



## Формализм базиса Паули в квантовых вычислениях

В. В. Никонов<sup>a</sup> and А. Н. Цирулёв<sup>b</sup>

Факультет математики, Тверской государственный университет, Садовый пер. 35, Тверь,  
Россия

**e-mail:** <sup>a</sup> nikonov.vv@tversu.ru <sup>b</sup> tsirulev.an@tversu.ru

*Получено 1 декабря 2020, в окончательной форме 28 декабря. Опубликовано 30 декабря 2020.*

**Abstract.** Эта статья посвящена квантовым вычислениям в базисе Паули, элементы которого обычно отождествляются со строками Паули. Этот подход позволяет представлять квантовые состояния, наблюдаемые величины и унитарные операторы в единой форме линейной комбинации строк Паули, так что все операции могут быть сведены к композициям строк. Тем не менее, формальное обоснование использования базиса Паули для квантовых вычислений должно основываться на сильных результатах комплексной линейной алгебры и теории гильбертовых пространств. Мы кратко рассматриваем основные особенности строк Паули для квантовых состояний и унитарных операторов, а также ключевые операции с ними, включая алгоритм для композиций строк и алгоритм преобразования из стандартного базиса в базис Паули.

**Keywords:** квантовые вычисления, базис Паули

**MSC numbers:** 81P16, 81P68

## 1. Введение

Теория квантовых вычислений остается в центре внимания на протяжении последних двух десятилетий. Различные типы и подтипы квантовых вычислений адаптированы для различных технологий и архитектур аппаратного обеспечения, но их математические структуры построены с использованием одних и тех же основных понятий гильбертова пространства, квантовой наблюдаемой величины, унитарного оператора и квантового состояния. В этой статье мы рассматриваем взаимодействующую составную квантовую систему, состоящую из  $n$  идентичных двухуровневых подсистем (кубитов), так что размерность соответствующего гильбертова пространства равна  $2^n$ . Квантовое вычисление в чистом состоянии с числом вентилей, которое полиномиально зависит от числа кубитов, может быть эффективно смоделировано классически. Поскольку универсальный квантовый компьютер, демонстрирующий квантовое превосходство, должен иметь большое количество кубитов, скажем,  $n \geq 1000$ , число базисных состояний составляет  $2^n > 10^{300}$ . Квантовые компьютеры с малым числом кубитов ( $n \sim 100$ ), которые будут доступны в ближайшее время, должны использоваться вместе с классическим компьютером. В обоих случаях многокубитные квантовые вычисления очень чувствительны к выбору вычислительного базиса [1, 2, 3].

Существует два общих варианта выбора базиса, и какой из них более эффективен, зависит как от данного алгоритма, так и от конкретного типа квантового компьютера. Во-первых, мы можем использовать стандартный ортонормированный базис в гильбертовом пространстве и затем построить подходящий базис в алгебре линейных операторов. Однако этот подход оказывается неудобным и неестественным при рассмотрении задач, связанных со смешанными состояниями, графовыми состояниями [4], коррекцией ошибок [3, 5, 6], тензорными сетями [7, 8, 9] и более общими вопросами, где измерения не являются проективными [10, 11, 12]. Второй вариант напрямую работает с базисом в алгебре операторов, и в этом случае элементы базиса обычно не могут быть разложены в тензорное произведение некоторых кет и бра векторов; базис Паули считается наилучшим выбором, поскольку он эрмитов, ортонормирован (по отношению к внутреннему произведению Гильберта-Шмидта) и составляет ортонормированный базис в алгебре Ли соответствующей унитарной группы. Группа Клиффорда, имеющая многочисленные применения в квантовых вычислениях, наиболее просто описывается в терминах базиса Паули [10, 14].

Основная цель этой статьи — дать систематический алгебраический обзор многокубитных систем в базисе Паули. Статья организована следующим образом. Раздел 2 содержит некоторые необходимые математические предварительные сведения. В разделе 3 мы даем краткое описание квантовых состояний для  $n$ -кубитовой квантовой системы в базисе Паули. Раздел 4 посвящен изучению некоторых вычислительных свойств строк Паули. В разделе 5 мы рассматриваем алгоритмы вычислений, предназначенные для перехода от стандартного

базиса к базису Паули.

На протяжении всей статьи мы используем естественные единицы с  $\hbar = c = 1$ . Для удобочитаемости некоторые обозначения сделаны контекстно-зависимыми: строчные латинские буквы в двоичных строках (например, в символах бра и кет) принимают значения 0 и 1, тогда как в строках Паули и индексах они принимают значения от 0 до 3.

## 2. Основные особенности базиса Паули

Мы будем рассматривать квантовую систему из  $n$  различных кубитов, где кубит ассоциируется с двумерным гильбертовым пространством  $\mathcal{H}$  и его двойственным (эрмитово сопряженным) пространством  $\mathcal{H}^\dagger$ . Пусть  $\mathcal{H}_n = \mathcal{H}^{\otimes n}$  и  $\mathcal{H}_n^\dagger = (\mathcal{H}^\dagger)^{\otimes n}$  — гильбертово пространство системы и его двойственное пространство соответственно, и пусть  $L(\mathcal{H}_n) = \mathcal{H}_n \otimes \mathcal{H}_n^\dagger$  — пространство линейных операторов, действующих на  $\mathcal{H}$  и  $\mathcal{H}^\dagger$  слева и справа соответственно. Тогда

$$\dim_{\mathbb{C}} \mathcal{H}_n = \dim_{\mathbb{C}} \mathcal{H}_n^\dagger = 2^n, \quad \dim_{\mathbb{C}} L(\mathcal{H}_n) = 2^{2n}.$$

Мы также будем предполагать, что пространство  $L(\mathcal{H}_n)$  оснащено внутренним произведением Гильберта-Шмидта,

$$\langle \hat{A}, \hat{B} \rangle = \text{tr}(\hat{A}^\dagger \hat{B}), \quad \hat{A}, \hat{B} \in L(\mathcal{H}_n), \quad (1)$$

которое является естественным расширением внутреннего произведения в  $\mathcal{H}_n$ . Реальное линейное пространство эрмитовых операторов обозначается далее как  $H(\mathcal{H}_n)$ .

Пусть  $\{|0\rangle, |1\rangle\}$  — ортонормированный базис в некотором одномерном кубитовом пространстве  $\mathcal{H}$ . Единичная матрица и матрицы Паули,

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

определяют четыре оператора Паули

$$\begin{aligned} \hat{\sigma}_0 &= |0\rangle\langle 0| + |1\rangle\langle 1|, & \hat{\sigma}_1 &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ \hat{\sigma}_2 &= -i|0\rangle\langle 1| + i|1\rangle\langle 0|, & \hat{\sigma}_3 &= |0\rangle\langle 0| - |1\rangle\langle 1|, \end{aligned}$$

которые являются эрмитовыми и унитарными одновременно и которые образуют базис в  $L(\mathcal{H})$ . Обратное преобразование задается

$$|0\rangle\langle 0| = \frac{\hat{\sigma}_0 + \hat{\sigma}_3}{2}, \quad |0\rangle\langle 1| = \frac{\hat{\sigma}_1 + i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 0| = \frac{\hat{\sigma}_1 - i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 1| = \frac{\hat{\sigma}_0 - \hat{\sigma}_3}{2}.$$

Напомним, что для  $k, l, m \in \{1, 2, 3\}$  имеем  $\text{tr} \hat{\sigma}_k = 0$ ,  $\hat{\sigma}_k^2 = \hat{\sigma}_0$ , и

$$\hat{\sigma}_k \hat{\sigma}_l = -\hat{\sigma}_l \hat{\sigma}_k, \quad \hat{\sigma}_k \hat{\sigma}_l = i \text{sign}(\pi) \hat{\sigma}_m, \quad (klm) = \pi(123), \quad (2)$$

где  $\pi(123)$  — это перестановка множества  $\{1, 2, 3\}$ .

Существует *стандартный*<sup>1</sup> двоичный базис в  $\mathcal{H}_n$ , который генерируется ортонормированными базисами  $\{|0\rangle, |1\rangle\}$  в соответствующих одномерных кубитовых пространствах. Математически позиция в тензорном произведении различает кубиты друг от друга. Поэтому для фиксированного  $n$  удобно записывать элемент этого базиса и соответствующий элемент двойственного базиса в виде

$$|k\rangle = |k_1 \dots k_n\rangle = |k_1\rangle \otimes \dots \otimes |k_n\rangle, \quad \langle k| = \langle k_1 \dots k_n| = \langle k_1| \otimes \dots \otimes \langle k_n|,$$

рассматривая строки  $k_1 \dots k_n$  ( $k_1, \dots, k_n \in \{0, 1\}$ ) как двоичное число и обозначая его десятичным представлением  $k$ . Например,  $|101\rangle = |5\rangle$  и  $|00110\rangle = |6\rangle$

В стандартном базисе,

$$|u\rangle = \sum_{k=0}^{2^n-1} u_k |k\rangle, \quad \hat{A} = \sum_{k,l=0}^{2^n-1} a_{kl} |k\rangle \langle l|,$$

где  $|u\rangle \in \mathcal{H}_n$  и  $\hat{A} \in L(\mathcal{H}_n)$ .

Базис Паули  $P(\mathcal{H}_n)$  в  $L(\mathcal{H}_n)$  определяется как

$$\{\hat{\sigma}_{k_1 \dots k_n}\}_{k_1, \dots, k_n \in \{0, 1, 2, 3\}}, \quad \hat{\sigma}_{k_1 \dots k_n} = \hat{\sigma}_{k_1} \otimes \dots \otimes \hat{\sigma}_{k_n}, \quad (3)$$

где  $\hat{\sigma}_{0 \dots 0}$  — единичный оператор. Очевидно, что  $P(\mathcal{H}_n)$  состоит из  $4^n$  элементов. Мы будем использовать компактные обозначения, такие как

$$\hat{\sigma}_K = \hat{\sigma}_{k_1 \dots k_n},$$

обозначая *строку Паули*  $k_1 \dots k_n$ , где  $k_1, \dots, k_n \in \{0, 1, 2, 3\}$ , соответствующей заглавной буквой  $K$ . При этом мы будем часто рассматривать  $K$  как число, то есть как десятичное представление строки; очевидно, что  $0 \leq K \leq 4^n - 1$ . Заметим, что строка Паули  $K$  и элемент  $\hat{\sigma}_K$  базиса Паули полностью определяют друг друга и, следовательно, могут быть отождествлены. Например, элементы стандартного базиса выражаются через элементы базиса Паули в Приложении A1 на странице 13.

Полезно сравнить  $P(\mathcal{H}_n)$  со стандартным базисом. Мы имеем

$$\hat{\sigma}_{k_1 \dots k_n} \hat{\sigma}_{k_1 \dots k_n} = \hat{\sigma}_{0 \dots 0}, \quad \text{tr } \hat{\sigma}_{0 \dots 0} = 2^n, \quad \text{tr } \hat{\sigma}_{k_1 \dots k_n} \big|_{k_1 \dots k_n \neq 0 \dots 0} = 0. \quad (4)$$

Базис Паули является эрмитовым, унитарным и ортогональным по отношению к внутреннему произведению (1). Заметим, что оператор  $|k\rangle \langle l|$  стандартного базиса не является унитарным и не является эрмитовым, если  $k \neq l$ . Стандартный

<sup>1</sup>Мы не используем обычный термин "вычислительный" так как он может привести к путанице. Базис Паули и стандартный базис вычислительны в одном и том же смысле.

базис не содержит единичного оператора, который имеет вид

$$\sum_{k=0}^{2^n-1} |k\rangle\langle k|$$

в этом базисе. В базисе Паули любой оператор  $\hat{U}$  из унитарной группы  $U(\mathcal{H}_n)$  (то есть  $\hat{U}^\dagger \hat{U} = \hat{\sigma}_{0\dots 0}$ ) имеет разложение в виде

$$\hat{U} = \sum_{i_1, \dots, i_n \in \{0,1,2,3\}} U_{i_1 \dots i_n} \hat{\sigma}_{i_1 \dots i_n}, \quad \hat{U}^\dagger = \sum_{i_1, \dots, i_n \in \{0,1,2,3\}} \bar{U}_{i_1 \dots i_n} \hat{\sigma}_{i_1 \dots i_n},$$

где

$$\sum_{i_1, \dots, i_n \in \{0,1,2,3\}} \bar{U}_{i_1 \dots i_n} U_{i_1 \dots i_n} = 1, \quad \sum_{\substack{i_1, \dots, i_n, j_1, \dots, j_n \in \{0,1,2,3\} \\ (i_1, \dots, i_n) \neq (j_1, \dots, j_n)}} \bar{U}_{i_1 \dots i_n} U_{j_1 \dots j_n} = 0.$$

Заметим, что последнее условие может быть очевидно разложено на  $2^{2n-1}(2^n - 1)$  независимых условий.

### 3. Квантовые состояния в базисе Паули

Квантовое состояние (оператор плотности) — это эрмитов, положительно полуопределённый (или просто положительный) оператор вида

$$\hat{\rho} = \frac{1}{2^n} \sum_{k_1, \dots, k_n \in \{0,1,2,3\}} a_{k_1 \dots k_n} \hat{\sigma}_{k_1 \dots k_n} \equiv \frac{1}{2^n} \sum_{K=0}^{4^n-1} a_K \hat{\sigma}_K, \quad (5)$$

где  $a_{k_1 \dots k_n} \in \mathbb{R}$  и

$$a_{0\dots 0} = 1, \quad |a_{k_1 \dots k_n}| \leq 1, \quad \sum_{k_1, \dots, k_n \in \{0,1,2,3\}} (a_{k_1 \dots k_n})^2 \leq 2^n. \quad (6)$$

Условия (6) гарантируют, что  $\hat{\rho}^\dagger = \hat{\rho}$ ,  $\text{tr} \hat{\rho} = 1$ , и  $\text{tr} \hat{\rho}^2 \leq 1$ . Для квантовых вычислений важно, что все коэффициенты в состоянии (5) являются действительными, и каждый из них, кроме  $a_{0\dots 0}$ , точно является результатом местного измерения с одним из базисных операторов (3),  $a_K \equiv a_{k_1 \dots k_n} = \text{tr}(\hat{\rho} \hat{\sigma}_{k_1 \dots k_n})$ . Все квантовые (чистые и смешанные) состояния образуют выпуклое множество (замкнутое многообразие, поскольку оно является прообразом 1 при отображении  $\text{tr} : H(\mathcal{H}_n) \rightarrow \mathbb{R}$ ) реальной размерности  $4^n - 1$  в реальном линейном многообразии  $\mathcal{S}_n \subset \text{Span}\{P(\mathcal{H}_n)\} = H(\mathcal{H}_n)$ , в то время как чистые состояния располагаются на границе  $\mathcal{S}_n$  и составляют реальное подмногообразие размерности  $2^{n+1} - 2$ .

Каждый элемент  $P(\mathcal{H}_n)$  является идемпотентом ( $\hat{\sigma}_K \hat{\sigma}_K = \hat{\sigma}_{0\dots 0}$ ), так что операторы

$$\hat{P}_K^\pm = \frac{\hat{\sigma}_{0\dots 0} \pm \hat{\sigma}_K}{2}$$

являются проекторами. Таким образом, наблюдаемая величина  $\hat{\sigma}_K = \hat{P}^+ - \hat{P}^-$  естественно сводится к проективным измерениям. Используя операторы  $\hat{P}_K^\pm$ , мы теперь можем доказать следующее практически важное утверждение, которое, по-видимому, не было рассмотрено в, по крайней мере, текущей литературе.

**Proposition 1.** *Условие  $|a_{k_1\dots k_n}| \leq 1$  в (6) следует из положительности оператора плотности (5) и первого условия в (6).*

Заметим, что эрмитовы проекторы  $\hat{P}_K^\pm = \hat{P}_K^\pm \hat{P}_K^\pm = (\hat{P}_K^\pm)^\dagger \hat{P}_K^\pm$  являются положительными операторами, так как очевидны неравенства

$$\langle u | \hat{P}_K^\pm | u \rangle = \langle u | (\hat{P}_K^\pm)^\dagger \hat{P}_K^\pm | u \rangle \geq 0.$$

В общем случае эрмитов оператор  $\hat{A} \in L(\mathcal{H}_n)$  является положительным тогда и только тогда, когда существует некоторый оператор  $\hat{B} \in L(\mathcal{H}_n)$  такой, что  $\hat{A} = \hat{B} \hat{B}^\dagger$ ; более того,  $\hat{B}$  может быть выбрано эрмитовым [15]. Это, в свою очередь, подразумевает, что ( $\hat{A}$  и  $\hat{\rho}$  положительны)

$$\text{tr}(\hat{A} \hat{\rho}) = \text{tr}(\hat{B} \hat{B}^\dagger \hat{\rho}) = \text{tr}(\hat{B}^\dagger \hat{\rho} \hat{B}) \geq 0,$$

так как  $\hat{B}^\dagger \hat{\rho} \hat{B}$ , очевидно, положителен. Таким образом,

$$\text{tr}(\hat{P}_K^\pm \hat{\rho}) = \frac{1 \pm a_K}{2} \geq 0, \quad (7)$$

так что  $-1 \leq a_K \leq 1$ . Доказательство завершено.  $\square$

В качестве примера запишем одно из практически полезных состояний в стандартном базисе и в базисе Паули, а именно трехкубитное состояние Гринбергера-Хорна-Зейлингера. Используя оператор  $CNOT$  и оператор Адамара  $\hat{U}_2^+$ , которые определены соотношениями (13) и (14) в Приложении А2, мы можем записать унитарное преобразование начального состояния  $|000\rangle$  в состояние  $\text{GHZ}_3$  в виде

$$\hat{U}_{\text{GHZ}_3} = (\hat{\sigma}_0 \otimes CNOT) \circ (CNOT \otimes \hat{\sigma}_0) \circ (\hat{U}_2^+ \otimes \hat{\sigma}_{00}),$$

из которого легко найти

$$\begin{aligned} \hat{\rho}_{\text{GHZ}_3} &= \frac{1}{2}(|000\rangle\langle 000| + |000\rangle\langle 111| + |111\rangle\langle 000| + |111\rangle\langle 111|) \\ &= \frac{1}{8}(\hat{\sigma}_{000} + \hat{\sigma}_{111} - \hat{\sigma}_{122} - \hat{\sigma}_{212} - \hat{\sigma}_{221} + \hat{\sigma}_{033} + \hat{\sigma}_{303} + \hat{\sigma}_{330}). \end{aligned}$$

## 4. Операции со строками Паули

Нам понадобится несколько фактов и определений, связанных с базисом Паули и множеством строк Паули длины  $n$ ,

$$\text{Str}_n = \{K = k_1 \dots k_n\}_{k_1, \dots, k_n \in \{0,1,2,3\}}.$$

Во-первых, рассмотрим множество  $\mathbb{F}_4 = \{0, 1, 2, 3\}$  как группу Клейна с правилами умножения

$$0*k = k, \quad k*k = 0, \quad k*l = m,$$

где  $k, l, m \in \{1, 2, 3\}$  и  $klm$  — любая перестановка 123. Во-вторых, пусть функция  $s : \mathbb{F}_4 \times \mathbb{F}_4 \rightarrow \{1, i, -i\}$  определяется своими значениями

$$\begin{aligned} s(0, 0) = s(0, k) = s(k, 0) = s(k, k) = 1, \quad k = 1, 2, 3, \\ s(1, 2) = s(2, 3) = s(3, 1) = i, \quad s(2, 1) = s(3, 2) = s(1, 3) = -i. \end{aligned}$$

Далее, пусть функция  $S : \text{Str}_n \times \text{Str}_n \rightarrow \{1, -1, i, -i\}$ ,  $(K, L) \mapsto S_{KL}$ , определяется как произведение

$$S_{KL} = s(k_1, l_1)s(k_2, l_2) \dots s(k_n, l_n), \quad K = k_1 k_2 \dots k_n, \quad L = l_1 l_2 \dots l_n.$$

Функция  $S$  симметрична или антисимметрична в зависимости от количества пар  $(k_r, l_r)$  ( $r$  — позиция в строках  $K$  и  $L$ ) таких, что  $k_r, l_r \in \{1, 2, 3\}$  и  $k_r \neq l_r$ , а также в зависимости от их взаимного порядка. Пусть  $w_{KL}^+$  и  $w_{KL}^-$  обозначают количество пар видов (1, 2), (2, 3), (3, 1) и видов (2, 1), (3, 2), (1, 3) соответственно, а  $w_{KL} = w_{KL}^+ + w_{KL}^-$ . Тогда

$$S_{KL} = (i)^{w_{KL}} (-1)^{w_{KL}^-}, \quad S_{(KL)} = \frac{S_{KL}}{2} (1 + (-1)^{w_{KL}}), \quad S_{[KL]} = \frac{S_{KL}}{2} (1 - (-1)^{w_{KL}}), \quad (8)$$

где круглые и квадратные скобки обозначают симметризацию и антисимметризацию, соответственно. Значения  $S_{KL}$ ,  $S_{(KL)}$ , и  $S_{[KL]}$  приведены в Таблице 2.

|                    |   |   |    |    |     |     |      |      |
|--------------------|---|---|----|----|-----|-----|------|------|
| $w_{KL} \bmod 4$   | 0 | 2 | 0  | 2  | 1   | 3   | 1    | 3    |
| $w_{KL}^- \bmod 2$ | 0 | 1 | 1  | 0  | 0   | 1   | 1    | 0    |
| $S_{KL}$           | 1 | 1 | -1 | -1 | $i$ | $i$ | $-i$ | $-i$ |
| $S_{(KL)}$         | 1 | 1 | -1 | -1 | 0   | 0   | 0    | 0    |
| $S_{[KL]}$         | 0 | 0 | 0  | 0  | $i$ | $i$ | $-i$ | $-i$ |

Таблица 1: Коэффициенты перед  $\hat{\sigma}_M$  в (9) для  $\hat{\sigma}_K \hat{\sigma}_L$ ,  $\{\hat{\sigma}_K, \hat{\sigma}_L\}$  и  $[i\hat{\sigma}_K, i\hat{\sigma}_L]$ .

Теперь композицию двух элементов базиса Паули и их антикоммутатор и коммутатор можно записать в виде компактных выражений, удобных для программирования на классическом компьютере:

$$\hat{\sigma}_K \hat{\sigma}_L = S_{KL} \hat{\sigma}_M, \quad \{\hat{\sigma}_K, \hat{\sigma}_L\} = S_{(KL)} \hat{\sigma}_M, \quad [i\hat{\sigma}_K, i\hat{\sigma}_L] = -S_{[KL]} \hat{\sigma}_M, \quad (9)$$

где

$$\hat{\sigma}_M = \hat{\sigma}_{m_1 \dots m_n}, \quad m_1 = k_1 * l_1, \dots, m_n = k_n * l_n. \quad (10)$$

Заметим, что две строки Паули длины  $n$  могут коммутировать, даже если у них есть различные ненулевые элементы в некоторых одинаковых позициях. Например, три оператора  $\hat{\sigma}_{11}$ ,  $\hat{\sigma}_{22}$  и  $\hat{\sigma}_{33}$  взаимно коммутируют. Также легко заметить, что унитарная матрица перехода, преобразующая стандартный базис  $\{|i_1 \dots i_n\rangle\langle j_1 \dots j_n|\}$  в базис Паули, состоит только из элементов  $0$ ,  $\pm 1$  и  $\pm i$ . В частности,

$$|00 \dots 0\rangle\langle 00 \dots 0| \rightarrow \frac{1}{2^n} \sum_{i_1, \dots, i_n \in \{0,3\}} \hat{\sigma}_{i_1 \dots i_n}.$$

Более общо, стандартные ортогональные проекторы могут быть выражены как

$$|i_1 \dots i_n\rangle\langle i_1 \dots i_n|_{i_1, \dots, i_n \in \{0,1\}} = \frac{1}{2^n} \sum_{k_1, \dots, k_n \in \{0,3\}} \chi_{k_1}^{i_1} \dots \chi_{k_n}^{i_n} \hat{\sigma}_{k_1 \dots k_n},$$

где

$$\chi_0^0 = \chi_3^0 = \chi_0^1 = 1, \quad \chi_3^1 = -1.$$

Некоторые важные операторы в базисе Паули приведены в Приложении А2 на странице 15.

Выражения (9) показывают, во-первых, что множество  $\{i\hat{\sigma}_K\}_{K=0}^{4^n-1}$  образует ортонормированный базис в  $\mathfrak{su}(n)$ . И, во-вторых, множество

$$\tilde{P}(\mathcal{H}_n) = \{\epsilon \hat{\sigma}_K \mid K \in \text{Str}_n, \epsilon \in \{\pm 1, \pm i\}\},$$

состоящее из  $4^{n+1}$  элементов, является группой; она называется Паули-группой ( $n$ -кубитовой). Нормализатор Паули-группы,

$$\mathcal{C}(\mathcal{H}_n) = \{\hat{U} \in U(\mathcal{H}_n) \mid \hat{U} \hat{\sigma}_K \hat{U}^\dagger \in \tilde{P}(\mathcal{H}_n), \hat{\sigma}_K \in \tilde{P}(\mathcal{H}_n)\},$$

называется группой Клиффорда. Из 2, 4, и 10 имеем следующее утверждение:

**Proposition 2.** *Взаимные унитарные преобразования операторов базиса Паули подчиняются соотношениям  $\hat{\sigma}_{i_1 \dots i_n} \hat{\sigma}_{k_1 \dots k_n} \hat{\sigma}_{i_1 \dots i_n} = \pm \hat{\sigma}_{i_1 \dots i_n}$ , где плюс берется только в том случае, если число троек  $(i_m k_m i_m)_{m \in \{1, \dots, n\}}$ , удовлетворяющих условиям  $i_m \neq k_m$ ,  $i_m \neq 0$ , и  $k_m \neq 0$ , четно.*

## 5. Алгоритмы перехода к базису Паули

В стандартном базисе и в базисе Паули оператор  $\hat{A} \in L(\mathcal{H}_n)$  (например, унитарное преобразование, наблюдаемая величина или оператор плотности) можно



выразить как

$$\begin{aligned}\hat{A} &= \sum_{i_0, \dots, i_{n-1}, j_0, \dots, j_{n-1} \in \{0,1\}} a_{i_{n-1} \dots i_0 j_{n-1} \dots j_0} |i_{n-1} \dots i_0\rangle \langle j_{n-1} \dots j_0| \\ &= \frac{1}{2^n} \sum_{i_0, \dots, i_{n-1} \in \{0,1,2,3\}} s_{i_{n-1} \dots i_0} \hat{\sigma}_{i_{n-1} \dots i_0},\end{aligned}$$

или, коротко,

$$\hat{A} = \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} a_{ij} |i\rangle \langle j| = \frac{1}{2^n} \sum_{I=0}^{4^n-1} S_I \hat{\sigma}_I. \quad (11)$$

Таким образом, мы имеем дело с задачей вычисления коэффициентов  $S_I$ , когда заданы коэффициенты  $a_i$ ; такой алгоритм недавно был предложен [13]. Наш подход основан на следующем наблюдении: все коэффициенты  $a_{ij}$  с двоичными строками  $i = i_{n-1} \dots i_0$  и  $j = j_{n-1} \dots j_0$ , которые имеют одну и ту же сумму

$$k = (k_{n-1} \dots k_0)_2 = (i_{n-1} \dots i_0)_2 \oplus (j_{n-1} \dots j_0)_2,$$

дают ненулевые вклады только в термины вида  $S_l^{(i \oplus j)} \hat{\sigma}_l$ , где  $l$  — двоичная строка  $l_{n-1} \dots l_0$ ,  $0 \leq l \leq 2^n - 1$ , и операторы  $\hat{\sigma}_l$  должны быть пересчитаны в форме (11). Прямолинейно (но громоздко) доказать, что строки  $I = I(k, l) = [I_0^{(k)}, \dots, I_{2^n-1}^{(k)}]_4$ ,  $k = i \oplus j$ , в  $\hat{\sigma}_I$  определяются

$$I = \bar{l} \wedge k + 2(l \wedge k) + 3(l \wedge \bar{k}), \quad (12)$$

где черта над буквой обозначает инверсию  $0 \leftrightarrow 1$  для каждого символа соответствующей двоичной строки, а  $\wedge$  обозначает логическую операцию И. На правой стороне в (12) мы рассматриваем результирующие двоичные строки как числа в четверичной системе. Для заданных двоичных строк  $i$  и  $j$  псевдокод этой процедуры приведен в Алгоритме 1.

Например, слагаемые

$$a_{010,001} |010\rangle \langle 001| = \frac{a_{21}}{2^3} (\hat{\sigma}_{011} + i\hat{\sigma}_{012} - i\hat{\sigma}_{021} + \hat{\sigma}_{022} + \hat{\sigma}_{311} + i\hat{\sigma}_{312} - i\hat{\sigma}_{321} + \hat{\sigma}_{322}),$$

$$a_{001,010} |001\rangle \langle 010| = \frac{a_{12}}{2^3} (\hat{\sigma}_{011} - i\hat{\sigma}_{012} + i\hat{\sigma}_{021} + \hat{\sigma}_{022} + \hat{\sigma}_{311} - i\hat{\sigma}_{312} + i\hat{\sigma}_{321} + \hat{\sigma}_{322}),$$

$$a_{101,110} |101\rangle \langle 110| = \frac{a_{56}}{2^3} (\hat{\sigma}_{011} - i\hat{\sigma}_{012} + i\hat{\sigma}_{021} + \hat{\sigma}_{022} - \hat{\sigma}_{311} + i\hat{\sigma}_{312} - i\hat{\sigma}_{321} - \hat{\sigma}_{322}),$$

$$a_{111,100} |111\rangle \langle 100| = \frac{a_{74}}{2^3} (\hat{\sigma}_{011} - i\hat{\sigma}_{012} - i\hat{\sigma}_{021} - \hat{\sigma}_{022} - \hat{\sigma}_{311} + i\hat{\sigma}_{312} + i\hat{\sigma}_{321} + \hat{\sigma}_{322})$$

внесут вклад в линейную комбинацию  $\hat{\sigma}_{011}$ ,  $\hat{\sigma}_{012}$ ,  $\hat{\sigma}_{021}$ ,  $\hat{\sigma}_{022}$ ,  $\hat{\sigma}_{311}$ ,  $\hat{\sigma}_{312}$ ,  $\hat{\sigma}_{321}$ , и  $\hat{\sigma}_{322}$  с

$$k = 010 \oplus 001 = 001 \oplus 010 = 101 \oplus 110 = 111 \oplus 100 = \mathbf{011}.$$

Элементы базиса Паули, возникающие в (12) из этих слагаемых, показаны в Таблице 2. Например, если  $l = 5 = (101)_2$ , то, в соответствии с (12),

$$\begin{aligned} I^{(3)}[5] &= [(010)_2 \wedge (011)_2]_4 + 2[(101)_2 \wedge (011)_2]_4 + 3[(101)_2 \wedge (100)_2]_4 \\ &= [010]_4 + 2[001]_4 + 3[100]_4 = 312. \end{aligned}$$

Далее, в качестве примера, слагаемое  $a_{101,110}|101\rangle\langle 110| = a_{56}|5\rangle\langle 6|$  вносит  $ia_{56}/2^3$  в  $S^{(3)}[5]$ , так как существуют тройки  $(l_0i_0j_0) = (110)_2$ ,  $(l_1i_1j_1) = (001)_2$ , и  $(l_2i_2j_2) = (111)_2$  в Алгоритме 1 (строки 17 – 26); поэтому  $sign = 1$ ,  $c = 1$ .

| $l$                | 0                    | 1                    | 2                    | 3                    | 4                    | 5                    | 6                    | 7                    |
|--------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| $l_2l_1l_0$        | 000                  | 001                  | 010                  | 011                  | 100                  | 101                  | 110                  | 111                  |
| $k_2k_1k_0$        | 011                  | 011                  | 011                  | 011                  | 011                  | 011                  | 011                  | 011                  |
| $\bar{l} \wedge k$ | 011                  | 010                  | 001                  | 000                  | 011                  | 010                  | 001                  | 000                  |
| $l \wedge k$       | 000                  | 001                  | 010                  | 011                  | 000                  | 001                  | 010                  | 011                  |
| $l \wedge \bar{k}$ | 000                  | 000                  | 000                  | 000                  | 100                  | 100                  | 100                  | 100                  |
| $\hat{\sigma}_I$   | $\hat{\sigma}_{011}$ | $\hat{\sigma}_{012}$ | $\hat{\sigma}_{021}$ | $\hat{\sigma}_{022}$ | $\hat{\sigma}_{311}$ | $\hat{\sigma}_{312}$ | $\hat{\sigma}_{321}$ | $\hat{\sigma}_{322}$ |

Таблица 2: Элементы базиса Паули, возникающие для  $k = 011$ .

**Algorithm 1** Преобразование в базис Паули.

---

```

1: Ввод количество кубитов  $n$ 
2: Ввод строки  $i = i_{n-1} \dots i_0$  и  $j = j_{n-1} \dots j_0$ ,  $i_s, j_s \in \{0, 1\}$ 
3: Ввод комплексное число  $a_{ij}$  — коэффициент в  $a_{ij}|i\rangle\langle j|$ 
4: //Составить номер строки  $k = i \oplus j$ 
5: Инициализация строки  $k = \text{null}$ 
6: for  $i_s = i_0, \dots, i_{n-1}$  do
7:   for  $j_s = j_0, \dots, j_{n-1}$  do
8:      $k_s = i_s \oplus j_s$ 
9:   end for
10: end for
11: Преобразовать  $(k_{n-1} \dots k_0)_2$  в  $\text{int } (k)_{10}$ 
12: //Для числа  $k$  заполнить два ряда
13: Инициализация  $S^{(k)}$  нулевым вектором длины  $2^n$  с комплексным типом
    данных
14: Инициализация  $I^{(k)}$  нулевой строковой матрицей длиной  $2^n$ 
15: Инициализация  $\text{int } cntr$  и  $sign \in \{1, -1, i, -i\}$  произвольными значениями
16: for  $l = 0$  до  $2^n - 1$  do
17:   Преобразовать  $(l)_{10}$  в  $(l_{n-1} \dots l_0)_2$ 
18:    $cntr = 0$  и  $sign = 1$ 
19:   for  $l_s = l_0, \dots, l_{n-1}$  do
20:     if  $l_s == 1$  then
21:       если  $(i_s, j_s) == (1, 1)$  тогда  $sign = -sign$ 
22:       если  $(i_s, j_s) == (0, 1)$  тогда  $cntr = cntr + 1$ 
23:       если  $(i_s, j_s) == (1, 0)$  тогда  $sign = -sign$ ,  $cntr = cntr + 1$ 
24:     end if
25:   end for
26:    $I^{(k)}[l] = \bar{l} \wedge k + 2(l \wedge k) + 3(l \wedge \bar{k})$ 
27:    $\text{int } c = cntr \pmod{4}$ ,  $S^{(k)}[l] += i^c \cdot sign \cdot a_{ij}$ 
28: end for
29: Возврат строки  $S^{(k)}$  и  $I^{(k)}$ .

```

---

## 6. Заключение

В этой статье мы описали основную технику работы с базисом Паули. Показано, что эта техника может сделать более удобными и алгоритмичными некоторые манипуляции с математическими выражениями, связанными с квантовыми схемами с большим числом кубитов. Мы представили новый эффективный

алгоритм с полиномиальной сложностью для перехода от стандартного базиса к базису Паули.

## Список литературы

- [1] B. Dirkse, M. Pompili, R. Hanson, M. Walter, S. Wehner *Witnessing Entanglement in Experiments with Arbitrary Noise* Quantum Science and Technology **5**, 035007, 2020 ([arXiv:1909.09119](#))
- [2] I. Hamamura and T. Imamichi *Efficient evaluation of quantum observables using entangled measurements* npj Quantum Information **6**, 56, 2020 ([arXiv:1909.09119](#))
- [3] O. Crawford, B. van Straaten, D. Wang, T. Parks, E. Campbell, S. Brierley *Efficient quantum measurement of Pauli operators in the presence of finite sampling error* Quantum **5**, 385–404, 2021 ([arXiv:1908.06942](#))
- [4] W. Klobus et al. *Higher dimensional entanglement without correlations*. Eur. Phys. J. D **73**, 29, 2019 ([arXiv:1808.10201](#))
- [5] T.J. O'Connor, Y. Yu, B. Helou, R. Laflamme *The robustness of magic state distillation against errors in Clifford gates* Quantum Information & Computation **13**, 361–378, 2013 ([arXiv:1205.6715](#))
- [6] C.A. Riofrio, D. Gross, S.T. Flammia, T. Monz, D. Nigg, R. Blatt, J. Eisert *Experimental quantum compressed sensing for a seven-qubit system* Nature Comm. **8**, 15305, 2017 ([arXiv:1608.02263](#))
- [7] S.S. Jahromi, R. Orus *A universal tensor network algorithm for any infinite lattice* Phys. Rev. D **99**, 195105, 2019 ([arXiv:1808.00680](#))
- [8] A.N. Tsirulev *A geometric view on quantum tensor networks* Europ. Phys. J. Web of Conferences **226**, No 4, 2020 (<https://doi.org/10.1051/epjconf/202022602022>)
- [9] I.M. Potashov, A.N. Tsirulev *Computational Algorithm for Covariant Series Expansions in General Relativity* Europ. Phys. J. Web of Conferences **173**, 03021, 2018 (<https://doi.org/10.1051/epjconf/201817303021>)
- [10] S. Bravyi and A. Kitaev *Universal quantum computation with ideal Clifford gates and noisy ancillas* Phys. Rev. A **71**, 022316, 2005 ([arXiv:quant-ph/0403025](#))
- [11] V. Danos and E. Kashefi *Determinism in the one-way model* Phys. Rev. A. **74**, 052310, 2006 ([arXiv:quant-ph/0506062](#))

- [12] V. Danos and E. Kashefi *Pauli measurements are universal* Electronic Notes in Theoretical Computer Science **170**, 95–100, 2007  
(<https://doi.org/10.1016/j.entcs.2006.12.013>)
- [13] D. Gunlycke, M.C. Palenik, and S.A. Fischer *Efficient algorithm for generating Pauli coordinates for an arbitrary linear operator* 2020  
([arXiv:2011.08942](https://arxiv.org/abs/2011.08942))
- [14] S. Bravyi and D. Maslov *Hadamard-free circuits expose the structure of the Clifford group*. 2020 ([arXiv: 2003.09412](https://arxiv.org/abs/2003.09412))
- [15] I. Bengtsson, K. Życzkowski *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, Cambridge, 2006
- [16] V.V. Shende, I.L. Markov, and S.S. Bullock *Minimal universal twoqubit controlled-NOT-based circuits* Phys. Rev. A, **69**, 062321, 2004  
([arXiv:quant-ph/0308033](https://arxiv.org/abs/quant-ph/0308033))

## Приложение

### A1. Базис Паули для $n = 2$

Для справки мы приведем здесь выражения элементов стандартного базиса в  $\mathcal{H}_2$  в терминах элементов базиса Паули. Напомним, что такие выражения в  $\mathcal{H}_1$  имеют вид

$$|0\rangle\langle 0| = \frac{\hat{\sigma}_0 + \hat{\sigma}_3}{2}, \quad |0\rangle\langle 1| = \frac{\hat{\sigma}_1 + i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 0| = \frac{\hat{\sigma}_1 - i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 1| = \frac{\hat{\sigma}_0 - \hat{\sigma}_3}{2}.$$


---

$$\begin{aligned} |00\rangle\langle 00| &= \frac{\hat{\sigma}_{00} + \hat{\sigma}_{03} + \hat{\sigma}_{30} + \hat{\sigma}_{33}}{4}, & |01\rangle\langle 00| &= \frac{\hat{\sigma}_{01} - i\hat{\sigma}_{02} + \hat{\sigma}_{31} - i\hat{\sigma}_{32}}{4}, \\ |10\rangle\langle 00| &= \frac{\hat{\sigma}_{10} + \hat{\sigma}_{13} - i\hat{\sigma}_{20} - i\hat{\sigma}_{23}}{4}, & |11\rangle\langle 00| &= \frac{\hat{\sigma}_{11} - i\hat{\sigma}_{12} - i\hat{\sigma}_{21} - \hat{\sigma}_{22}}{4}, \end{aligned}$$


---

$$\begin{aligned} |00\rangle\langle 01| &= \frac{\hat{\sigma}_{01} + i\hat{\sigma}_{02} + \hat{\sigma}_{31} + i\hat{\sigma}_{32}}{4}, & |01\rangle\langle 01| &= \frac{\hat{\sigma}_{00} - \hat{\sigma}_{03} + \hat{\sigma}_{30} - \hat{\sigma}_{33}}{4}, \\ |10\rangle\langle 01| &= \frac{\hat{\sigma}_{11} + i\hat{\sigma}_{12} - i\hat{\sigma}_{21} + \hat{\sigma}_{22}}{4}, & |11\rangle\langle 01| &= \frac{\hat{\sigma}_{10} - \hat{\sigma}_{13} - i\hat{\sigma}_{20} + i\hat{\sigma}_{23}}{4}, \end{aligned}$$


---

$$\begin{aligned}
|00\rangle\langle 10| &= \frac{\hat{\sigma}_{10} + \hat{\sigma}_{13} + i\hat{\sigma}_{20} + i\hat{\sigma}_{23}}{4}, & |01\rangle\langle 10| &= \frac{\hat{\sigma}_{11} - i\hat{\sigma}_{12} + i\hat{\sigma}_{21} + \hat{\sigma}_{22}}{4}, \\
|10\rangle\langle 10| &= \frac{\hat{\sigma}_{00} + \hat{\sigma}_{03} - \hat{\sigma}_{30} - \hat{\sigma}_{33}}{4}, & |11\rangle\langle 10| &= \frac{\hat{\sigma}_{01} - i\hat{\sigma}_{02} - \hat{\sigma}_{31} + i\hat{\sigma}_{32}}{4}, \\
|00\rangle\langle 11| &= \frac{\hat{\sigma}_{11} + i\hat{\sigma}_{12} + i\hat{\sigma}_{21} - \hat{\sigma}_{22}}{4}, & |01\rangle\langle 11| &= \frac{\hat{\sigma}_{10} - \hat{\sigma}_{13} + i\hat{\sigma}_{20} - i\hat{\sigma}_{23}}{4}, \\
|10\rangle\langle 11| &= \frac{\hat{\sigma}_{01} + i\hat{\sigma}_{02} - \hat{\sigma}_{31} - i\hat{\sigma}_{32}}{4}, & |11\rangle\langle 11| &= \frac{\hat{\sigma}_{00} - \hat{\sigma}_{03} - \hat{\sigma}_{30} + \hat{\sigma}_{33}}{4}.
\end{aligned}$$

## А2. Некоторые унитарные операторы в базисе Паули

Оператор CNOT:

$$CNOT = \frac{\hat{\sigma}_{00} + \hat{\sigma}_{01} + \hat{\sigma}_{30} - \hat{\sigma}_{31}}{2} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|, \quad (13)$$

Контролируемый фазовый оператор:

$$CZ = \frac{\hat{\sigma}_{00} + \hat{\sigma}_{03} + \hat{\sigma}_{30} - \hat{\sigma}_{33}}{2} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|.$$

Известно, что  $CNOT$  и  $CZ$  принадлежат группе Клиффорда  $\mathcal{C}(\mathcal{H}_2)$ . Также известны некоторые множества генераторов и канонические формы для операторов группы  $\mathcal{C}(\mathcal{H}_n)$  (см., например, [14]), но количество элементов в этих группах растет экспоненциально (фактически немного быстрее) с ростом  $n$ : например,  $\mathcal{C}(\mathcal{H}_1)$  порядка 24, а  $\mathcal{C}(\mathcal{H}_2)$  порядка 11520. Поэтому возникает проблема нахождения практически подходящего [16] набора унитарных операторов для построения групп Клиффорда и соответствующего формализма стабилизаторов. Здесь мы вводим однокубитовый оператор Адамара  $\hat{U}_2^+$  и псевдо-Адамаровы операторы  $\hat{U}_2^-$ ,  $\hat{U}_1^\pm$  и  $\hat{U}_3^\pm$ , подчиняющиеся соотношениям  $(\hat{U}_1^\pm)^2 = (\hat{U}_2^\pm)^2 = (\hat{U}_3^\pm)^2 = \hat{\sigma}_0$ . Они унитарны и эрмитовы и определяются

$$\begin{aligned}
\hat{U}_1^\pm &= \frac{\hat{\sigma}_2 \pm \hat{\sigma}_3}{\sqrt{2}} = \frac{1}{\sqrt{2}} (\pm |0\rangle\langle 0| - i|0\rangle\langle 1| + i|1\rangle\langle 0| \mp |1\rangle\langle 1|), \\
\hat{U}_2^\pm &= \frac{\hat{\sigma}_1 \pm \hat{\sigma}_3}{\sqrt{2}} = \frac{1}{\sqrt{2}} (\pm |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| \mp |1\rangle\langle 1|), \\
\hat{U}_3^\pm &= \frac{\hat{\sigma}_1 \pm \hat{\sigma}_2}{\sqrt{2}} = e^{\mp i\pi/4} |0\rangle\langle 1| \pm e^{\pm i\pi/4} |1\rangle\langle 0|.
\end{aligned} \quad (14)$$

Они могут быть использованы для построения унитарных преобразований  $\hat{\sigma}_i \leftrightarrow \pm \hat{\sigma}_j$  ( $i \neq j$ ) и  $\hat{\sigma}_i \rightarrow -\hat{\sigma}_i$  ( $i = 1, 2, 3$ ):

$$\hat{U}_k^\pm \hat{\sigma}_i \hat{U}_k^\pm = \pm \hat{\sigma}_j, \quad \hat{U}_k^\pm \hat{\sigma}_k \hat{U}_k^\pm = -\hat{\sigma}_k, \quad i \neq j \neq k, \quad i, j, k \in \{1, 2, 3\},$$

или, более подробно,

$$\begin{aligned}\hat{U}_1^\pm \hat{\sigma}_2 \hat{U}_1^\pm &= \pm \hat{\sigma}_3, & \hat{U}_1^\pm \hat{\sigma}_3 \hat{U}_1^\pm &= \pm \hat{\sigma}_2, & \hat{U}_1^\pm \hat{\sigma}_1 \hat{U}_1^\pm &= -\hat{\sigma}_1, \\ \hat{U}_2^\pm \hat{\sigma}_1 \hat{U}_2^\pm &= \pm \hat{\sigma}_3, & \hat{U}_2^\pm \hat{\sigma}_3 \hat{U}_2^\pm &= \pm \hat{\sigma}_1, & \hat{U}_2^\pm \hat{\sigma}_2 \hat{U}_2^\pm &= -\hat{\sigma}_2, \\ \hat{U}_3^\pm \hat{\sigma}_1 \hat{U}_3^\pm &= \pm \hat{\sigma}_2, & \hat{U}_3^\pm \hat{\sigma}_2 \hat{U}_3^\pm &= \pm \hat{\sigma}_1, & \hat{U}_3^\pm \hat{\sigma}_3 \hat{U}_3^\pm &= -\hat{\sigma}_3.\end{aligned}$$

Далее, для однородности, обозначим  $\hat{\sigma}_0$  как  $\hat{U}_0$ . Таким образом, например, мы можем выбрать полный набор генераторов для  $\mathcal{C}(\mathcal{H}_1)$  в виде ( $\hat{U}_i \equiv \hat{U}_i^+$ ,  $i = 1, 2, 3$ )

$$\{\hat{U}_0, \hat{U}_1, \hat{U}_2, \hat{U}_3\}.$$

В общем случае  $\tilde{P}(\mathcal{H}_n)$ , полный набор генераторов для группы  $\mathcal{C}(\mathcal{H}_n)$  составляют операторы вида

$$\{\hat{U}_{i_1 \dots i_n} = \hat{U}_{i_1} \otimes \dots \otimes \hat{U}_{i_n}\}_{i_1, \dots, i_n \in \{0, 1, 2, 3\}}.$$