из некоторого языка  $L$  <sup>6</sup>.

В качестве первого шага построим машину  $M'$ , которая принимает строки  $l$ . При этом пара  $(x, M)$  считается заданной и встроена в код  $M'$ . Ключевым свойством  $M'$  является следующее:  $M'$  принимает строки  $l \in L$  в том и только том случае если  $M$  принимает  $x$ . Таким образом возможны два случая:

- $L(M') = L(M_L)$  если  $M'$  принимает  $l$  как результат приема пары  $(x, M)$
- $L(M') = \emptyset$  если  $M'$  отвергает любые исходные данные  $l$ , т. е. в случае если  $M$  никогда не завершает свою работу при исходных данных  $x$

На следующем шаге вспомним про свойство  $P$  и допустим, что язык  $L$  (который принимает машина  $M'$ ) имеет свойство  $P$ , т. е.  $L \in P$ . Также предположим, что  $\emptyset \notin P$  <sup>7</sup>. Т. о. если подать код для  $M'$  на вход машины  $M_P$ , то  $M_P$  примет исходные данные (код  $M'$ ) если  $L(M') \in P$  и отклонит их если  $L(M') = \emptyset$ .

С другой стороны пара  $(x, M)$  встроена в исходный код  $M'$ , т. е. можно полагать что  $M_P$  получает на вход именно пару  $(x, M)$  и принимает ее если  $M$  принимает  $x$  ( $L(M') \in P$ ) и отвергает эту пару если  $M$  не принимает  $x$  ( $L(M') = \emptyset \notin P$ ). Таким образом с помощью  $M_P$  мы построили универсальную машину Тьюринга и показали что ее язык является рекурсивным, что невозможно в силу теоремы [О языке универсальной машины Тьюринга \(Теорема 20.5.3\)](#).  $\square$

<sup>6</sup>Никакой взаимосвязи между языком  $L$  и свойством  $P$  на этом шаге

<sup>7</sup> Если  $\emptyset \in P$  тогда можно рассмотреть свойство  $\bar{P} = \{ \forall L : L \notin P \}$ . В этом случае  $\emptyset \notin \bar{P}$

## 20.6 Классы сложности $P$ , $NP$

При решении той или иной задачи возникают прежде всего два вопроса. Имеет ли поставленная задача решение в принципе, т. е. может ли быть построен алгоритм решающий поставленную задачу. Как только найден положительный ответ на первый вопрос, т. е. построен алгоритм решающий задачу, то следующей проблемой встает вопрос о практической реализуемости предложенного решения. Здесь нам поможет теория сложности алгоритмов которая решает вопрос о реализуемости тех или иных алгоритмов.

В следующей таблице [35] приведены некоторые большие числа которые полезны при анализе сложности алгоритмов

**Пример 20.6.1.** Факторизация целых чисел методом перебора *Допустим что перед нами стоит задача о факторизации целого числа  $x$  (см. пример 13.0.2). В двоичном представлении  $x$  состоит из  $N$  знаков, т. е.  $2^N \leq x < 2^{N+1}$ . В простейшем варианте (перебор делителей) мы можем перебирать все целые числа от 2 до  $2^{\frac{N}{2}}$  и для каждого из таким чисел  $2 < y \leq 2^{\frac{N}{2}}$  искать остаток от деления  $x$  на  $y$ . Если  $x$  делится на  $y$  то задача решена и  $y$  объявляется делителем числа  $x$ . Если ни одно из чисел  $y$  не делит  $x$ , то  $x$  объявляется простым. Т. о. исходная задача бьется на  $2^{\frac{N}{2}}$  подзадач об отыскании остатка от деления.*

*Допустим что в числе  $x$  20 знаков, т. е.  $N = 20$ . В этом случае необходимо выполнить  $2^{10} = 1024$  операций деления чтобы найти решение исходной задачи, что может быть легко сделано на простых компьютерах.*

*Вместе с тем если увеличить число знаков в 30 раз -  $N = 600$ , то для решения поставленной задачи необходимо выполнить  $2^{300}$  операций деления. Если посмотреть на табл. 20.3, то можно увидеть что это число много больше числа атомов во вселенной  $2^{265}$ . Т. е. даже если каждый атом вселенной будет представлять собой некоторое простейшее вычислительное устройство, которое вычисляет остаток от деления двух целых чисел, то использовав все атомы вселенной невозможно будет решить поставленную задачу.*

*Т. о. несмотря на присутствие простого алгоритма, задача факторизации целых чисел, посредством этого алгоритма, становится практически не реализуемой для чисел длиной 600 символов в двоичной записи несмотря на то, что число 600 кажется не очень большим по сравнению с 20 (где задача является практически реализуемой).*

| Физический аналог   | Число   |
|---|---|
| Вероятность быть убитым молнией (в течение дня)   | 1 из 9 миллиардов ( $2^{33}$ )                              |
| Вероятность выиграть главный приз в государственной лотерее США   | 1 из 4000000 ( $2^{22}$ )                                   |
| Вероятность выиграть главный приз в государственной лотерее США и быть убитым молнией в течение того же дня | 1 из $2^{61}$   |
| Вероятность утонуть (в США в течение года)  | 1 из 59000 ( $2^{16}$ )                                     |
| Вероятность погибнуть в автокатастрофе (в США в году)   | 1 из 6100 ( $2^{13}$ )                                      |
| Вероятность погибнуть в автокатастрофе (в США в течение времени жизни)                                      | 1 из 88 ( $2^7$ )   |
| Время до следующего оледенения  | 14000 ( $2^{14}$ ) лет                                      |
| Время до превращения Солнца в сверхновую звезду   | $10^9$ ( $2^{30}$ ) лет                                     |
| Возраст планеты   | $10^{10}$ ( $2^{34}$ ) лет                                  |
| Возраст Вселенной   | $10^{51}$ ( $2^{170}$ )                                     |
| Число атомов планеты  | $10^{57}$ ( $2^{190}$ )                                     |
| Число атомов Солнца   | $10^{67}$ ( $2^{223}$ )                                     |
| Число атомов галактики  | $10^{77}$ ( $2^{265}$ )                                     |
| Число атомов Вселенной  | $10^{84}$ ( $2^{280}$ ) см <sup>3</sup>                     |
| Если Вселенная конечна:   |   |
| Полное время жизни вселенной  | $10^{11}$ ( $2^{37}$ ) лет<br>$10^{18}$ ( $2^{61}$ ) секунд |
| Если Вселенная бесконечна:  |   |
| Время до остывания легких звезд   | $10^{14}$ ( $2^{47}$ ) лет                                  |
| Время до отрыва планет от звезд   | $10^{15}$ ( $2^{50}$ ) лет                                  |
| Время до отрыва звезд от галактик   | $10^{19}$ ( $2^{64}$ ) лет                                  |
| Время до разрушения орбит гравитационной радиацией  | $10^{20}$ ( $2^{67}$ ) лет                                  |
| Время до разрушения черных дыр процессами Хокинга   | $10^{64}$ ( $2^{213}$ ) лет                                 |
| Время до превращения материи в жидкость при нулевой температуре   | $10^{65}$ ( $2^{216}$ ) лет                                 |

Таблица 20.3: Большие числа [35]

### 20.6.1 Иерархия классов сложности

Ниже даются формальные определения для задач которые являются практически реализуемыми  $P$ . Также определяется класс задач которые являются практически не реализуемыми (до тех пор пока не доказано, что  $P = NP$ ).

**Определение 20.6.1** (Размер задачи). Размером задачи  $N$  мы будем называть число символов алфавита машины Тьюринга, содержащихся на ленте в исходном состоянии, т. е. другими словами размером задачи мы будем считать длину строки которая поступает на вход машины Тьюринга.

Например в примере 20.6.1 размером задачи является длина числа  $x$  (для которого ищутся делители) в двоичной записи.

**Определение 20.6.2** (Класс  $P$ ). Задача (алгоритм) принадлежит к классу  $P$  (Polynomial) если он может быть решен за  $O(N^k)$  шагов на детерминированной машине Тьюринга. Здесь  $N$  - размер исходной задачи,  $k$  - произвольное целое число, которое не зависит от  $N$ .

Класс  $P$  определяет класс задач которые являются практически реализуемыми. Например задача о сортировке неупорядоченных данных (списка) может быть решена за  $O(N \log N) = O(N^2)$  шагов, где  $N$  - число элементов в списке, который надо отсортировать (размер задачи).

**Определение 20.6.3** (Класс  $NP$ ). Задача (алгоритм) принадлежит к классу  $NP$  (Nondeterministic Polynomial) если он может быть решен за  $O(N^k)$  шагов на не детерминированной машине Тьюринга. Здесь  $N$  - размер исходной задачи,  $k$  - произвольное целое число, которое не зависит от  $N$ .

Одним из примеров  $NP$  задачи является задача факторизации целых чисел. Не детерминированная машина Тьюринга может угадать решение (за один шаг) и проверить его (умножить два угаданных числа и сравнив результат умножения с исходным числом) за полиномиальное время. Вместе с тем вопрос о принадлежности задачи факторизации к классу  $P$  является открытым.

Задача о равенстве классов  $P$  и  $NP$  является одной из важнейших нерешенных задач математики и, наверное, важнейшей из нерешенных задач теории алгоритмов. Для того чтобы показать каким образом  $NP$  задача может быть сведена к  $P$  необходимо ввести класс  $NP$ -полных задач, которые являются, в некотором смысле, самыми сложными из  $NP$  задач.

**Определение 20.6.4** (Класс  $NPC$  ( $NP$ -полный ( $NP$ -complete))). Задача  $M$  принадлежит к классу  $NPC$ , если любая  $NP$  задача может быть сведена к  $M$  (см. рис. 20.8).



Рис. 20.7: Соотношение классов сложности  $P$ ,  $NP$  и  $NPC$ . Представленная картина соответствует предположению  $P \neq NP$ . В этом случае  $P \subset NP$ ,  $NPC \subset NP$ . Любая задача из  $P$  и  $NP$  может быть за полиномиальное время сведена к  $NPC$ .



Рис. 20.8: Класс  $NPC$ . Вход для любой  $NP$  задачи  $x$  может быть преобразован в вход  $y$  для некоторой задачи из класса  $NPC$ . Преобразование  $x \rightarrow y$  может быть сделано за  $O(N^k)$  шагов, где  $N = |x|$  - длина  $x$ ,  $k$  - некоторое целое число независимое от  $N$ .

Таким образом если будет найден полиномиальный алгоритм хотя бы для одной  $NPC$  задачи, то будут найдены полиномиальные алгоритмы для всех  $NP$  задач (см. [рис. 20.7](#)).

## 20.6.2 Теорема Кука-Левина

Как только мы ввели класс сложности  $NPC$  встает вопрос о задачах которые в него входят. Ниже будет показано, что задача SAT (о выполнимости булевой формулы в конъюнктивной нормальной форме) является  $NP$  полной.

**Теорема 20.6.1** (Кук-Левин). *Задача о выполнимости булевой формулы в КНФ является  $NP$  полной, т. е. принадлежит классу  $NPC$ .*

*Доказательство.* Доказательство состоит из двух частей. Во первых мы должны доказать задача SAT (см. пример [20.3.1](#)) принадлежит классу  $NP$ . Во вторых мы должны показать, что любая задача из класса  $NP$  может быть сведена к задаче SAT за полиномиальное время.

Принадлежность к классу  $NP$  доказывается очевидным образом, - т. к. существует возможность проверить истинность решения за число шагов  $O(N)$ ,

где  $N$  - число булевых операций использованных в рассматриваемой булевой формуле.

TBD







## Часть 6

# Ответы на вопросы



## Глава 21

# Квантовая электродинамика

## 21.1 Квантование электромагнитного поля

### 21.1.1 5: Число мод

Сколько мод электромагнитного поля с длиной волны  $\lambda \geq 500\text{нм}$  находятся в кубе квантования со стороной  $L = 1\text{мм}$ ?

Диапазону длин волн  $\lambda \geq \lambda_0 = 500\text{нм}$  соответствует диапазон частот  $\omega \leq \omega_0 = \frac{2\pi c}{\lambda_0}$ .

Воспользуемся формулой 1.47

$$dN = 2 \left( \frac{L}{2\pi c} \right)^3 \omega^2 d\omega d\Omega$$

откуда

$$\begin{aligned} N &= \int_0^{\omega_0} 2 \left( \frac{L}{2\pi c} \right)^3 \omega^2 d\omega \int_{4\pi} d\Omega = \\ &= 8\pi \int_0^{\omega_0} \left( \frac{L}{2\pi c} \right)^3 d\omega = 8\pi \left( \frac{L}{2\pi c} \right)^3 \frac{\omega_0^3}{3} = \\ &= \frac{8\pi}{3} \left( \frac{L}{\lambda_0} \right)^3 \approx 67 \cdot 10^9 \end{aligned}$$

## 21.2 Взаимодействие света с атомом

### 21.2.1 13: Определение частоты перехода атома лития

Обозначим через  $\Omega_R^{(1,2)}$  эффективные частоты Раби для измерения 1 и 2 соответственно. Расстройки частот для двух экспериментов  $\delta_{1,2}$ . Таким обра-

зом имеем

$$\begin{aligned}\Omega_R^{(1)} &= \sqrt{\omega_R^2 + \delta_1^2}, \\ \Omega_R^{(2)} &= \sqrt{\omega_R^2 + \delta_2^2}\end{aligned}\quad (21.1)$$

С другой стороны из графиков [рис. 2.19](#) видно что максимальная вероятность обнаружить атомы лития в состоянии  $|2\rangle$  для частоты  $\omega_2 = 2\pi \cdot 228.4\text{МГц}$  будет  $P_2 = 0.49$ , с другой стороны ([2.27](#)) имеем

$$P_2 = \left( \frac{\omega_R}{\Omega_R^{(2)}} \right)^2 = \frac{1}{1 + \frac{\delta_2^2}{\omega_R^2}},$$

откуда

$$\omega_R = 0.98 \cdot \delta_2. \quad (21.2)$$

С другой стороны можно заключить, что

$$\frac{\Omega_R^{(1)} \cdot 6\text{мкс}}{2} = \pi$$

и

$$\frac{\Omega_R^{(2)} \cdot 12.5\text{мкс}}{2} = \pi,$$

т. о.

$$\Omega_R^{(1)} = 2\pi \cdot 0.167\text{МГц},$$

и

$$\Omega_R^{(2)} = 2\pi \cdot 0.08\text{МГц},$$

Из ([21.1](#)) и ([21.2](#)) можно получить

$$\delta_2 = 2\pi \cdot 0.057\text{МГц},$$

т. е. два кандидата

$$f_0 = 228.4 \pm 0.057\text{МГц} = 228.343\text{МГц}, 228.457\text{МГц} \quad (21.3)$$

Для  $\delta_1$  имеем

$$\delta_1 = \sqrt{\left(\Omega_R^{(1)}\right)^2 - \omega_R^2} = 2\pi \sqrt{0.167^2 - (0.98 \cdot 0.057)^2}\text{МГц} = 2\pi \cdot 0.157\text{МГц}$$

т. о. получаем очередные два кандидата

$$f_0 = 228.5 \pm 0.157\text{МГц} = 228.343\text{МГц}, 228.657\text{МГц} \quad (21.4)$$

Из (21.3) и (21.4) окончательно имеем

$$f_0 = 228.343 \text{ МГц.}$$

Стоит отметить, что полученное значение отличается от реального  $f_0 = 228.205 \text{ МГц}$ . Отличие вызвано влиянием эффекта Зеемана от магнитного поля, которое обычно присутствует в таких экспериментах.



## Глава 22

# Квантовая оптика

### 22.1 Квантовая теория лазера

#### 22.1.1 6: Естественная ширина линии

Из (3.24) имеем

$$D = \frac{A}{2\bar{n}_{st}} = \frac{10^6}{2 \cdot 10^6} = 0.5\Gamma_{\text{ц}}.$$





# Предметный указатель

перепутанные состояния, 341  
 $\sigma$ - алгебра  
     определение, 351  
 AES, 389  
 Основная теорема о рекуррентных  
     соотношениях, 376  
 Малая теорема Ферма, 292, 386  
 Золотое правило Ферми, 145  
 алгоритм Гровера, 303  
 алгоритм Шора, 279  
 Функция Эйлера, 362, 385  
 О мощности множества машин  
     Тьюринга, 407  
 О невычислимости, 409  
 О языке универсальной машины  
     Тьюринга, 410  
 Об операторном тождестве, 208  
 Безу, 382  
 , 387  
 Хинчин-Винер, 117, 119  
 Стоун, 323

## А

Абелева группа, 363, 396  
     определение, 362  
 Адиабатическая теорема  
     определение теоремы, 343  
 Аксиома  
     Аддитивность  
         определение, 352  
     Не-отрицательность  
         определение, 352

## Нормировка

    определение, 352  
 Аксиомы Колмогоровской теории  
     вероятностей  
         пример, 352  
 Алгоритм ECDH, 400  
     пример, 400  
 алгоритм RSA, 268, 269, 276, 384  
     генерация ключей, 384  
     де шифрование, 386  
     шифрование, 385

## Б

Базисные состояния Белла, 240  
     генерация, 241  
     регистрация, 242  
 Безу  
     определение теоремы, 379  
 бозон, 245, 346  
 Булева формула  
     определение, 402

## В

вектор Джонса, 189, 192  
 вектор Стокса, 190  
 Вероятность  $P$   
     определение, 352  
 Выбор базовой точки  
     пример, 399  
 Вычислимая функция  
     определение, 406

**Г**

Гамильтониан, 20, 28, 37, 91, 93,  
124, 135, 216, 337, 339, 347

системы атом-поле, 52

Гамильтонов граф

пример, 405

Генерация ключей (Elgamal)

пример, 389

Гильбертово пространство

определение, 367

гомодин, 185, 221, 227

гомодинный детектор, 184

**Д**

Двумерное преобразование Фурье

определение, 376

двумерное преобразование Фурье,

300

определение, 376

Декогеренция, 315, 327

скорость, 329

Детерминированная машина

Тьюринга

определение, 404

Дешифрование (Elgamal)

пример, 390

Дизъюнкция (логическое “ИЛИ”)

определение, 402

Дискретное логарифмирование на

эллиптической кривой

пример, 301

Дискретный логарифм

определение, 387

Дискретный логарифм в кольце

вычетов по модулю  $p$

определение, 388

Добротность, 81

определение, 81

**З**

Задача

определение, 405

Золотое правило Ферми

определение теоремы, 347

**И**

Игра Мермина-Переса

пример, 249

Измерение энергии двухуровневого

атома

пример, 330

Интерферометр Маха-Цендера, 183

**К**

квантование

свободного электромагнитного  
поля, 19

электромагнитного поля при  
разложении его по плоским  
волнам, 28

Китаев

определение теоремы, 276

Класс  $NP$

определение, 413

Класс  $NPC$  ( $NP$ -полный

( $NP$ -complete))

определение, 413

Класс  $P$

определение, 413

КНФ - Конъюнктивная

нормальная форма (SAT)

определение, 402

Конъюнкция (логическое “И”)

определение, 401

Криптостойкость одноразового

блокнота

определение теоремы, 267

Кук-Левин

определение теоремы, 414

**Л**

Лагранж

определение теоремы, 362

Линейное пространство  
определение, 365

## М

Малая теорема Ферма  
определение теоремы, 383  
Матрица плотности, 44, 46, 76, 121,  
145, 156, 258, 259, 264, 327,  
358  
Мера  
определение, 351  
Моноид  
определение, 361  
Мультипликативная группа кольца  
вычетов  
определение, 362

## Н

Не-детерминированная машина  
Тьюринга  
определение, 404  
Нетривиальное свойство языка  
машины Тьюринга  
определение, 409

## О

О мощности множества машин  
Тьюринга  
определение теоремы, 406  
О невычислимости  
определение теоремы, 407  
О порядке  $(\mathbb{Z}/n\mathbb{Z})^\times$   
определение теоремы, 362  
О языке универсальной машины  
Тьюринга  
определение теоремы, 407  
Об операторном тождестве  
определение теоремы, 365  
Одноразовый блокнот, 266  
Основная теорема о рекуррентных  
соотношениях  
определение теоремы, 401

Отрицательный элемент  
определение, 380

## П

парадокс ЭПР, 232, 334  
параметры Стокса  
квантовый случай, 192  
классический случай, 190  
Переменный Штарк - эффект, 61  
Плотность распределения  
случайной величины  
определение, 355  
Поле, 382, 396  
Поле (алгебра)  
определение, 363  
Поле  $\mathbb{C}$   
пример, 363  
Поле  $\mathbb{Q}$   
пример, 363  
Поле  $\mathbb{R}$ , 396  
пример, 363  
Преобразование Адамара, 244, 286,  
288, 311, 328  
определение, 275  
Приводимость к 3-КНФ (3-SAT)  
определение теоремы, 402  
Приводимость к КНФ  
определение теоремы, 402  
Пространство событий  
определение, 352  
пример, 352  
Прямолинейное движение  
материальной точки  
пример, 336

## Р

Размер задачи  
определение, 413  
Райс  
определение теоремы, 409  
Распределение Пуассона

определение, 355  
 распределение Пуассона, 39, 112,  
 113, 166, 174, 201

Рекурсивно перечислимый язык  
 (Recursively enumerable  
 language)

определение, 406

Рекурсивный язык (Recursive  
 language)

определение, 405

## С

Сжатое вакуумное состояние, 210

сжатый вакуум, 210

Симметричный делитель.

Классический случай

пример, 180

Скалярное произведение

пример, 398

Случайная величина

определение, 354

Смешанное состояние, 43, 259, 331

определение, 326

Соотношение Безу

пример, 379

Среднее случайной величины

определение, 355

Стоун

определение теоремы, 367

## Т

Тензорное (внешнее) произведение  
 линейных операторов

определение, 365

Тензорное произведение, 75, 88, 290

определение, 365

Тензорное произведение линейных  
 пространств

определение, 365

теорема Лагранжа, 396, 399

Теорема об общих делителях

определение теоремы, 377

## У

Универсальная машина Тьюринга

определение, 407

Универсальный набор квантовых  
 вентиляей

определение, 276

## Ф

фермион, 346

фотон, 32, 35, 37, 59, 65, 71, 236,  
 245, 264

неразрушающие измерения, 62

перепутанное состояние, 248,  
 269

Функция распределения случайной  
 величины

определение, 355

Функция Эйлера

определение, 382

пример, 382

Функция Эйлера произведения  
 (обобщенная  
 мультипликативность)

свойство, 383

Функция Эйлера простого числа

свойство, 382

## Х

Хинчин-Винер

определение теоремы, 356

## Ц

Циклическая группа

определение, 362

## Ч

частота Раби, 59

Чистое состояние, 149, 234, 259, 329

определение, 326

## Ш

Шифрование (Elgamal)

пример, [390](#)

## **Я**

Язык машины Тьюринга  $L(M)$

определение, [404](#)



# Литература

- [1] Aravind, P. Quantum mysteries revisited again / P Aravind // J.Phys. — 2004. — 10. — Vol. 72. — P. 1303–7. — [https://www.researchgate.net/publication/228356664\\_Quantum\\_mysteries\\_revisited\\_again](https://www.researchgate.net/publication/228356664_Quantum_mysteries_revisited_again).
- [2] Bell, J. S. On the Einstein-Podolsky-Rosen paradox / John S. Bell // Physics. — 1964. — Vol. 1. — P. 195–200.
- [3] Bennett, C. H. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states / Charles H. Bennett, S. Wiesner // Physical Review Letters. — 1992. — Vol. 69, no. 20. — P. 2881–2884. — <http://dx.doi.org/10.1103/PhysRevLett.69.2881>.
- [4] Brassard, G. Multi-Party Pseudo-Telepathy / G. Brassard, A. Broadbent, A. Tapp // eprint arXiv:quant-ph/0306042. — 2003. — Jun.
- [5] Can quantum-mechanical description of physical reality be considered complete? / A. Einstein, B. Podolsky, N. Rosen et al. // Physical review. — 1935. — Vol. 47, no. 10. — P. 777–780.
- [6] Dense Coding in Experimental Quantum Communication / Klaus Mattle, Harald Weinfurter, Paul G. Kwiat, Anton Zeilinger // Physical Review Letters. — 1996. — Jun. — Vol. 76, no. 25. — P. 4656–4659. — <http://dx.doi.org/10.1103/PhysRevLett.76.4656>.
- [7] Freedman, S. J. Experimental test of local hidden-variable theories / Stuart J. Freedman, John F. Clauser // Phys. Rev. Lett. — 1972. — Apr. — Vol. 28. — P. 938–941. — <http://link.aps.org/doi/10.1103/PhysRevLett.28.938>.
- [8] Gordon, D. M. Discrete logarithms in  $gf(p)$  using the number field sieve / Daniel M. Gordon // SIAM J. Discrete Math. — 1993. — Vol. 6. — P. 124–138.
- [9] Grover, L. K. A fast quantum mechanical algorithm for database search / Lov K. Grover // ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING. — ACM, 1996. — P. 212–219.

- [10] Hartle, J. B. Wave function of the universe / J. B. Hartle, S. W. Hawking // Phys. Rev. D. — 1983. — Dec. — Vol. 28. — P. 2960–2975. — <https://link.aps.org/doi/10.1103/PhysRevD.28.2960>.
- [11] Hopcroft, J. E. Introduction to Automata Theory, Languages, and Computation (3rd Edition) / John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman. — Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2006.
- [12] Immanuel Bloch. Introduction to Quantum Optics. — <https://class.coursera.org/qoptintro-001>. — 2016. — [Online; accessed 23-February-2016].
- [13] Ivan Murashko. Analyze of quantum fourier transform circuit implementation / Ivan Murashko, Constantine Korikov // Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 15th International Conference, NEW2AN 2015, and 8th Conference, ruSMART 2015, St. Petersburg, Russia, August 26-28, 2015, Proceedings / Ed. by Sergey Balandin, Sergey D. Andreev, Yevgeni Koucheryavy. — Springer, 2015. — Vol. 9247 of Lecture Notes in Computer Science. — <http://dx.doi.org/10.1007/978-3-319-23126-6>.
- [14] Kim, Y.-H. Quantum teleportation with a complete bell state measurement / Yoon-Ho Kim, Sergei P. Kulik, Yanhua Shih // Phys. Rev. Lett. — 2001. — Vol. 86, no. 7. — P. 1370–1373. — <http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0010046>.
- [15] Lamb, W. E. Anti-photon / W. E. Lamb // Applied Physics B. — 1995. — Vol. 60, no. 2. — P. 77–84. — <http://dx.doi.org/10.1007/BF01135846>.
- [16] Nielsen, M. Quantum Computation and Quantum Information / M.A. Nielsen, I.L. Chuang. Cambridge Series on Information and the Natural Sciences. — Cambridge University Press, 2000. — <http://books.google.ru/books?id=65FqEKQOfP8C>.
- [17] Proos, J. Shor's discrete logarithm quantum algorithm for elliptic curves / John Proos, Christof Zalka // Quantum Info. Comput. — 2003. — Jul. — Vol. 3, no. 4. — P. 317–344. — <https://arxiv.org/abs/quant-ph/0301141>.
- [18] Schoof, R. J. Elliptic curves over finite fields and the computation of square roots mod  $p$  / René J. Schoof // Mathematics of Computation. — 1985. — Vol. 44. — P. 483–494. — URL: <http://cr.yp.to/bib/entries.html#1985/schoof>.



- [19] Seeing a single photon without destroying it / G. Nogues, A. Rauschenbeutel, S. Osnaghi et al. // Nature. — 1999. — Vol. 400. — P. 239–242.
- [20] Shannon, C. E. A mathematical theory of communication / C. E. Shannon // Bell system technical journal. — 1948. — Vol. 27. — P. 379–423, 623–656.
- [21] Shannon, C. E. Communication Theory of Secrecy Systems / Claude E. Shannon // Bell Systems Technical Journal. — 1949. — Vol. 28. — P. 656–715.
- [22] Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring / Peter W. Shor // FOCS. — IEEE Computer Society, 1994. — P. 124–134.
- [23] Strengths and weaknesses of quantum computing / Charles H. Bennett, Ethan Bernstein, Gilles Brassard, Umesh Vazirani // SIAM J. Comput. — 1997. — oct. — Vol. 26, no. 5. — P. 1510–1523. — <http://dx.doi.org/10.1137/S0097539796300933>.
- [24] Washington, L. C. Elliptic Curves: Number Theory and Cryptography, Second Edition / Lawrence C. Washington. — 2 edition. — Chapman & Hall/CRC, 2008.
- [25] Wikipedia. Дискретное логарифмирование — Wikipedia, The free encyclopedia. — [http://ru.wikipedia.org/wiki/Дискретное\\_логарифмирование](http://ru.wikipedia.org/wiki/Дискретное_логарифмирование). — 2013. — [Online; accessed 29-October-2013].
- [26] Wikipedia. Autler–townes effect — wikipedia, the free encyclopedia. — "2017". — [Online; accessed 17-April-2017]. [https://en.wikipedia.org/w/index.php?title=Autler-Townes\\_effect&oldid=763887291](https://en.wikipedia.org/w/index.php?title=Autler-Townes_effect&oldid=763887291).
- [27] Wootters, W. K. A single quantum cannot be cloned / W. K. Wootters, W. H. Zurek // Nature. — 1982. — October. — Vol. 299, no. 5886. — P. 802–803. — <http://dx.doi.org/10.1038/299802a0>.
- [28] Yamamoto, Y. Preparation, measurement and information capacity of optical quantum states / Y. Yamamoto, H. A. Haus // Rev. Mod. Phys. — 1986. — Oct. — Vol. 58, no. 4. — P. 1001–1020.
- [29] Zurek, W. H. Decoherence and the transition from quantum to classical—revisited / W. H. Zurek // Los Alamos Science. — 2002. — no. 27. — P. 2–25. — <http://vukuz.ru/books/zurek.pdf>.

- [30] А. М. Яглом. Вероятность и информация / А. М. Яглом, И. М. Яглом. — Москва: Наука, 1973. — С. 512.
- [31] А. Н. Колмогоров. Основные понятия теории вероятностей / А. Н. Колмогоров. — Москва: Наука, 1974.
- [32] Александр Семенович Холево. Вероятностные и статистические аспекты квантовой теории / Александр Семенович Холево. — Москва, Ижевск: Институт компьютерных исследований, 2003. — С. 410.
- [33] Александр Семенович Холево. Статистическая структура квантовой теории / Александр Семенович Холево. — Москва, Ижевск: Институт компьютерных исследований, 2003. — С. 192.
- [34] Александр Семенович Холево. Математические основы квантовой информатики / Александр Семенович Холево. — Москва, 2016. — С. 125. — <http://www.rqc.ru/education/lecture-courses/holevo-mathematical-fundamentals-of-quantum-informatics/Holevo22.pdf>.
- [35] Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. — Москва: Триумф, 2002. — С. 816.
- [36] В. А. Ильин. Линейная алгебра / В. А. Ильин, Э. Г. Поздняк. — 6 изд. — Москва: Физматлит, 2005. — С. 115.
- [37] В. В. Белокуров. Квантовая телепортация - обыкновенное чудо / В. В. Белокуров, О. Д. Тимофеевская, О. А. Хрусталева. — Ижевск: НИЦ Регулярная и хаотическая динамика, 2000. — С. 256.
- [38] В. Л. Гинзбург. Теоретическая физика и астрофизика / В. Л. Гинзбург. — Москва: Наука, 1981.
- [39] В. П. Быков. Лазерная электродинамика / В. П. Быков. — Москва: Физматлит, 2006. — С. 384.
- [40] "Википедия". "Дельта-функция — Википедия, свободная энциклопедия". — "2019". — "<https://ru.wikipedia.org/?oldid=99318415>".
- [41] "Википедия". "Преобразование Фурье — Википедия, свободная энциклопедия". — "2019". — "<https://ru.wikipedia.org/?oldid=99860150>".
- [42] Г. Б. Двайт. Таблицы интегралов и другие математические формулы / Г. Б. Двайт. — Москва: Наука, 1973. — С. 228.

- [43] Г. Хакен. Лазерная светодинамика / Г. Хакен. — Москва: Мир, 1988.
- [44] Д. Н. Клышко. Основные понятия квантовой физики с операциональной точки зрения / Д. Н. Клышко // УФН. — 1998. — Vol. 168, no. 9. — P. 975–1015.
- [45] Д. Ф. Смирнов. Новые явления в квантовой оптике: антигруппировка и субпуассоновская статистика фотонов, сжатые состояния / Д. Ф. Смирнов, А. С. Трошин // УФН. — 1987. — Vol. 153, no. 2.
- [46] Дж. Клаудер. Основы квантовой оптики / Дж. Клаудер, Э. Судершан. — Москва: Мир, 1970. — С. 428.
- [47] Карлов, Н.В. Колебания, волны, структуры / Карлов, Н.В., Кириченко, Н.А. — Физматлит, 2003. — Р. 496.
- [48] Квантовая оптика и квантовая радиофизика / Р. Глаубер, У. Лэмб, Н. Кролль, Ж. Вантер. — Москва: Мир, 1966. — С. 452.
- [49] Квантовая теория лазера - проблема неравновесной статистической механики. Квантовые флуктуации излучения лазера / Ф. Арекки, М. Скалли, Г. Хакен, В. Вайдлих. — Москва: Мир, 1974.
- [50] Л. Мандель. Оптическая когерентность и квантовая оптика / Л. Мандель, Э. Вольф. — Москва: Наука. ФИЗМАТЛИТ, 2000. — С. 896.
- [51] Лев Васильевич Тарасов. Введение в квантовую оптику / Лев Васильевич Тарасов. — 2 изд. — Москва: ЛКИ, 2008. — С. 304.
- [52] М. Лэкс. Флуктуации и когерентные явления / М. Лэкс. — Мир: Наука, 1974.
- [53] М. О. Скалли. Квантовая оптика / М. О. Скалли, М. С. Зубайри. — Москва: Физматлит, 2003. — С. 512.
- [54] Михаил Борисович Менский. Квантовые измерения и декогеренция. Модели и феноменология / Михаил Борисович Менский. — Москва: Физматлит, 2001. — С. 228.
- [55] Николай Константинович Верещагин. Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств / Николай Константинович Верещагин, Александр Шень. — 4 изд. — Москва: МЦНМО, 2012. — С. 112. — <ftp://ftp.mccme.ru/users/shen/logic/sets/part1.pdf>.

- [56] Поль Дирак. Принципы квантовой механики / Поль Дирак. — Москва: Наука, 1979.
- [57] Р. Лоудон. Квантовая теория света / Р. Лоудон. — Москва: Мир, 1976.
- [58] Р. Фейнман. Фейнмановские лекции по физике (вып. 8, 9). Квантовая механика / Р. Фейнман, Р. Лейтон, М. Сэндс. — Москва: Мир, 1978. — С. 525.
- [59] С. А. Ахманов. Физическая оптика / С. А. Ахманов, С. Ю. Никитин. — 2 изд. — Москва: МГУ, Наука, 2004. — С. 656.
- [60] С. Я. Килин. Квантовая оптика. Поля и их детектирование / С. Я. Килин. — 2 изд. — Москва: Едиториал УРСС, 2003. — С. 176.
- [61] Уильям Люиселл. Излучение и шумы в квантовой электронике / Уильям Люиселл. — Москва: Наука, 1972.
- [62] Физика квантовой информации / Под ред. А. Цайлингера. — Москва: Постмаркет, 2002. — С. 376.