Классические и квантовые вычисления

А. Китаев; написал М. Вялый

12 лекция (07/05/98)

Симплектические (стабилизирующие) коды

Это аналог классических линейных кодов. Пусть есть множество $N = \{0,1\}^n = \mathbb{F}_2^n$. *Линейный код* $M \subseteq N$ — это линейное подпространство. Линейные коды удобно задавать двойственным базисом (как множество решений системы линейных уравнений).

Пример 1 (Код Хэмминга). Он задается как решения системы уравнений

$$\begin{cases} x_{001} + x_{011} + x_{101} + x_{111} = \mu_1(x) = 0 \\ x_{010} + x_{011} + x_{110} + x_{111} = \mu_2(x) = 0 \\ x_{100} + x_{101} + x_{110} + x_{111} = \mu_3(x) = 0 \end{cases}$$

Поэтому код Хэмминга образует подпространство коразмерности 3.

Квантовые коды будут устроены так же, только вместо контрольных сумм будут использоваться σ-операторы ($\sigma(\alpha_1, \beta_1, \ldots, \sigma_n, \alpha_n)$ в предыдущих обозначениях).

Давайте зададим таким способом код Шора. Для кода Шора $\mathcal{N} = \mathbb{B}^{\otimes r^2}$, $\dim \mathcal{M} = 2$. Кодовое подпространство было порождено двумя векторами

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

(Напомним, что базисные вектора в данном случае мы договорились записывать в виде 0-1-матриц размера $r \times r$.)

Каким условиям удовлетворяют базисные вектора $\mathcal{M}$?

1) Для любых $i, j,\ (j < r)$ выполнено $\sigma^z_{i,j}\sigma^z_{i,j+1}|\xi\rangle = |\xi\rangle$, т. е. каждая строка состоит из повторений одного бита.

2) Для любого $i < r$ $\prod_j \left(\sigma^x_{i,j}\sigma^x_{i+1,j}\right)|\xi\rangle = |\xi\rangle$. Что означает это условие? Оператор $\prod_j \left(\sigma^x_{i,j}\sigma^x_{i+1,j}\right)$ переводит базисный вектор $\left| \begin{matrix} \ldots & \ldots & \ldots \\ y_i & \ldots & y_i \\ y_{i+1} & \ldots & y_{i+1} \\ \ldots & \ldots & \ldots \end{matrix} \right\rangle$ в вектор $\left| \begin{matrix} \ldots & \ldots & \ldots \\ y_i \oplus 1 & \ldots & y_i \oplus 1 \\ y_{i+1} \oplus 1 & \ldots & y_{i+1} \oplus 1 \\ \ldots & \ldots & \ldots \end{matrix} \right\rangle$ (остальные строки не меняются). Эти два вектора должны входить в $|\xi\rangle$ с одинаковыми коэффициентами.

Утверждение. *Если $|\xi\rangle$ удовлетворяет 1) и 2), то $|\xi\rangle = c_0|\xi\rangle_0 + c_1|\xi\rangle_0$.*

Прежде чем перейти к изучению более общих квантовых кодов, рассмотрим подробнее свойства σ-операторов.

Как уже говорилось, σ-операторы удобно индексировать элементами группы $G = (\mathbb{F}_2)^2$. Будем обозначать мультииндекс σ-оператора $\gamma = (\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n) \in G^n$.

σ-операторы образуют базис в $\mathbf{L}(\mathbb{B}^{\otimes n})$, более того, есть естественная G^n-градуировка:

$$\mathbf{L}(\mathbb{B}^{\otimes n}) = \bigoplus_{\gamma \in G^n} \big(\sigma(\gamma)\big).$$

Для σ-операторов выполнены следующие соотношения

$$\sigma(\gamma_1)\sigma(\gamma_2) = c(\gamma_1, \gamma_2)\sigma(\gamma_1 \oplus \gamma_2), \qquad c(\gamma_1, \gamma_2) \in \mathbb{C}.$$

Рассмотрим унитарные преобразования — действия унитарных операторов $X \mapsto UXU^\dagger$. Такое действие не меняется при домножении U на число, равное по модулю единице, поэтому группа унитарных преобразований имеет вид $\mathbf{UT}(\mathbb{B}^{\otimes n}) = \mathbf{U}(\mathbb{B}^{\otimes n})/\mathbf{U}(1)$. Отметим, что унитарные преобразования — это в точности автоморфизмы $*$-алгебры $\mathbf{L}(\mathbb{B}^{\otimes n})$.

Нас интересуют такие преобразования, для которых $U\sigma(\gamma)U^\dagger = \sigma(u(\gamma)) \cdot c(\gamma)$ ($u : G^n \to G^n$ — некоторая функция). Группа таких преобразований называется *расширенной симплектической группой* и обозначается $\mathrm{ESp}_2(n)$. Операторы из этой группы будем называть симплектическими. Приведем примеры.

1) σ-матрицы. $\sigma(f)\sigma(\gamma)\sigma(f)^\dagger = \sigma(f)\sigma(\gamma)\sigma(f) = (-1)^{\omega(f,\gamma)}\sigma(\gamma)$, где

$$\omega(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n; \alpha_1', \beta_1', \ldots, \alpha_n', \beta_n') = \sum (\alpha_i \beta_i' - \alpha_i' \beta_i) \pmod 2.$$

   В данном случае $u(\gamma) = \gamma$.

2) Оператор $S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Непосредственно проверяется, что $S\sigma^x S = \sigma^z$, $S\sigma^z S = \sigma^x$, $S\sigma^y S = -\sigma^y$. Таким образом, преобразование $S \cdot S^\dagger \in \mathrm{ESp}_2(1)$.

Основные свойства введенного отображения $u : G^n \to G^n$ таковы:

1) u линейно на G^n;

2) u сохраняет форму ω, т. е. $\omega(u(f), u(g)) = \omega(f, g)$.

Отображения с такими свойствами, как известно, называются симплектическими; они образуют *симплектическую группу* $\mathrm{Sp}_2(n)$. Таким образом, определен гомоморфизм $\theta : \mathrm{ESp}_2(n) \to \mathrm{Sp}_2(n)$.

Теорема. $\operatorname{Im}\theta = \mathrm{Sp}_2^n$, $\operatorname{Ker}\theta = G^n$. *(Таким образом,* $\mathrm{ESp}_2(n)/G^n \cong \mathrm{Sp}_2(n)$*).*

Для доказательства теоремы можно использовать следующую лемму, представляющую самостоятельный интерес. (Ни теорему, ни лемму мы доказывать не будем).

Лемма. *Группа* $\mathrm{ESp}_2(n)$ *порождается элементами* $(S \cdot S^\dagger)[i]$, $(K \cdot K^\dagger)[i]$, $\big(\Lambda(\sigma^x) \cdot \Lambda^\dagger(\sigma^x)\big)[i,j]$.

(Напомним, что $K = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}$.)

Можно показать, что $|\,\mathrm{ESp}_2(1)| = 24$. Если учитывать фазовые множители, то получилась бы *группа Клиффорда* из $24 \cdot 8 = 192$ элементов.

$$W\sigma_1^z W^\dagger = \sigma_1^z$$
$$W\sigma_2^z W^\dagger = \sigma_1^z\sigma_2^z$$
$$W\sigma_2^x W^\dagger = \sigma_2^x$$
$$W\sigma_1^x W^\dagger = \sigma_1^x\sigma_2^x$$

Посмотрим на действие оператора $W = \Lambda(\sigma^x)[1,2]$. По определению, имеем $W|a,b\rangle = |a, a\oplus b\rangle$. На врезке показано действие W на образующие алгебры $\mathbf{L}(\mathbb{B}^{\otimes 2})$. Приведенные равенства можно без труда проверить прямым вычислением. Однако полезно обратить внимание на объяснение “на пальцах”. Оператор σ^z можно понимать как измерение значения соответствующего бита. Первые два равенства просто показывают, как меняются эти значения при замене базиса, задаваемой W. Третье равенство показывает, что перемена второго бита коммутирует с заменой базиса W. Четвертое — что перемена первого бита при неизменном втором бите в повернутом базисе означает одновременную перемену обоих битов в исходном базисе.

Дадим теперь определение симплектического кода. В пространстве $\mathcal{N} = \mathbb{B}^{\otimes n}$ мы веделим подпространство $\mathcal{M}$ условиями $X_j|\xi\rangle = |\xi\rangle$ (X_j будем называть *проверочными операторами*). Проверочные операторы будут иметь вид

$$X_j = (-1)^{\phi_j}\sigma(f_j), \quad f_j \in G^n, \quad \phi_j \in \{0,1\}. \tag{$*$}$$

Без ограничения общности можно считать, что $\{f_j\}$ линейно независимы. Потребуем еще, чтобы все операторы X_j коммутировали. Поскольку $X_jX_k = (-1)^{\omega(f_j,f_k)}X_kX_j$, условие коммутирования означает, что $\omega(f_j,f_k) = 0$.

Определение. *Симплектический квантовый код* задается условиями $(*)$, где все X_j коммутируют.

Итак, симплектическому квантовому коду соответствует изотропное подпространство $F \subseteq G^n$; изотропность означает, что для любых $f,g \in F$ выполнено $\omega(f,g) = 0$.

Теорема. $\dim\mathcal{M} = 2^{n-\dim F}$.

Лемма. *Любой симплектический код приводится преобразованиями из* $\mathrm{ESp}_2(n)$ *к стандартному виду, когда первые* $s = \dim F$ *бит равны 0.*

Действительно, подпространство $F \subseteq G^n$ можно перевести симплектическим преобразованиям в подпространство F', состоящее из векторов вида $(0,\beta_1,0,\beta_2,\ldots,0,\beta_s,0,\ldots,0)$, где β_i — произвольные.

Теперь посмотрим, какие ошибки способен замечать симплектический код. Напомним, что код замечает ошибки из $E(n,k)$, если

$$\forall\, Z \in \mathcal{E}(n,k)\ |\xi\rangle,|\eta\rangle \in \mathcal{M}\ \Big(\langle\xi|Z|\eta\rangle = c(Z)\langle\xi|\eta\rangle\Big). \tag{$**$}$$

По соображениям линейности, достаточно рассматривать лишь $Z = \sigma(g)$, $|g| \le k$.

Пусть $|\eta\rangle \in \mathcal{M}$, т. е. $(-1)^{\phi_j}\sigma(f_j)|\eta\rangle = |\eta\rangle$ для всех j. Обозначим $Z|\eta\rangle = |\psi\rangle$, где $Z = \sigma(g)$. Как мы сейчас увидим, вектор $|\psi\rangle$ является собственным для всех проверочных операторов X_j, поэтому он либо принадлежит кодовому подпространству $\mathcal{M}$, либо ему ортогонален. Подействуем проверочным оператором на $|\psi\rangle$:

$$X_j|\psi\rangle = (-1)^{\phi_j}\sigma(f_j)\sigma(g)|\eta\rangle = (-1)^{\omega(f_j,g)}ZX_j|\eta\rangle = (-1)^{\omega(f_j,g)}Z|\eta\rangle = (-1)^{\omega(f_j,g)}|\psi\rangle.$$

Условие $|\psi\rangle \in \mathcal{M}$ равносильно условию $\forall j\ \omega(f_j,g) = 0$. Такие g образуют линейное подпространство, которое мы обозначим F_+, т. е. $F_+ = \{g \in G^n : \forall\, f \in F\ \omega(f,g) = 0\}$.

Возможны следующие три случая:

1) $g \notin F_+$. При этом $|\psi\rangle \perp \mathcal{M}$, поэтому $\langle\xi|\sigma(g)|\eta\rangle = 0$. Такую ошибку код заметит.

2) $g \in F$. Такую ошибку код не заметит, но она несущественна, т. е. не меняет кодового вектора $|\eta\rangle$ (с точностью до фазового множителя). Пусть $g = a_1 f_1 + \cdots + a_s f_s$, тогда $\sigma(g) = c(g) X_1^{a_1} \ldots X_s^{a_s}$, где $c(g) = \pm 1, \pm \mathrm{i}$. В этом случае $\langle\xi|\sigma(g)|\eta\rangle = c(g)\langle\xi|\eta\rangle$.

3) $g \in F_+ \setminus F$. В этом случае (проверьте!) $\langle\xi|\sigma(g)|\eta\rangle$ не имеет вида $c(g)\langle\xi|\eta\rangle$. Такую ошибку код не замечает, и это плохо.

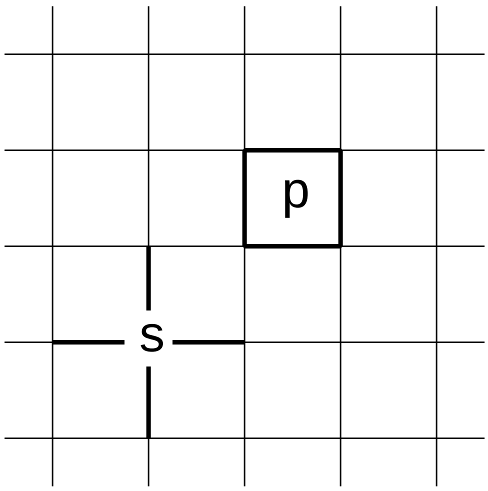
Этими рассуждениями доказана теорема.

Теорема. *Кодовое расстояние для симплектического кода равно*

$$d(\mathcal{M}) = \min\{|f| : f \in F_+ \setminus F\}$$

Заметим отличие от классических линейных кодов. Там кодовое расстояние определялось как наименьшая норма вектора из подпространства с выкинутым нулем. А для симплектических кодов нуль раздулся до подпространства.

Пример: торические коды.



Приведем важный пример симплектического кода. Он строится так. Пусть есть квадратная решетка на торе размера $r \times r$. q-биты соответствуют ребрам этой решетки. Таким образом, всего имеется $n = r^2$ q-битов. Проверочные операторы будут двух типов.

Тип I задается гранями. Выберем некоторую грань p и сопоставим ей проверочный оператор

$$A_p = \sigma(f_p^{(z)}) = \prod_{j \in \textit{граница}(p)} \sigma_j^z.$$

Тип II задается вершинами. Выберем некоторую вершину s и сопоставим ей проверочный оператор

$$B_s = \sigma(f_s^{(x)}) = \prod_{j \in \textit{звезда}(s)} \sigma_j^x.$$

Операторы A_p и B_s коммутируют, поскольку граница и звезда всегда пересекаются по четному числу ребер. (Перестановочность операторов одного типа очевидна).

Хотя мы указали $r^2 + r^2 = 2r^2$ проверочных операторов (по одному на грань и на вершину), между ними есть соотношения. Произведение всех A-операторов, как и произведение всех B-операторов, равны тождественному. Можно показать, что других соотношений нет. Поэтому $\dim F = 2r^2 - 2$, а $\dim \mathcal{M} = 2^2$. Торический код позволяет закодировать 2 q-бита. Посмотрим, чему равно кодовое расстояние для торического кода.

В случае торического кода имеются естественные разложения

$$F = F^{(x)} \oplus F^{(z)} \qquad F_+ = F_+^{(x)} \oplus F_+^{(z)}$$

на подпространства, соответствующие проверочным операторам, связанным с гранями и с вершинами. Элементы подпространств $F^{(z)}$, $F_+^{(z)}$ имеют вид $(0, \beta_1, \ldots, 0, \beta_n)$; им можно сопоставить 1-цепи, т. е. формальные линейные комбинации ребер с коэффициентами $\beta_1, \ldots, \beta_n \in \mathbb{F}_2$. Элементам подпространств $F^{(x)}$, $F_+^{(x)}$ сопоставляются 1-коцепи. Рассмотрим вектор $f_p^{(z)} \in F^{(z)}$, отвечающий грани с номером p. Ему будет сопоставлена 1-цепь, являющаяся границей этой грани. Легко видеть, что пространство $F^{(z)}$ состоит из всех 1-границ. Аналогично, векторам $f_s^{(x)}$ будут сопоставляться 1-кограницы, порождающие все пространство 1-кограниц.

Возьмем произвольный элемент $g \in F_+,\ \ g = g^{(x)} + g^{(z)}$. Условия коммутирования перепишутся следующим образом:

$$\omega(f_s^{(x)}, g) = 0 \ \Leftrightarrow\ \omega(f_s^{(x)}, g^{(z)}) = 0$$
$$\omega(f_p^{(z)}, g) = 0 \ \Leftrightarrow\ \omega(f_p^{(z)}, g^{(x)}) = 0$$

Чтобы выполнялось $\omega(f_s^{(x)}, g^{(z)}) = 0$, нужно, чтобы в любой звезде было четное число ребер с ненулевыми весами из $g^{(z)}$. Другими словами $g^{(z)}$ — это 1-цикл. Аналогично, $g^{(x)}$ должен быть 1-коциклом.

Итак, пространства $F_+^{(z)}$, $F_+^{(x)}$ состоят из 1-циклов и 1-коциклов, а пространства $F^{(z)}$, $F^{(x)}$ состоят — из 1-границ и 1-кограниц. Следовательно, кодовое расстояние есть минимальная мощность (количество ненулевых коэффициентов) по циклам, не являющимся границами, и коциклам, не являющимся кограницами. Легко видеть, что этот минимум равен r (нужны либо цикл, либо разрез, не гомологичные 0). Это означает, что торический код исправляет $\lfloor (r-1)/2 \rfloor$ ошибок.

Будем обозначать коды описанного вида через $\mathrm{TOR}(r)$.

Замечание. Торические коды являются очень важным примером, обладающим рядом замечательных свойств. В частности, это *коды с локальными проверками.* Последовательность кодов называется кодами с локальными проверками, если выполнены следующие условия:

– каждый проверочный оператор действует на ограниченное константой число q-бит;

– каждый q-бит входит в ограниченное константой число проверочных операторов;

– кодовое расстояние неограниченно возрастает.

Такие коды представляют интерес для задачи построения вычислительных схем, устойчивых к ошибкам. При исправлении ошибок могут происходить новые ошибки. Но для кодов с локальными проверками схемы исправления ошибок имеют фиксированную глубину, поэтому одна ошибка при работе такой схемы портит ограниченное число q-бит.

Процедура исправления ошибок (симплектические коды)

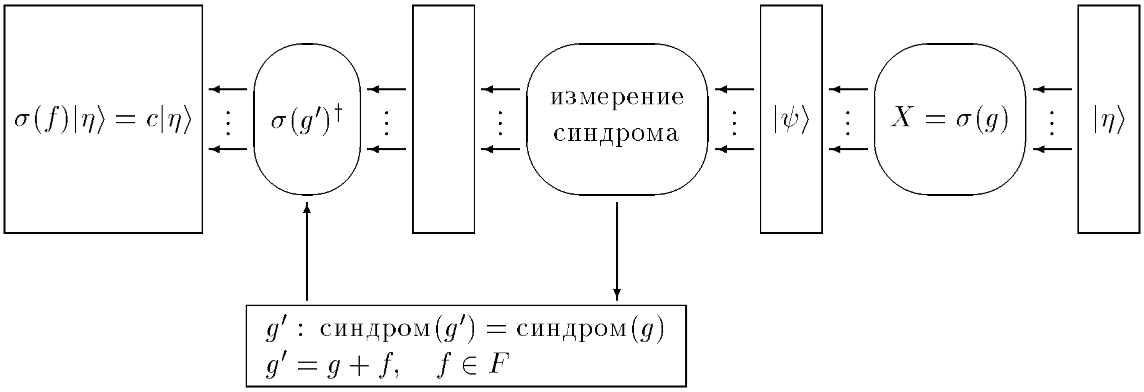
Вспомним, что $Z = Y^\dagger X$, $X = \sigma(g_1)$, $Y = \sigma(g_2)$. Тогда $Z = c\sigma(g_1 - g_2)$ $\ (|c| = 1)$. Назовем *синдромом* ошибки g_1 вектор $(\omega(g_1, f_1), \ldots, \omega(g_1, f_s))$ (для g_2 — аналогично).

Пусть $|\eta\rangle \in \mathcal{M}$. Обозначим $|\psi\rangle = X|\eta\rangle$. Проверочные операторы действуют на $|\psi\rangle$ так: $X_j|\psi\rangle = (-1)^{\omega(g_1, f_j)}|\psi\rangle$.

Если кодовое расстояние равно k, то выполнено

$$\forall\, g_1, g_2\ \Big((|g_1| \le k, |g_2| \le k) \Rightarrow \big((g_1 - g_2 \in F) \vee (g_1 - g_2 \notin F_+) \big) \Big).$$

Условие $g_1 - g_2 \in F$ означает эквивалентность ошибок g_1 и g_2, то есть $\sigma(g_1)|\eta\rangle = c\sigma(g_2)|\eta\rangle$ для любого вектора $|\eta\rangle$ из кодового подпространства. Условие $g_1 - g_2 \in F_+$ равносильно тому, что синдромы ошибок g_1 и g_2 не совпадают. Итак либо ошибки эквивалентны, либо их можно различить по синдрому. Следовательно, по синдрому можно определить ошибку с точностью до эквивалентности, т. е. по модулю подпространства F.



Сх. 1. Исправление ошибки.

Теперь ясно, как нужно исправлять ошибку. После того как опредлен синдром, применим оператор, обратный к оператору восстановленной по синдрому ошибки. Получим состояние, отличающееся от исходного лишь на фазовый множитель.

Выше рассмотрен случай одной ошибки. На самом деле ошибка состоит в действии преобразования матриц плотности вида

$$T = \sum_{|h|\le k, |h'|\le k} b_{h,h'}\sigma(h) \cdot \sigma(h')^\dagger,$$

где на место $\cdot$ нужно подставлять матрицу плотности.

В качестве упражнения проверьте как работает приведенная выше схема в случае такого общего преобразования матриц плотности.

Общее определение исправляющего ошибки преобразования дается так. Исправляющее преобразование $P : \mathbf{L}(\mathcal{N}) \to \mathbf{L}(\mathcal{N})$ исправляет ошибки из $\mathcal{E}$, если

$$\forall\, T \in \mathcal{E} \cdot \mathcal{E}^\dagger \;\exists\, c = c(T) \;\forall\, \rho \in \mathbf{L}(\mathcal{M}) \;\Big(PT\rho = c(T)\rho\Big).$$

Если при этом T сохраняет след, то $c(T) = 1$.

Можно доказать следующую теорему.

Теорема. *Исправляющее преобразование существует тогда и только тогда, когда код $\mathcal{M}$ исправляет ошибки из $\mathcal{E}$.*