Классические и квантовые вычисления

А. Китаев; написал М. Вялый

11 лекция (23/04/98)

Коды: классические и квантовые

Если есть последовательность унитарных операторов $U_1, \dots, U_L$ и последовательность приближений $\tilde{U}_1, \dots, \tilde{U}_L$, $\|\tilde{U}_j - U_j\| < \delta$, то выполняется неравенство

$$\|\tilde{U}_L \cdot \dots \cdot \tilde{U}_1 - U_L \cdot \dots \cdot U_1\| < L\delta.$$

В общем случае это неравенство неулучшаемо. Поэтому при последовательном применении приближенных реализаций операторов, составляющих квантовую схему, постепенно теряется точность. Возникает важный вопрос, имеющий прямое отношение к физической реализации квантового компьютера: можно ли производить квантовые вычисления без накопления ошибок?

Ответ на этот вопрос положительный. Идея состоит в том, чтобы заменить каждый q-бит, использующийся в вычислениях, несколькими. В пространстве $\mathbb{B}^{\otimes n}$ выделим подпространство $\mathcal{M}$, $\dim \mathcal{M} = 2$, соответствующее одному q-биту, $\mathbb{B} \hookrightarrow \mathbb{B}^{\otimes n}$.

Оператору $U : \mathbb{B} \to \mathbb{B}$ сопоставляется квантовая схема $\hat{U}$, и результат ее применения сопоставляется применению оператора U к закодированному биту.

Конструкции, необходимые для организации вычислений без потери точности, довольно сложны, поэтому мы ограничимся более простым вопросом: как сохранять неограниченно долго заданное квантовое состояние? (Легко понять, что это — частный случай предыдущего вопроса, когда реализуется последовательность тождественных операторов.)

Определение. *Квантовый код типа (n, m) — это подпространство $\mathcal{M} \subseteq \mathbb{B}^{\otimes n}$ размерности m.*

Ошибки, возникающие при хранении информации, будут приводить к тому, что состояние системы будет выходить за $\mathcal{M}$. Поэтому необходимо научиться восстанавливать состояние системы после воздействия ошибок определенного типа.

Классические коды

Вначале разберем случай классических кодов. *Классический код* — это подмножество $M \subseteq \{0,1\}^n$. Задача исправления ошибок в классическом случае формулируется так.

Есть: *входы* — слова из M; *канал связи*, который является “отображением” $\{0,1\}^n \to \{0,1\}^{n'}$, более точно, канал связи задается условными вероятностями $p(y|x)$ приема слова y при передаче слова x.

Естественно использовать модель независимо распределенных ошибок, тогда

$$p(y|x) = p_0^{d(x,y)} p_1^{n-d(x,y)}, \text{ где } p_1 = 1 - p_0, \quad d(x,y) \text{ — расстояние Хэмминга (число различных бит).}$$

Однако для анализа гораздо проще предположить, что ненулевые вероятности будут только при условии $d(x, y) \le k$, где k задает интересующий нас порог точности, и все такие ошибки считать равновероятными.

Введем обозначения. Пусть $N = \{0,1\}^n$ — множество входов; $N' = \{0,1\}^{n'}$ — множество выходов; множество переходов (оно же — множество ошибок) $E \subseteq N \times N'$. Обозначим $E(n,k) = \{(x,y) | d(x,y) \le k\}$.

Определение. *Код M исправляет ошибки из множества E, если из $(x_1, y) \in E$ и $(x_2, y) \in E$ следует $x_1 = x_2$.*

Другими словами это условие можно сформулировать так: для любых пар (x_1, y_1), (x_2, y_2), принадлежащих E, из $x_1 \ne x_2$ следует $y_1 \ne y_2$.

Дополним определение: если $E = E(n,k)$, то говорят, что *код исправляет k ошибок.*

Пример 1. Код, основанный на повторении. $M = \{(0,0,0),(1,1,1)\} \subseteq \{0,1\}^3$.

Такой код исправляет одну ошибку.

Очевидное обобщение примера 1 приводит к классическим кодам, исправляющим любое количество ошибок. Построим более интересные примеры классических кодов. Для начала дадим еще одно стандартное определение.

Определение. *Кодовое расстояние* — $d(M) = \min\{d(x_1,x_2) : x_1, x_2 \in M;\ x_1 \ne x_2\}$.

В примере 1 $d(M) = 3$. Имеется очевидное утверждение.

Утверждение. *Код исправляет k ошибок тогда и только тогда, когда $d(M) > 2k$.*

Примеры классических кодов

1) M_n типа $(n, 2)$, $d(M_n) = n$.

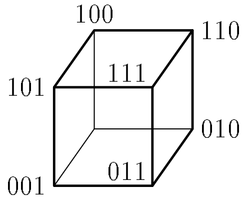
$$M_n = \{(\underbrace{0,\dots,0}_{n});\ (\underbrace{1,\dots,1}_{n})\}.$$

Это самая простая схема кодирования. Повторяем каждый бит много раз, а после каждой операции восстанавливаем кодовое слово, заменяя значения битов на то, которое встречается в большинстве.

Эта серия кодов, как будет показано ниже, не обобщается на квантовый случай.

2) Проверка на четность. Код $M_n^{(2)}$, типа $(n, 2^{n-1})$, $d(M) = 2$. Состоит из всех *четных* слов, т. е. слов, содержащих четное число единиц.

3) Код Хэмминга H_r. Число кодовых бит $n = 2^r - 1$. Код типа $(n, 2^{n-r})$.



Все кодовые биты можно занумеровать ненулевыми двоичными словами длины r. (На врезке показан пример с $r = 3$.) Каждому слову из $\{0,1\}^n$ тогда сопоставляются естественным способом значения x_α битовых переменных: x_α показывает знак на α-м месте. Введем множество контрольных сумм

$$\mu_j(x) = \sum_{\alpha:\alpha_j=1} x_\alpha.$$

Суммирование здесь понимается по модулю 2. На врезке обведены биты, входящие в три контрольные суммы (полезно увидеть в этой картинке трехмерный куб). Равенства контрольных сумм 0 задают множество слов кода Хэмминга (оно является подпространством по модулю 2). Можно показать, что для кода Хэмминга $d = 3$.

Квантовые коды

Будем давать определения аналогично классическому случаю. Ошибки теперь образуют линейное пространство $\mathcal{E} \subseteq \mathbf{L}(\mathcal{N}, \mathcal{N}')$. Каждая ошибка переводит вектор $|\xi\rangle \in \mathcal{N}$ в вектор $|\eta\rangle \in \mathcal{N}'$. Есть и прямой аналог множества $E(n,k)$. Рассмотрим $\mathcal{N} = \mathcal{N}' = \mathbb{B}^{\otimes n}$. Через $\mathcal{E}[A]$ обозначим те ошибки, которые действую на q-битах из множества A и не действуют на остальных битах. Т. е. $\mathcal{E}[A] = \mathbf{L}(\mathbb{B}^{\otimes A}) \otimes I_{\mathbb{B}^{\otimes \setminus A}}$. Тогда полагаем

$$\mathcal{E}(n,k) = \sum_{|A| \le k} \mathcal{E}[A].$$

(Здесь стоит просто сумма подпространств, не прямая.)

Мы рассматриваем такой общий вид ошибок, чтобы иметь принципиальную возможность анализировать и устойчивость общих преобразований матриц плотности к ошибкам.

Свойства преобразований матриц плотности будут даны в качестве задач для самостоятельного решения, здесь нам потребуется существование нормы на преобразованиях матриц плотности, согласованной с тензорным произведением. Эту норму будем обозначать $\|\cdot\|_\diamond$.

Рассмотрим преобразование матриц плотности $T = (T_1)^{\otimes n}$, где $\|T_1 - I\|_\diamond < \delta$. (Полагаем, что на все биты действует одно и тоже малое возмущение.) Запишем $T_1 = I + R_1$, $\|R_1\|_\diamond < \delta$ и перепишем в этих обозначениях выражение для T

$$T = (I + R_1)^{\otimes n} = I + \sum_{|A| \le k} R_1^{\otimes A} \otimes I_{\setminus A} + \underbrace{\sum_{|A| > k} R_1^{\otimes A} \otimes I_{\setminus A}}_{P}.$$

Последний член оценим по норме $\|P\|_\diamond = O(\delta^k)$, им будем пренебрегать. Преобразования $R_1^{\otimes A}$ имеют вид $R_1^{\otimes A}\rho = \sum\limits_i X_i \rho Y_i^\dagger$, где X_i, $Y_i \in \mathcal{E}(A)$; символически это можно записать так: $R_1^{\otimes A} \in \mathcal{E}(A) \cdot \mathcal{E}^\dagger(A)$. Сумма преобразований $\sum_{|A| \le k} R_1^{\otimes A} \otimes I_{\setminus A}$ лежит в $\mathcal{E}(n,k) \cdot \mathcal{E}^\dagger(n,k)$.

Все операторы такого вида будем учитывать точно. Таким образом, будем рассматривать коды, устойчивые к ошибкам из $\mathcal{E}(n,k) \cdot \mathcal{E}^\dagger(n,k)$.

В последующем изложении мы не будем касаться вопроса о реализации операторов исправления ошибок, это облегчает дело.

Определение. *Квантовый код (подпространство $\mathcal{M} \subseteq \mathcal{N}$) исправляет ошибки из $\mathcal{E} \subseteq \mathbf{L}(\mathcal{N}, \mathcal{N}')$ если*

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M} \;\; \forall\, X, Y \in \mathcal{E} \qquad (\langle \xi_2 | \xi_1 \rangle = 0) \Longrightarrow \Big(\langle \xi_2 | Y^\dagger X | \xi_1 \rangle = 0 \Big).$$

Это определение фиксирует формально требование "различные состояния переходят в различные состояния". Конечно, нужно еще предъявить и процедуру восстановления состояния, но это мы сейчас рассматривать не будем.

Пример 2. Рассмотрим квантовый аналог кода с повторением. $\mathcal{M} = (|0,\ldots,0\rangle, |1,\ldots,1\rangle)$. Рассмотрим два состояния $|\xi_1\rangle = |0,\ldots,0\rangle + |1,\ldots,1\rangle$ и $|\xi_2\rangle = |0,\ldots,0\rangle - |1,\ldots,1\rangle$. Ошибки выберем так: $X = \mathrm{id}$, $Y = \sigma^z[1]$; видно, что $X, Y \in \mathcal{E}(n,1)$. Таким образом, $Y|\xi_2\rangle = |\xi_1\rangle$, в прямом противоречии с определением кода, исправляющего ошибки. Мы видим, что код с произвольно большим повторением не защищает даже от одной ошибки.

Ошибки вида $\sigma^x[1]$, где $\sigma^x \stackrel{\mathrm{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, называются классическими, а ошибки вида $\sigma^z[1]$ называются фазовыми.

Кодовое расстояние

В определении квантового кода, исправляющего ошибки, речь шла только о парах ортогональных состояний. Давайте посмотрим, что получается на произвольных парах. Оказывается, что

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \qquad \langle\xi_2|Y^\dagger X|\xi_1\rangle = c(Y^\dagger X)\langle\xi_2|\xi_1\rangle.$$

Действительно, пусть $|\eta_1\rangle, \ldots, |\eta_m\rangle$ — ортонормированный базис $\mathcal{M}$, обозначим $Z = Y^\dagger X$. По определению кода, исправляющего ошибки, $\langle\eta_j|Z|\eta_k\rangle = 0$ при $j \neq k$. А $\langle\eta_j|Z|\eta_j\rangle = c$ (не зависит от j), так как

$$\langle\eta_j|Z|\eta_j\rangle - \langle\eta_k|Z|\eta_k\rangle = \langle\eta_j - \eta_k|Z|\eta_j + \eta_k\rangle + \langle\eta_k|Z|\eta_j\rangle - \langle\eta_j|Z|\eta_k\rangle = 0.$$

(Все три слагаемых в правой части равенства равны нулю, так как входящие в них пары векторов ортогональны).

Заметим, что если $X, Y \in \mathcal{E}(n,k)$, то $Z = Y^\dagger X \in \mathcal{E}(n, 2k)$.

Определение. Код $\mathcal{M}$ *замечает* ошибки из $\mathcal{E}' \subseteq \mathbf{L}(\mathcal{N})$, если

$$\forall\, |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M} \;\; \forall\, Z \in \mathcal{E}' \qquad \langle\xi_2|Z|\xi_1\rangle = c(Z)\langle\xi_2|\xi_1\rangle.$$

Кодовым расстоянием называется наименьшее число $d = d(\mathcal{M})$, при котором код не замечает ошибки из $\mathcal{E}(n,d)$.

Таким образом, код исправляет k ошибок, если $2k < d(\mathcal{M})$.

Пример 3 (код Шора). Опишем серию кодов со сколь угодно большим кодовым расстоянием. Эти коды используют $n = r^2$ кодовых бит, кодируют один бит, т. е. $m = \dim \mathcal{M} = 2$, и $d = r$.

Поскольку количество бит – точный квадрат, удобно задавать базисные состояния в таком кодовом пространстве в виде матрицы. В этих обозначениях код Шора порождается векторами

$$|\xi_\alpha\rangle = \sum_{y_1,\ldots,y_r \in \{0,1\}^r} (-1)^{\alpha \sum_{i=1}^r y_i} \left| \begin{matrix} y_1 & \ldots & \ldots & y_1 \\ y_2 & \ldots & \ldots & y_2 \\ \ldots & \ldots & \ldots & \ldots \\ y_r & \ldots & \ldots & y_r \end{matrix} \right\rangle.$$

Для анализа кода Шора нам потребуется классификация операторов с помощью матриц Паули. Их, вообще говоря, три, но четвертой матрицей Паули будем считать единичную. Введем также несколько нестандартную индексацию матриц Паули:

$$\sigma_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad \sigma_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma^z; \qquad \sigma_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma^x; \qquad \sigma_{11} = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} = \sigma^y.$$

Матрицы Паули замечательны, например, тем, что они эрмитовы и унитарные одновременно. Введенная индексация позволяет удобно записывать коммутационные соотношения между матрицами Паули

$$\sigma_{\alpha\beta}\sigma_{\alpha'\beta'} = (-\mathrm{i})^{\alpha\beta' - \alpha'\beta}\sigma_{\alpha\oplus\alpha', \beta\oplus\beta'} \qquad\qquad \sigma_{\alpha\beta}\sigma_{\alpha'\beta'} = (-1)^{\alpha\beta'-\alpha'\beta}\sigma_{\alpha'\beta'}\sigma_{\alpha\beta}.$$

Множество индексов образует группу $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ или 2-мерное пространство над полем $\mathbb{F}_2$.

Матрицы Паули образуют базис пространства $\mathbf{L}(\mathbb{B})$:

$$\mathbf{L}(\mathbb{B}) = (\sigma_{00}) \oplus (\sigma_{01}) \oplus (\sigma_{10}) \oplus (\sigma_{11}).$$

На пространстве $\mathbb{B}^{\otimes n}$ будет уже 4^n базисных операторов. Введем обозначение

$$\sigma(f) = \sigma(\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_n, \beta_n) \stackrel{\text{def}}{=} \sigma_{\alpha_1,\beta_1} \otimes \sigma_{\alpha_2,\beta_2} \otimes \cdots \otimes \sigma_{\alpha_n,\beta_n}.$$

Здесь $f \in G^n = \mathbb{F}_2^{2n}$.

Используя коммутационные соотношения, можно написать, с точностью до общего фазового множителя, $\sigma(f) = c\sigma(f^{(x)}) \cdot \sigma(f^{(z)})$, где $f^{(x)} = (\alpha_1, 0, \alpha_2, 0, \ldots)$, называется классической ошибкой, а $f^{(z)} = (0, \beta_1, 0, \beta_2, \ldots)$ — фазовой ошибкой.

Теперь проанализируем код Шора. В силу линейности определения достаточно ограничиться изучением базисных ошибок. Пусть $Z \in \mathcal{E}(r^2, k)$, $(k < r)$; представим $Z = \sigma(f) = c\sigma(f^{(x)})\sigma(f^{(z)})$. Поскольку $|f| \le k$ ($|f|$ — число ненулевых переменных в f), то $|f^{(x)}|, |f^{(z)}| \le k < r$.

Достаточно показать, что в этом случае $\langle \xi_1 | Z | \xi_0 \rangle = 0$, $\langle \xi_1 | Z | \xi_1 \rangle = \langle \xi_0 | Z | \xi_0 \rangle$. Рассмотрим два случая.

1) Классическая составляющая отлична от 0. В этом случае каждое базисное состояние

$$\left| \begin{matrix} y_1 & \ldots & \ldots & y_1 \\ y_2 & \ldots & \ldots & y_2 \\ \ldots & \ldots & \ldots & \ldots \\ y_r & \ldots & \ldots & y_r \end{matrix} \right\rangle$$

изменяется под действием Z в некоторых e битах, $0 < e < r$. Поэтому в скалярных произведениях все слагаемые будут равны 0.

2) $f^{(x)} = 0$. Ошибка чисто фазовая: $Z = (\sigma^z)^{\beta_{11}} \otimes \cdots \otimes (\sigma^z)^{\beta_{rr}}$, $\sum \beta_{ij} < r$. Обозначим $\lambda_i = \sum_j \beta_{ij}$. Тогда (см. формулу для векторов $|\xi_\alpha\rangle$)

$$Z|\xi_\alpha\rangle \;=\; \sum_{y_1,\ldots,y_r} (-1)^{\sum_i (\lambda_i + \alpha) y_i} \left| \begin{matrix} y_1 & \ldots & \ldots & y_1 \\ y_2 & \ldots & \ldots & y_2 \\ \ldots & \ldots & \ldots & \ldots \\ y_r & \ldots & \ldots & y_r \end{matrix} \right\rangle$$

Нас интересуют значения λ_j по модулю 2. Возможны 3 случая:

а) $(\lambda_1, \ldots, \lambda_r) = (0, \ldots, 0) \pmod 2$.

б) $(\lambda_1, \ldots, \lambda_r) = (1, \ldots, 1) \pmod 2$.

в) $(\lambda_1, \ldots, \lambda_r) \ne (0, \ldots, 0), (1, \ldots, 1) \pmod 2$.

Случай (б), в действительности, реализоваться не может, так как $\sum_i \lambda_i \le k < r$. В случае (а) все скалярные произведения обращаются в ноль, $Z\langle \xi_\alpha | Z | \xi_{\alpha'} \rangle = 0$. В случае (в) $Z|\xi_\alpha\rangle = |\xi_\alpha\rangle$, то есть Z действует на кодовом подпространстве тождественным образом. (Такая ошибка, по существу, не является ошибкой, поскольку ничего не портит). Следовательно, $Z\langle \xi_\alpha | Z | \xi_{\alpha'} \rangle = \langle \xi_\alpha | \xi_{\alpha'} \rangle$.

Итак, код Шора замечает $r - 1$ ошибку; кодовое расстояние равно r.

Замечание. Код Шора основан на дуальности между классическими и фазовыми ошибками, которая выражается равенством $\sigma^z = S\sigma^x S^\dagger$. Внутри каждой строки $y_i, \ldots, y_i$ реализован обычный повторительный код, исправляющий классические ошибки. Строки организованы в аналогичный код, отличающийся заменой базиса в каждом q-бите: $\sum_{y_1,\ldots,y_r} (-1)^{\alpha(\sum_i y_i)} |y_1, \ldots, y_r\rangle = (S \otimes \cdots \otimes S)|\alpha, \ldots, \alpha\rangle$. Этот код исправляет фазовые ошибки.