Заметки по теории вероятностей

Авторы: Хоружий Кирилл

От: *1 апреля 2021 г.*

Содержание

1 Основы квантой криптографии

1.1 Протокол BB84

Пусть есть вертикальная и диагональная поляризация, а также 4 квантовых состояния

шифр Вернама Протокол Диффи — Хеллмана Алгоритм RSA

Классическая кирптография: + изученность, стандартизированность - не выдерживает создание квантового компьютера

Квантовая криптография: + не ставит перехватчик перед вычислительными задачами - мало изучены, возможны атаки

Постквантовая криптография: + выдерживает существование квантового компьютера - недостаточная изученность, авось и классический может взломать

1.2 Теория Информации

пусть $h(p)$ – информационное содержание события вероятности p. Верно следующее утверждение:

$$h(p_1) > h(p_2) \quad \Leftarrow \quad p_1 < p_2.$$

Также вполне логично предположить, что $h(1) = 0$, а также что $h(p_1 p_2) = h(p_1) + h(p_2)$.

Это приводит к функции вида

$$h(x) = -\log x = \log_2 \frac{1}{x}$$

Распределением вероятностей будем считать некоторый набор $\{p_i\}$ такой, что $\sum p_i = 1$. Информация, выдаваемая источником может быть найдена, как *матожидание*

$$H(P) = -\sum_i p_i \log p_i,$$

иначе функция называется энтропией Шеннона, – мера того, насколько неизвестно что выдаст источник.

Также энтропия Шеннона – среднее количество вопросов, которые необходимо задать. Ещё это среднее количество битов, которое необходимо, чтобы закодировать выход источника.

Неравенство Крафта позволяет сформулировать условие к префиксному коду.

Также можно сформулировать, что разность между практической и теоретической длиной слова $\geqslant 0$, что соответсвует неравенству Гиббса.

- Коды Хаффмана
- Maassen-Uffink entropic

1.3 Измерения в базисе

Возвращаемся к состояниям

$$|0\rangle_+ = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$|1\rangle_+ = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$|0\rangle_\times = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$
$$|1\rangle_\times = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Пусть есть некоторый ортонормированный базис $\{|e_i\rangle\}$ и состояние $|\xi\rangle$. Вероятность исхода i при измерении $|\xi\rangle$ в базисе $\{|e_i\rangle\}$ равна

$$\Pr(i) = |\langle e_i|\xi\rangle|^2.$$

2 Основные понятия теории вероятностей

2.1 Элементы комбинаторики

Для начала подружимся с комбинаторикой, взяв некоторую её проекцию на теорвер

Thr 2.1. *Пусть множества $A = \{a_1, \dots, a_k\}$ состоит из k элементов, а множество $B = \{b_1, \dots, b_m\}$ – из m элементов. Тогда можно образовать равно km пар (a_i, b_j).*

Thr 2.2. *Общее количество различных наборов при выборе k элементов из n без возвращения и с учётом порядка равняется*

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!},$$

где A_n^k называется числом размещений из n элементов по k элементов.

Thr 2.3. *Общее количество различных наборов при выборе k элементов из n без возвращения и без учета порядка равняется*

$$C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!},$$

где число C_n^k называется числом сочетаний из n элементов по k элементов.

Thr 2.4. *Общее количество различных наборов при выборе k элементов из n с возвращением и без учёта порядка равняется*

$$C_{n+k-1}^k = C_{n+k-1}^{n-1}.$$

2.2 События и операции над ними

Def 2.5. *Пространством элементарных исходов* называют множество Ω, содержащее все возможные взаимоисключающие результаты данного случайного эксперимента. Элементы множества Ω называются *элементарными исходами* и обозначаются ω.

Def 2.6. *Событиями* называются подмножества Ω. Говорят, что *произошло событие* A, если эксперимент завершился одним из элементарных исходов, входящих в множество A.

Вообще в силу таких определений события и множества оказываются очень похожими, так что определены операции *объединения*, *пересечения*, *дополнения*, а также взятия *противоположеного* $\bar{A} = \Omega \backslash A$. Также можно выделить достоверное событие Ω и невозможное $\varnothing$.

События A и B называются *несовместными*, если они не могут произойти одновременно: $A \cap B = \varnothing$. События $A_1, \dots, A_n$ называются *попарно несовместными*, если несовместны любые два из них: $A_i \cap A_j = \varnothing$, $\forall i \neq j$. Говорят, что событие A *влечет* событие B ($A \subseteq B$), если $A \Rightarrow B$.

2.3 Дискретное пространство элементарных исходов

Пространство элементарных исходов назовём дискретным, если множество Ω конечно или счётно: $\Omega = \{\omega_1, .., \omega_n, \dots\}$.

Def 2.7. Сопоставим каждому элементарному исходу ω_i число $p_i \in [0, 1]$ так, чтобы $\sum p_i = 1$. Вероятностью события A называют число

$$\mathrm{P}(A) = \sum_{\omega_i \in A} p_i,$$

где с случае $A = \varnothing$ считаем $\mathrm{P}(A) = 0$.

Def 2.8 (Классическое определение вероятности)**.** Говорят, что эксперимент описывается *классической вероятностной моделью*, если пространство его элементарных исходов состоит из конечного числа равновозможных исходов. Для любого события верно, что

$$\mathrm{P}(A) = \frac{\operatorname{card} A}{\operatorname{card} \Omega}. \tag{2.1}$$

Эту формулу называют *классическим определением вероятности.*

Тут стоит вспомнить три схемы из модели с урнами: схема выбора с возвращением и с учётом порядка (n^k), выбора без возвращения и с учётом порядка (A_n^k), а также выбора без возвращения и без учёта порядка (C_n^k), описываются классической вероятностной моделью. А вот схема выбора с возвращением и без учёта порядкауже не описывается классической вероятностью.

Пример с гипергеометрическим распределением

Из урны, в которой K белых и $N-K$ чёрных шаров, наудачу и без возвращения вынимают n шаров, где $n \leqslant N$. Термин «наудачу» означает, что появление любого набора из n шаров равновозможно. Найти вероятность того, что будет выбрано k белых и $n-k$ чёрных шаров.

Результат – набор из n шаров. Общее число $\operatorname{card}\Omega = C_N^n$. Пусть A_k – событие, состоящее в том, что в наборе окажется k белых и $n-k$ черных. Есть ровно C_K^k способов выбрать k белых шаров из K, и C_{N-K}^{n-k} способов выбрать $n-k$ черных шаров из $N-K$. Тогда $\operatorname{card} A_k = C_K^k C_{N_K}^{n-k}$,

$$\mathrm{P}(A_k) = \frac{\operatorname{card} A_k}{\operatorname{card}\Omega} = \frac{C_K^k C_{N_K}^{n-k}}{C_N^n}.$$

Этот набор вероятностей называется *гипергеометрическим распределением* вероятностей.

2.4 Дискретное пространство элементарных исходов

Пространство элементарных исходов назовём дискретным, если множество Ω конечно или счётно: $\Omega = \{\omega_1, .., \omega_n, \dots\}$.

Def 2.9. Сопоставим каждому элементарному исходу ω_i число $p_i \in [0,1]$ так, чтобы $\sum p_i = 1$. Вероятностью события A называют число

$$\mathrm{P}(A) = \sum_{\omega_i \in A} p_i,$$

где с случае $A = \varnothing$ считаем $\mathrm{P}(A) = 0$.

Def 2.10 (Классическое определение вероятности)**.** Говорят, что эксперимент описывается *классической вероятностной моделью*, если пространство его элементарных исходов состоит из конечного числа равновозможных исходов. Для любого события верно, что

$$\mathrm{P}(A) = \frac{\operatorname{card} A}{\operatorname{card}\Omega}. \tag{2.2}$$

Эту формулу называют *классическим определением вероятности.*

Тут стоит вспомнить три схемы из модели с урнами: схема выбора с возвращением и с учётом порядка (n^k), выбора без возвращения и с учётом порядка (A_n^k), а также выбора без возвращения и без учёта порядка (C_n^k), описываются классической вероятностной моделью. А вот схема выбора с возвращением и без учёта порядкауже не описывается классической вероятностью.

Пример с гипергеометрическим распределением

Из урны, в которой K белых и $N-K$ чёрных шаров, наудачу и без возвращения вынимают n шаров, где $n \leqslant N$. Термин «наудачу» означает, что появление любого набора из n шаров равновозможно. Найти вероятность того, что будет выбрано k белых и $n-k$ чёрных шаров.

Результат – набор из n шаров. Общее число $\operatorname{card}\Omega = C_N^n$. Пусть A_k – событие, состоящее в том, что в наборе окажется k белых и $n-k$ черных. Есть ровно C_K^k способов выбрать k белых шаров из K, и C_{N-K}^{n-k} способов выбрать $n-k$ черных шаров из $N-K$. Тогда $\operatorname{card} A_k = C_K^k C_{N_K}^{n-k}$,

$$\mathrm{P}(A_k) = \frac{\operatorname{card} A_k}{\operatorname{card}\Omega} = \frac{C_K^k C_{N_K}^{n-k}}{C_N^n}.$$

Этот набор вероятностей называется *гипергеометрическим распределением* вероятностей.

2.5 Геометрическая вероятность

Def 2.11. Пусть некоторая область $\Omega \subset \mathbb{R}^k$ такая, что $\mu(\Omega)$ конечна. Пусть эксперимент состоит из равновероятного выбора случайной точки в области Ω. *Геометрическое определение вероятности*:

$$\mathrm{P}(A) = \frac{\mu(A)}{\mu\Omega}.$$

Если для точки выполнены условия геометрического определения, то говорят, что точка *равномерно распределена* в Ω.

3 Аксиоматика теории вероятностей

3.1 Алгебра и σ-алгебра событий

Def 3.1. Множество $\mathcal{A}$, элментами которого являются некоторые подмножества Ω называют *алгеброй*, если оно удовлетворяет следующим условиям:

A1) $\Omega \sin \mathcal{A}$ (алгебра содержит достоверные события);

A2) если $A \in \mathcal{A}$, то $\bar{A} \in \mathcal{A}$ (вместе с любым множеством алгебра содержит противоположное к нему);

A3) если $A \in \mathcal{A}$ и $B \in \mathcal{A}$, то $A \cup B \in \mathcal{A}$ (вместе с любыми двумя множествами алгебра содержит их объединение).

Вообще из A1 и A2 следует, что $\varnothing = \bar{\Omega} \in \mathcal{A}$. Пункт A3 экстраполируется на любой конечный набор. Кстати, объединение можно заменить (в силу закона де Моргана) на пересечение:

$$xy \in \mathcal{A} \quad \Leftrightarrow \quad \overline{xy} \in \mathcal{A} \quad \Leftrightarrow \quad \overline{x} + \overline{y} \in \mathcal{A}.$$

Thr 3.2 (закон де Моргана)**.** *Для множеств x, y верно, что*

$$\overline{x + y} = \overline{x} \cdot \overline{y}, \qquad \overline{xy} = \overline{x} + \overline{y},$$

где $xy = x \cap y$, $x + y = x \cup y$.

В случае счётного пространства элементарных исходов A3 алгебры оказывается недостаточно, так приходим к σ-алгебре:

Def 3.3. Множество $\mathcal{F}$, элеменатми которого являются некоторые подмножества Ω называется σ-алгеброй, если выполнены следующий условия:

S1) $\Omega \sin \mathcal{F}$ (алгебра содержит достоверные события);

S2) если $A \in \mathcal{F}$, то $\bar{A} \in \mathcal{F}$ (вместе с любым множеством алгебра содержит противоположное к нему);

S3) если $\{A_i\} \in \mathcal{F}$, то $\cup_i A_i \in \mathcal{F}$ (вместе с любым *счетным* набором событий σ-алгебра содержит их объединение).

Def 3.4. Минимальной σ-алгеброй, содержащей набор множеств $\mathcal{U}$, называется пересечение всех σ-алгебр, содержащих $\mathcal{U}$.

Def 3.5. Минимальная σ-алгебра, содержащая множество $\mathcal{U}$ всех интервалов на вещественной прямой называется *борелевской сигма-алгеброй* в $\mathbb{R}$ и обозначается $\mathfrak{B}(\mathbb{R})$.

Итак, оказался определен специальный класс $\mathcal{F}$ подмножеств Ω, названный σ-алгеброй событий. Примнеие счетного числа любых операция к множествам из $\mathcal{F}$ снова дает множество из $\mathcal{F}$. *Собтиями* будем называть только множества $A \in \mathcal{F}$.

3.2 Мера и вероятностная мера

Def 3.6. Пусть Ω – некоторое непустое множество $\mathcal{F}$ – σ-алгебра его подмножеств. Функция

$$\mu \colon \mathcal{F} \mapsto \mathbb{R} \cap [0, +\infty) \cup \{+\infty\}$$

называется *мерой* на $(\Omega, \mathcal{F})$, если она удовлетворяет условиям

μ1) $\mu(A) \geqslant 0$ для любого множества $A \in \mathcal{F}$;

μ2) $\forall$ счетного $\{A_i\} \in \mathcal{F}$ таких, что $A_i \cap A_j = \varnothing$, $\forall i \neq j$ мера их объединения равна сумме их мер:

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu(A_i).$$

Последнее свойство называют *счётное аддитивностью* или σ-аддитивностью меры.

Thr 3.7 (свойство непрерывности меры)**.** *Пусть дана убывающая последовательность* $B_1 \supseteq B_2 \supseteq B_2 \supset B_3 \supset \ldots$ *множеств из* $\mathcal{F}$*, причем* $\mu(B_1) < \infty$*. Пусть* $B = \cap_i^\infty B_i$*. Тогда* $\mu(B) = \lim\limits_{n\to\infty} \mu(B_n)$*.*

Def 3.8. Пусть Ω – непустое множество, $\mathcal{F}$ – σ-алгебра его подмножеств. Мера $\mu\colon \mathcal{F} \mapsto \mathbb{R}$ называется *нормированной*, если $\mu(\Omega) = 1$. Другое название нормированной меры – *вероятность*.

Def 3.9. Пусть Ω – пространство элементарных исходов, $\mathcal{F}$ – σ-алгебра его подмножеств (событий). *Вероятностью* или *вероятностной мерой* на $(\Omega, \mathcal{F})$ называется функция

$$\mathrm{P}\colon \mathcal{F} \mapsto \mathbb{R}$$

обладающая свойствами

P1) $\mathrm{P}(A) \geqslant 0$ для любого события $A \in \mathcal{F}$;

P2) для любого счётного набора *попарно несовместных* событий $\{A_i\} \in \mathcal{F}$ имеет равенство

$$\mathrm{P}\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{k=1}^{\infty} \mathrm{P}(A_i);$$

P3) вероятность достоверного события равна единице: $\mathrm{P}(\Omega) = 1$.

Свойства (P1) – (P3) называют *аксиомами вероятности*.

Def 3.10. Тройка $\langle \Omega, \mathcal{F}, \mathrm{P} \rangle$, в которой Ω – пространство элементарных исходов, $\mathcal{F}$ – σ-алгебра его подмножеств и P – вероятная мера на $\mathcal{F}$, называется *вероятностным пространством*.

Вообще, для вероятности верны следующие свойства

1. $\mathrm{P}(\varnothing) = 0$.
2. Для любого конечного набора попарно несовместных событий $A_1, \ldots, A_n \in \mathcal{F}$ имеет место равенство $\mathrm{P}(A_1 \cup \ldots \cup A_n) = \mathrm{P}(A_1) + \ldots + \mathrm{P}(A_n)$.
3. $\mathrm{P}(\bar{A}) = 1 - \mathrm{P}(A)$.
4. Если $A \subseteq B$, то $\mathrm{P}(B \backslash A) = \mathrm{P}(B) - \mathrm{P}(A)$.
5. $A \subseteq B$, то $\mathrm{P}(A) \leqslant \mathrm{P}(B)$.
6. $\mathrm{P}(A_1 \cup \ldots \cup A_n) \leqslant \sum_{i=1}^n P(A_i)$.

И это всё, конечно, хорошо, но если мы хотим что-то посчитать, то

Thr 3.11 (Формула включения-исключения)**.** *Для вероятности, в частности для двух событий, верно, что*

$$\mathrm{P}(A \cup B) = P(A) + P(B) - P(A \cap B)$$

и, обобщая, для объединения n *множеств*

$$\mathrm{P}(A_1 \cup \ldots \cup A_n) = \sum_{i=1}^{n} \mathrm{P}(A_i) - \sum_{i<j} \mathrm{P}(A_i A_j) + \sum_{i<j<m} \mathrm{P}(A_i A_j A_m) - \ldots + (-1)^{n-1} \mathrm{P}(A_1 A_2 \ldots A_n).$$

4 Условная вероятность и независимость

4.1 Условная вероятность

Def 4.1. Условной вероятностью события A при условии, что произошло событие B, называется число

$$\mathrm{P}(A|B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)},$$

которое само собой определено только при $\mathrm{P}(B) = 0$.

Thr 4.2. *Если* $\mathrm{P}(B) > 0$ *и* $\mathrm{P}(A) > 0$*, то*

$$\mathrm{P}(A \cap B) = \mathrm{P}(B)\,\mathrm{P}(A|B) = \mathrm{P}(A)\,\mathrm{P}(B|A).$$

Thr 4.3. *Для любых событий* $A_1, \ldots, A_n$ *верно равенство:*

$$\mathrm{P}(A_1 \ldots A_n) = \mathrm{P}(A_1) \cdot \mathrm{P}(A_2|A_1) \cdot \mathrm{P}(A_3|A_1 A_2) \cdot \ldots \cdot \mathrm{P}(A_n|A_1 \ldots A_{n-1}),$$

если все участвующие в нём условные вероятности определены.

4.2 Независимость событий

Def 4.4. События A и B называются *независимыми*, если $\mathrm{P}(A \cap B) = \mathrm{P}(A)\,\mathrm{P}(B)$.

Из этого определения вытекает следующие леммы.

Lem 4.5. *Пусть* $\mathrm{P}(B) > 0$. *Тогда события A и B независимы тогда и только, когда* $\mathrm{P}(A|B) = \mathrm{P}(A)$.

Lem 4.6. *Пусть A и B несовместны. Тогда независимыми они будут только в том случае, если* $\mathrm{P}(A) = 0$ *или* $\mathrm{P}(B) = 0$.

Другими словами несовместные события не могут быть независимыми. Зависимость между ними – просто причинно-следственная: если $A \cap B = \varnothing$, то $A \subseteq \bar{B}$, т.е. при выполнении A события B *не происходит*.

Lem 4.7. *Если события A и B независимы, то независимы и события A и $\bar{B}$, $\bar{A}$ и B, $\bar{A}$ и $\bar{B}$.*

Def 4.8. События $A_1, \ldots, A_n$ называются *независимыми в совокупности*, если для любого $1 \leqslant k \leqslant n$ и любого набора различных меж собой индекс $1 \leqslant i_1 < \ldots < i_k \leqslant n$ имеет место равенство

$$\mathrm{P}(A_{i_1} \cap \ldots \cap A_{i_k}) = \mathrm{P}(A_{i_1}) \cdot \ldots \cdot \mathrm{P}(A_{i_k}).$$

4.3 Формула полной вероятности

Def 4.9. Конечный или счётный набор попарно несовместных событий $\{H_i\}$ таких, что $\mathrm{P}(H_i) > 0\ \forall i$ и $\cup_i H_i = \Omega$, называется *полной группой событий* или разбиением пространства Ω. Также события, образующие полную группу событий, часто называют *гипотезами*.

При подходящем выборе гипотез для любого события A могут быть сравнительно просто вычислены $\mathrm{P}(A|H_i)$ и, собственно, $\mathrm{P}(H_i)$. Как посчитать вероятность события A?

Thr 4.10 (формула полной вероятности)**.** *Пусть дана полная группа событий $\{H_i\}$. Тогда вероятность любого события A может быть вычислена по формуле*

$$\mathrm{P}(A) = \sum_{i=1}^{\infty} \mathrm{P}(H_i) \cdot \mathrm{P}(A|H_i).$$