ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—февраль 2015. Том 22, № 1. С. 86–99

УДК 519.178

О ПОИСКЕ АНТИПОДАЛЬНЫХ ВЕРШИН В СИММЕТРИЧНОМ ГРАФЕ КЭЛИ ГРУППЫ БУЛЕВА КУБА

И. М. Хузиев[1]
[1]Московский физико-технический институт,
ул. Первомайская, 5, корп. 2, 141700 Долгопрудный, Россия
e-mail: ilnur.khuziev@yandex.ru

Аннотация. Вводится отношение антиподальности в графе и задача поиска антиподальной вершины. Приводится вероятностный алгоритм решения оракульной задачи для симметричного графа Кэли над группой $\mathbb{Z}_2^n$, когда число запросов к оракулу полиномиально по степени вершин. Ил. 1, библиогр. 5.

Ключевые слова: граф, автоморфизм, антиподальность, оракул.

Введение

В данной работе рассматриваются оракульные задачи поиска на графах. Оракульные задачи (решающие деревья) имеют доступ к входу через оракул. Сложность алгоритма измеряется количеством запросов к оракулу. В задаче с априорной информацией предполагается, что вход задачи удовлетворяет некоторым свойствам. Другими словами, алгоритм решения задачи обязан корректно работать не на всех входах, а только на тех, которые удовлетворяют указанным свойствам.

Одним из видов оракульных задач являются задачи поиска на графах. Задано семейство графов F, оракул предоставляет доступ к следующей информации: ячейкам матрицы смежности графа, изоморфного $f_n \in F$, числу n, имени начальной вершины. Требуется найти вершину, «парную» к начальной (отношение, в котором должны стоять начальная вершина и верный ответ алгоритма, определяется конкретной задачей). Например, требуется найти вершину, находящуюся на расстоянии диаметра.

Ниже формулируем частный случай такой задачи — задачу поиска антиподальной вершины — и приводим достаточно эффективный вероятностный алгоритм её решения для симметричных графов Кэли группы $\mathbb{Z}_2^n$.

Эта задача связана с одним из самых важных вопросов современной теоретической информатики — сравнением возможностей классических и квантовых алгоритмов.

Известно некоторое количество оракульных задач с априорной информацией (promise problem), в которых квантовые алгоритмы экспоненциально лучше классических (см., например, [2]).

В [3] показано, что квантовое блуждание[1)] экспоненциально быстрее любого оракульного вероятностного алгоритма находит диаметрально противоположную вершину в специально построенном семействе графов.

Возникает вопрос: в каких семействах графов можно доказать экспоненциальный разрыв с помощью квантового блуждания и аналогичной оракульной постановки задачи? В [3] показывается, что для задачи поиска диаметрально противоположной вершины в булевом кубе разрыв не более чем полиномиальный. Естественным обобщением графа булева куба являются симметричные графы Кэли над группой $\mathbb{Z}_2^n$, свойства которых рассматриваются в разд. 1.

Определение 1. *Граф Кэли* $\mathrm{Cay}(G, S)$ над группой G с множеством образующих S — это граф (V, E), где $V = G$, и $(v_1, v_2) \in E$ равносильно существованию такого $e \in S$, что $ev_1 = v_2$. Будем предполагать, что $S^{-1} = S$ (граф неориентированный) и $1 \notin S$ (вершины не имеют петель). Если $S = \{e \in \mathbb{Z}_2^n \mid |e| = s\}$, то $\mathrm{Cay}\big(\mathbb{Z}_2^n, S\big)$ будем обозначать через $\mathrm{Cay}(s)$.

Квантовое блуждание в булевом кубе исследовалось в [4]. Оно обладает таким свойством: начавшись в вершине $(0, \ldots, 0) \in \mathbb{Z}_2^n$, квантовое блуждание в некоторый момент времени сконцентрировано в вершине $(1, \ldots, 1) \in \mathbb{Z}_2^n$. В графе $\mathrm{Cay}(s)$ квантовое блуждание обладает аналогичным свойством [5], но в отличие от булева куба и склеенных бинарных деревьев из [3] для вершины из $\mathrm{Cay}(s)$ может существовать несколько вершин, отстоящих от данной на расстояние диаметра графа. Поэтому требуется сформулировать другую оракульную задачу. Для этого требуется ответить на вопрос: можно ли по матрице смежности графа, изоморфного $\mathrm{Cay}(s)$, понять, какие пары вершин являются диаметрально противоположными в терминах расстояния Хэмминга?

В данной работе даётся положительный ответ на этот вопрос. Для этого в разд. 2 вводится понятие антиподальной вершины. Отношение антиподальности и постановка оракульной задачи для поиска антиподальной вершины обобщают задачу поиска диаметрально противопо-

[1)] Квантовое блуждание является естественным обобщением классического случайного блуждания и исследуется во многих работах. Достаточно подробно о квантовом блуждании можно прочитать в [4, 5].

ложной вершины из [3].

Главным результатом этой статьи является вероятностный алгоритм поиска антиподальной вершины в $\mathrm{Cay}(s)$ (разд. 2). Из оценки на число запросов к оракулу этого алгоритма следует, что при фиксированных s разрыв между классическими и квантовыми алгоритмами в оракульной задаче поиска антиподальной вершины в графе $\mathrm{Cay}(s)$ не более чем полиномиальный.

Корректность алгоритма поиска антиподальной вершины основана на теореме о локальных связях, которая доказывается в разд. 3. Результат теоремы 3 интересен и сам по себе. При рассмотрении графов $\mathrm{Cay}(s)$ полезным инструментом оказывается граф слоёв (слой — множество вершин с одинаковым весом Хэмминга), получаемый из графа отождествлением всех вершин слоя. Теорема о локальных связях утверждает, что если между парой вершин в графе $\mathrm{Cay}(s)$ есть путь длины 2, то проекции всех путей длины 2 между этими вершинами дают в графе слоёв все пути длины 2 между проекциями этих вершин.

1. Структура графа $\mathrm{Cay}(s)$

В общем случае задача описания группы автоморфизмов графа является сложной, но для $\mathrm{Cay}(s)$ её удаётся решить.

В [1] доказано, что всякий автоморфизм графа $\mathrm{Cay}(s)$ сохраняет хэммингово расстояние 2 при $s \notin \left\{\frac{n}{2}, \frac{n-1}{2}, \frac{n+1}{2}, n\right\}$.

Данный результат позволяет без особого труда доказать следующие утверждения.

Теорема 1 [1]. *Пусть $s \notin \left\{\frac{n}{2}, \frac{n-1}{2}, \frac{n+1}{2}, n\right\}$ и s нечётно. Тогда множество автоморфизмов $Cay(s)$ совпадает с автоморфизмами булева куба $Cay(1)$.*

Замечание 1. Всякий автоморфизм булева куба f может быть представлен в виде $f = h \circ g$, где g — сдвиг, а f — перестановка координат.

Автоморфизм сдвига, порождённый вектором $v_0 = (x_1, \ldots, x_n)$, где $x_i \in \mathbb{Z}_2$, действует по правилу $g_{v_0}(u) = u + v_0$.

Автоморфизм перестановки координат, порождённый перестановкой на n элементах σ, действует по правилу $f_\sigma(v) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

Теорема 2. *Пусть $s \notin \left\{\frac{n}{2}, \frac{n-1}{2}, \frac{n+1}{2}, n\right\}$ и s чётно. Тогда каждая из двух компонент связности графа $Cay(s)$ имеет множество автоморфизмов, порождённое сдвигами на векторы чётного веса Хэмминга и перестановками координат.*

Опишем некоторые свойства графов $\mathrm{Cay}(s)$, которые потребуются далее. Отдельно отметим лемму 1, из которой следуют теоремы 1 и 2 при дополнительном ограничении $6s \leqslant n$.

Для полноты изложения приведём доказательство широко известного утверждения.

Утверждение 1. *Пусть $s < n$. Тогда*

(i) *если s чётно, то $\mathrm{Cay}(s)$ имеет 2 компоненты связности — вершины чётного и нечётного весов*;

(ii) *если s нечётно, то граф $\mathrm{Cay}(s)$ имеет одну компоненту связности.*

Доказательство. Обозначим линейную оболочку множества S (в пространстве $\mathbb{Z}_2^n$) через $\mathrm{Lin}(S)$. Легко видеть, что множество вершин, достижимых из v, равно $v + \mathrm{Lin}(S) = \{v + e \mid e \in \mathrm{Lin}(s)\}$.

(i) Все элементы $\mathrm{Lin}(S)$ имеют чётный вес. Покажем, что $\mathrm{Lin}(S)$ содержит все векторы веса 2. Рассмотрим произвольные числа $m \neq k$ (номера координат). Выберем некоторый вектор $e_1 \in S$, имеющий единицу на k-й позиции и нуль на m-й; вектор e_2 строится из вектора e_1 инвертированием m-й и k-й координат. Тогда вектор $e_1 + e_2 \in \mathrm{Lin}(S)$ имеет единицы только в m-й и k-й координатах. Следовательно, $\mathrm{Lin}(S)$ содержит все векторы чётного веса. Значит, если разность двух векторов имеет чётный вес, то они лежат в одной компоненте связности.

Используя соотношение $|v+u| \equiv |v|+|u| \pmod 2$, получаем, что вершины чётного и нечётного весов не могут быть связаны в графе $\mathrm{Cay}(s)$.

(ii) Аналогично п. (i) $\mathrm{Lin}(S)$ содержит все векторы чётного веса. Так как $\mathrm{Lin}(S)$ содержит вектор нечётного веса, $\mathrm{Lin}(S)$ также содержит все векторы веса 1. Но эти векторы порождают всё пространство $\mathbb{Z}_2^n$ (они образуют базис). Утверждение 1 доказано.

Определение 2. *Слоем веса p* называется множество $L_p = \{v \in V \mid |v| = p\}$. Будем для удобства ассоциировать слой и его вес.

Определение 3. Определим *граф слоёв*. Множество вершин этого графа есть $V' = \{L_p \mid p \in \{1, \ldots, n\}\}$. Множество рёбер E' состоит из таких пар слоёв (L_p, L_q), что найдутся вершины $v \in L_p,\ u \in L_q$, между которыми есть ребро в $\mathrm{Cay}(s)$: $(v, u) \in E$.

Утверждение 2 (связность слоёв). *Слои, связанные со слоём l, составляют множество*

$$N(l) = \{t \in [|l - s|, \min(l + s,\ 2n - (l + s))] \mid t \equiv |l - s| \bmod 2\}.$$

Доказательство. Пусть вершина v имеет вес l и вершина u — сосед v. Значит, существует образующая e такая, что $|e| = s$ и $u = v + e$. Обозначим вектор $(v_1 \cdot u_1, \ldots, v_n \cdot u_n)$ через $v \cap u$.

Пусть $p = |e \cap v|$ — число координат, которые равны единице в векторах e и v. Ясно, что p не может быть меньше $l + s - n$. Значит,

$$\max(0, l + s - n) \leqslant p \leqslant \min(|v|, |e|) = \min(l, s). \tag{1}$$

Заметим, что (i) $l - p$ координат равны единице в векторе v, но равны нулю в e, (ii) $s - p$ координат равны единице в векторе e, но равны нулю в v. Отсюда

$$|u| = (l - p) + (s - p) = (l + s) - 2p. \tag{2}$$

Объединяя (1) и (2), получаем

$$(l + s) - 2\min(l, s) \leqslant |u| \leqslant l + s - 2\max(0, l + s - n). \tag{3}$$

Поскольку $(l + s) - 2\min(l, s) = |l - s|$, из (3) следует включение:

$$N(l) \subset \big\{t \in [|l - s|, \min(l + s, n - (l + s - n))] | t \equiv |l - s| \bmod 2\big\}.$$

Для доказательства включения в обратную сторону достаточно заметить, что оценка (1) точна для всех v. Утверждение 2 доказано.

Утверждение 3 (число связей). *Дан граф Cay(s). Пусть $(l, t) \in E'$. Тогда каждый вектор v, $|v| = l$, имеет*

$$\binom{l}{(s + l)/2 - t/2}\binom{n - l}{(s + t)/2 - l/2}$$

соседей веса t в графе Cay(s).

Доказательство. Пусть $|v| = l$, $e \in S$ и $p = |e \cap v|$. Тогда $|v + e| = t$ равносильно условию $(l - p) + (s - p) = t$. Значит, $p = (s + l - t)/2$. Число векторов e таких, что $|e| = s$, $|e \cap v| = p$, равно

$$\binom{l}{p}\binom{n - l}{s - p} = \binom{l}{(s + l)/2 - t/2}\binom{n - l}{(s + t)/2 - l/2}.$$

Утверждение 3 доказано.

Лемма 1. *Определим*

$$k(l) = \binom{l}{l/2}\binom{n - l}{s - l/2}$$

для $0 \leqslant l \leqslant 2(s - 1)$, где l чётно. Пусть $6s \leqslant n$. Тогда $k(l + 2) < k(l)$.

Доказательство. Из определения получаем

$$k(l+2) = k(l)\frac{(l+1)(l+2)(s-l/2)(n-l-s+l/2)}{(l/2+1)^2(n-l-1)(n-l)}.$$

Утверждение леммы следует из следующей оценки:

$$\begin{aligned}&\frac{(l+1)(l+2)(s-l/2)(n-l-s+l/2)}{(l/2+1)^2(n-l-1)(n-l)}\\ &= \frac{4(l+1)(s-l/2)(n-l-s+l/2)}{(l+2)(n-l-1)(n-l)} \leqslant 4\frac{l+1}{l+2}\frac{s(n-s)}{(n-2s+1)(n-2s+2)}\\ &\qquad < 4\frac{(n/s-1)}{(n/s-2+1/s)(n/s-2+2/s)} \leqslant 4\frac{(n/s-2)}{(n/s-2)(n/s-2)} \leqslant 1.\end{aligned}$$

Лемма 1 доказана.

Ниже приводятся доказательства теорем 1 и 2. Как показано в [1], в них достаточно использовать равенство $\operatorname{argmax} k(l) = 2$. Однако далее потребуется и доказанная в лемме 1 монотонность функции $k(l)$. Из этой леммы также следует, что $\arg\max\limits_{l} k(l) = 2$ при $6s \leqslant n$.

Следствие 1. *Пусть* $s \notin \left\{\frac{n-1}{2}, \frac{n}{2}, \frac{n+1}{2}, n\right\}$, $f \in \operatorname{Aut} G(s)$. *Если* 0^n *является неподвижной точкой* f, *то каждый слой под действием* f *переходит в себя.*

Доказательство. Убедимся, что в случае нечётного s достаточно показать, что множество L_1 инвариантно относительно действия автоморфизма f.

Действительно, пусть доказано

Утверждение 4. *Всякий автоморфизм* f, *сохраняющий точку* v, *сохраняет множество* $L_1^v = \{u \in V \mid |v-u| = 1\}$.

Тогда для автоморфизма f существует такая перестановка координат σ, что $f_\sigma \circ f$ сохраняет все точки множества L_1. Применив для автоморфизма $f_\sigma \circ f$ утверждение 4 ко всем точкам множества L_1, получим, что L_2 сохраняется под действием $f_\sigma \circ f$, т. е. L_2 сохраняется и под действием f. Продолжая эти рассуждения, получим, что сохраняются все слои.

В случае чётного s аналогично показывается, что из инвариантности множества L_2 следует утверждение теоремы 2.

Перейдём теперь к доказательству инвариантности первого и второго слоёв.

Если 0^n неподвижна, то множество L_s также инвариантно.

Пусть $k(v)$ — число вершин u таких, что $(v,u) \in E$ и $|u| = s$. Так как L_s и матрица смежности инвариантны, то $k(v) = k(f(v))$. Значит, функция $k(v)$ зависит только от веса вектора v. Из утверждения 3 имеем $k(l) = k(v)$, где $|v| = l$.

Для каждого $l \notin [0, 2s]$ выполнено $k(l) = 0$. В силу леммы 1 если $l, l' \in [0, 2s]$ и l, l' чётны, то $k(l) \neq k(l')$. Поэтому из утверждения 2 следует $k(l) \neq k(l')$ для любых слоёв l, l', связанных со слоем s.

Стало быть, если $v \in L_l$, $l \in [0, 2s]$, l чётно, то $f(v) \in L_l$. Другими словами, L_l инвариантно.

Пусть s чётно. С учётом вышесказанного L_2 инвариантно.

Пусть s нечётно. Тогда слои L_{s-1} и L_{s+1} инвариантны. Используя условие $6s \leqslant n$ и утверждение 2, получаем, что L_1 — единственный слой, который связан только со слоями $s-1$ и $s+1$. Значит, L_1 инвариантно. Следствие 1 доказано.

2. Отношение антиподальности

Определение 4. Пусть дан граф G. Вершина u называется *антиподальной* для вершины v, если для любого автоморфизма $f \in \operatorname{Aut} G$, сохраняющего вершину v, $f(v) = v$, выполняется также $f(u) = u$.

Замечание 2. В общем случае отношение антиподальности является рефлексивным и транзитивным, но необязательно симметричным.

Определим теперь оракульную задачу поиска антиподальной вершины в регулярном графе. Пусть $G = (V, E)$ — граф и $|V| \leqslant 2^n$. Функция $f : V \to \{0,1\}^{2n}$ задаёт отображение вершин в имена (строки). Число возможных имён экспоненциально больше числа вершин.

Алгоритм может отправить оракулу имя вершины и число. Оракул ответит именем соседа переданной вершины, соответствующего переданному числу. Если имя вершины или число некорректны, то оракул возвращает пустую строку.

Алгоритму на вход подаётся имя любой вершины v. Алгоритм решает задачу поиска антиподальной вершины, если на выходе будет выведено имя одной из антиподальных к v вершин.

Сложностью алгоритма будем называть число его запросов к оракулу в худшем случае. *Сложностью задачи* (на семействе графов) назовём минимальную сложность алгоритма, решающего задачу.

Через $f(G) = (f(V), f(E))$ обозначим образ графа G, порождаемый отображением f. Заметим, что $f(G)$ изоморфен G.

Далее будем рассматривать задачу поиска антиподальной вершины для семейства симметричных графов Кэли над группой $\mathbb{Z}_2^n$.

Будем называть *условиями связности* условия (i) $s \notin \left\{n, \frac{n}{2}, \frac{n-1}{2}, \frac{n-1}{2}\right\}$, (ii) либо s нечётно, либо n чётно. Заметим, что условие (ii) необходимо и достаточно для того, чтобы противоположные вершины находились в одной компоненте связности $\mathrm{Cay}(s)$. (Вершину v называем *противоположной* u, если $|u - v| = n$.)

Результаты разд. 1 говорят, что если выполнены условия связности, то каждая вершина $\mathrm{Cay}(s)$ имеет ровно одну антиподальную вершину: согласно теоремам 1 и 2 единственная вершина из L_n является антиподальной, найдутся перестановки, которые не сохраняют вершины из слоёв $L_p,\ p \neq n$, (например, циклическая перестановка $\sigma = (2, 3, \ldots, n, 1)$ не сохраняет ни одной вершины, кроме 0^n и 1^n).

Теорема 3. *Пусть $s \leqslant n/6$ и выполнены условия связности. Тогда существует вероятностный алгоритм, который решает задачу поиска антиподальной вершины с вероятностью $1-o(1)$ и число запросов к оракулу равно $O\big(m^4\ \frac{n}{s}\big)$, где $m = \binom{n}{s}$ — степень вершин графа.*

Замечание 3. Тривиальной верхней оценкой для связных графов является $2|E| = \sum\limits_{v \in V} \deg v$: за такое число запросов можно узнать всю структуру графа, запросив в каждой вершине имена всех её соседей. Если s растёт не слишком быстро, то приводимый алгоритм экспоненциально (по n) лучше тривиальной оценки.

Ниже приведено описание вспомогательного алгоритма по шагам, затем показана корректность алгоритма. Количество запросов к оракулу, которое делает вспомогательный алгоритм, очевидно из описания. Этот алгоритм используется как процедура при построении алгоритма для теоремы 3.

2.1. Описание вспомогательного алгоритма. Пусть v_0 — имя начальной вершины. Без ограничения общности можно считать, что v_0 — образ вершины 0^n.

Шаг инициализации

1. Алгоритм делает m запросов, чтобы узнать имена всех соседей v_0. Полученное множество обозначим через $N(v_0)$.

2. Алгоритм выбирает случайный элемент $v_1 \in N(v_0)$.

3. Для каждого u — соседа v_1 (т. е. $(u, v_1) \in f(E)$) — алгоритм находит вес вершины $f^{-1}(u)$, выполняя следующие действия:

(a) получить имена всех соседей вершины u;

(b) вычислить x — число соседей u из множества $N(v_0)$;

(c) вычислить $|f^{-1}(u)| = k^{-1}(x)$.

Этот шаг требует m^2 запросов.

4. Выполняется присваивание $t = 1$.

На шаге t алгоритм хранит в памяти следующее:

1) имя вершины v_t, причём $|f^{-1}(v_k)| = ts$,

2) множество $N(v_t) = \{u \in f(V) \mid (u, v_t) \in f(E)\}$,

3) число $|f^{-1}(u)|$ для каждого $u \in N(v_t)$.

Если шаг $(t+1)s \leqslant n$, то

1. Алгоритм выбирает случайную вершину $v_{t+1} \in N(v_t)$, для которой выполнено $|f^{-1}(v_{t+1})| = (t+1)s$.

2. Алгоритм делает m запросов, чтобы построить множество $N(v_{t+1})$.

3. Для каждого $u \in N(v_{t+1})$ алгоритм вычисляет

$$j(u) = \min_{x \in N(v_t) \cap N(u)} |f^{-1}(x)|.$$

Эта операция требует m запросов для каждого u.

Алгоритм вычисляет вес прообраза вершины u по формуле $|f^{-1}(u)| = j(u) + s$.

4. Выполняется присваивание $t := t + 1$.

Если $(t+1)s = n$, то

Алгоритм в множестве $N(v_t)$ находит элемент с весом $|f^{-1}(u)| = n$ и выдаёт ответ.

Если $(t+1)s > n$, то

1. Алгоритм выбирает произвольную вершину $v_{t+1} \in N(v_t)$, для которой выполнено $|f^{-1}(v_{t+1})| = n - s$.

2. Алгоритм выбирает случайное число $i \in \{1, \ldots, m\}$, запрашивает i-го соседа v_{t+1} и возвращает ответ оракула.

2.2. Доказательство корректности вспомогательного алгоритма.

Утверждение 5. *Вспомогательный алгоритм правильно определяет веса вершин v_i на всех промежуточных шагах. С вероятностью не меньше $\frac{1}{m}$ алгоритм находит антиподальную вершину.*

Доказательство. Рассмотрим шаг инициализации, $N(v_0)$ — в точности множество $f(L_s)$. Выбранный элемент v_1 является элементом веса s. Согласно лемме 1 функция k обратима на множестве возможных x. Значит, число $k^{-1}(x)$ действительно равно весу прообраза $|f^{-1}(u)|$.

Итак, корректность алгоритма на первом шаге проверена. По индукции докажем корректность алгоритма на следующих шагах.

Пусть $(t+1)s \leqslant n$. В предположении корректности предыдущего шага в множестве $N(v_t)$ должны быть вершины u со свойством $|f^{-1}(u)| = (t+1)s$, т. е. выбор v_{t+1} возможен. Согласно теореме о локальных связях (разд. 3) для всякой вершины $u \in N(v_{t+1})$ выполнено соотношение

$$j(u) = |f^{-1}(u)| - s.$$

Таким образом, веса прообразов вершин из $N_{v_{t+1}}$ определяются алгоритмом корректно.

Если $(t+1)s = n$, то в предположении корректности предыдущих шагов ровно один из соседей v_t является вершиной веса n. Поэтому алгоритм даёт правильный ответ.

Если $(t+1)s > n$, то из утверждения 2 следует, что один из соседей v_{t+1} является вершиной веса n. Поэтому с вероятностью $\frac{1}{m}$ алгоритм даёт правильный ответ. Утверждение 5 доказано.

Легко видеть, что 1) число шагов $\leqslant \frac{n}{s}$, каждый шаг требует m^2+m запросов, 2) если $s \mid n$, то алгоритм даёт правильный ответ, 3) если $s \nmid n$, то алгоритм даёт верный ответ с вероятностью $\frac{1}{m}$. В любом случае ответом алгоритма является одна из вершин, связанных со слоём $n-s$. Из соображений симметрии вероятность того, что алгоритм даст ответ $v \in L_p$ из слоя, связанного со слоем $n-s$, равна $\frac{1}{|L_p|m}$.

2.3. Доказательство теоремы 3. Искомый алгоритм повторяет вспомогательный алгоритм mn раз и возвращает вершину, которая встречается среди ответов вспомогательного чаще всего.

Из неравенства Чебышёва следует, что правильный ответ будет возвращён хотя бы $\sqrt{n}$ раз с вероятностью $1-o(1)$. Из неравенства Чернова следует, что вероятность того, что вершина $v \in L_p$ будет возвращена более чем $\sqrt{n}$ раз, оценивается как $e^{-2\varepsilon^2 mn}$, где $\varepsilon = \frac{1}{\sqrt{n}} - \frac{1}{|L_p|m} = \frac{1+o(1)}{\sqrt{n}}$. Таким образом, получаем оценку сверху вероятности того, что какая-либо вершина веса меньше n встречается среди ответов вспомогательного больше чем $\sqrt{n}$ раз: $s\binom{n}{2s}e^{-2m} = o(1)$. Значит, верный ответ будет получен с вероятностью $1-o(1)$.

3. Теорема о локальных связях

Теорема 4. *Пусть вершины v, u, q таковы, что (v,u) и $(u,q) \in E$, $|v| = l$ и $|q| = t$. Тогда условие $(l,x),(t,x) \in E'$ равносильно существованию вершины $w \in L_x$ такой, что $(v,w),(w,q) \in E$.*

Доказательство. Найдём каждый слой x такой, что существуют векторы $e_1,\ e_2$ веса s, удовлетворяющие условиям $|v+e_1|=x$ и $v+e_1+e_2=q$, и покажем, что найденное множество совпадает с множеством слоёв, смежных со слоями l и t (рис. 1).

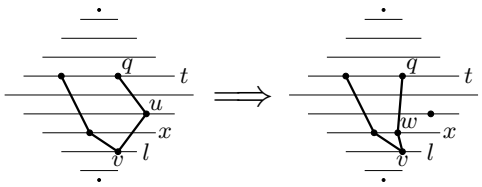

Рис. 1. Теорема о локальных связях. Можно пропустить путь между вершинами через любой допустимый слой

Заметим, что хэммингово расстояние между v и q не больше чем $2s$ и оно чётно (утверждение 2).

Разделим n координат на 4 части: первая размера $a=|v\cap q|$ — координаты, в которых оба вектора v и q имеют единицу, вторая размера b_1 — координаты, в которых v имеет единицу, исключая уже выбранные в первой части ($a+b_1=l$), третья размера b_2 — аналогично для q ($a+b_2=t$), четвёртая размера d — оставшиеся координаты (оба вектора имеют нули).

Пусть e_1 имеет $\alpha,\ \beta,\ \gamma,\ \delta$ единиц среди координат первой, второй, третьей и четвёртой частей соответственно. Тогда вектор e_2 должен иметь $\alpha,\ b_1-\beta,\ b_2-\gamma,\ -\ \delta$ единиц в соответствующих частях: в первой и четвёртой — на тех позициях, что и e_1, во второй и третьей — в тех позициях, где e_1 имеет нуль. Таким образом, e_2 полностью определяется вектором e_1.

Все параметры удовлетворяют следующим соотношениям:

$$\begin{gathered} b_1+b_2\leqslant 2s,\\ \alpha\leqslant a,\quad \beta\leqslant b_1,\quad \gamma\leqslant b_2,\quad \delta\leqslant d,\quad a+b_1+b_2+d=n,\\ |v|+(\gamma+\delta)-(\alpha+\beta)=|v+e_1|,\\ \alpha+\beta+\gamma+\delta=|e_1|=s,\quad \alpha+(b_1-\beta)+(b_2-\gamma)+\delta=|e_2|=s. \end{gathered}\tag{4}$$

Последние два соотношения дают $\beta+\gamma=\frac{b_1+b_2}{2}$, $\alpha+\delta=s-\frac{b_1+b_2}{2}$.

Легко заметить, что если $(\alpha,\beta,\gamma,\delta)$ удовлетворяет условиям (4), то существуют векторы e_1,e_2 с нужными свойствами.

Вес $|v+e_1|$ минимален, если вес $|v\cap e_1|$ максимален. Последнее выполняется при $\alpha=\min\left(a, s-\frac{b_1+b_2}{2}\right)$ и $\beta=\min\left(b_1,\frac{b_1+b_2}{2}\right)$. Таким образом, получили максимально возможное значение x:

$$\begin{aligned}\max x &= (a+b_1)+(\gamma+\delta)-(\alpha+\beta)=a+b_1+s-2(\alpha+\beta)\\ &= a+b_1+s-2(\min(a,s-(b_1+b_2)/2)+\min(b_1,(b_1+b_2)/2))\end{aligned}$$

$$= \max(s-a-b_1, a+b_1-s, s-a-b_2, a+b_2-s)$$
$$= \max(|l-s|, |t-s|) = A.$$

Вес $|v+e_1|$ максимален, если вес $|v \cap e_1|$ минимален. Последнее выполнено при $\delta = \min\left(d, s - \frac{b_1+b_2}{2}\right)$ и $\gamma = \min\left(b_2, \frac{b_1+b_2}{2}\right)$. Таким образом, получили минимально возможное значение x:

$$\begin{aligned}|v+e_1| &= (a+b_1)+(\gamma+\delta)-(\alpha+\beta) = a+b_1-s+2(\gamma+\delta)\\ &= a+b_1-s+2(\min(b_2,(b_1+b_2)/2)+\min(d, s-(b_1+b_2)/2))\\ &= \min((a+b_1+b_2+d)+(b_2+d-s), a+b_1+s, a+b_2+s,\\ &\qquad (a+b_1+b_2+d)+(b_2+d-s))\\ &= \min(\min(l+s, 2n-l-s), \min(t+s, 2n-t-s)) = B.\end{aligned}$$

Пусть $(\alpha, \beta, \gamma, \delta)$ — допустимый набор параметров, соответствующий векторам e_1, e_2. Заметим, что если набор $(\alpha', \beta', \gamma', \delta') = (\alpha-1, \beta, \gamma, \delta+1)$ допустим, то $|v+e_1'| = 2+|v+e_1|$; если набор $(\alpha'', \beta'', \gamma'', \delta'') = (\alpha, \beta-1, \gamma+1, \delta)$ допустим, то $|v+e_1''| = 2+|v+e_1|$; если $|v+e_1| \neq A$, то хотя бы один из этих двух наборов допустим.

Другими словами, числа $B, B+2, B+4, \ldots, A-2, A$ — все возможные значения для x. Таким образом,

$$\{x \mid \exists w \in L_x,\ (v,w),(v,q) \in E\} = \{x \in [B,A] \mid x \equiv |l-s| \bmod 2\}.$$

Из утверждения 2 следует, что

$$\{x \mid (x,l),(x,t) \in E'\} = \{x \in [B,A] \mid x \equiv |l-s| \bmod 2\}.$$

Теорема 4 доказана.

ЛИТЕРАТУРА

1. **Красин В. Ю.** О слабых изометриях булева куба // Дискрет. анализ и исслед. операций. Сер. 1. 2006. Т. 13, №4. С. 26–32.
2. **Нильсен М., Чанг И.** Квантовые вычисления и квантовая информация. М.: Мир, 2006. 824 с.
3. **Childs A. M., Cleve R., Deotto E., Farhi E., Gutmann S., Spielman D. A.** Exponential algorithmic speedup by quantum walk // Proc. 35th ACM Symp. Theory of Computing (STOC 2003). P. 59–68.
4. **Kempe J.** Discrete quantum walks hit exponentially faster // Proc. 7th Int. Workshop Randomization and Approximation Techniques in Computer Science (RANDOM'03). 2003. P. 354–369. (Lect. Notes Comput. Sci.;Vol. 2764).

5. Khuziev I. Quantum walk in symmetric Cayley graph over $\mathbb{Z}_2^n$. 2013. arXiv:1305.6849

Ильнур Масхудович Хузиев

Статья поступила
3 марта 2014 г.

Исправленный вариант —
26 августа 2014 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
January–February 2015. Volume 22, No. 1. P. 86–99

UDC 519.178

ABOUT SEARCHING FOR ANTIPODAL VERTEXES IN SYMMETRIC CAYLEY GRAPHS

I. M. Khuziev[1]
[1]Moscow Institute of Physics and Technology,
5/2 Pervomaiskaya St., 141700 Dolgoprudnyi, Russia
e-mail: ilnur.khuziev@yandex.ru

Abstract. We present the antipodality relation and search for an antipodal vertex. We also give a randomized algorithm solving the oracle problem in symmetric Cayley graphs over group $\mathbb{Z}_2^n$. The number of queries is polynomial over the graph's degree. Ill. 1, bibliogr. 5.

Keywords: graph, automorphism, antipodality, oracle.

REFERENCES

1. **V. Yu. Krasin**, On the weak isometries of the Boolean cube, *J. Appl. Ind. Math.,* **1**, No. 4, 463–467, 2007.
2. **M. A. Nielsen** and **I. L. Chuang**, *Quantum Computation and Quantum Information,* Cambridge Univ. Press, Cambridge, 2000.
3. **A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann**, and **D. A. Spielman**, Exponential algorithmic speedup by quantum walk, in *Proc. 35th ACM Symp. Theory of Computing, San Diego, CA, USA, June* 9–11, 2003, 59–68, ACM, New York, 2003.
4. **J. Kempe**, Discrete quantum walks hit exponentially faster, in S. Arora, K. Jansen, J. D. P. Rolim, and A. Sahai, eds., *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (Proc. 7th Int. Workshop on Randomization and Approximation Techniques in Comp. Sci.,*

Princeton, NJ, USA, Aug. 24–26, 2003), 354–369, Springer-Verl., Berlin, 2003 (Lect. Notes Comput. Sci., Vol. 2764).

5. **I. M. Khuziev**, Quantum walk in symmetric Cayley graph over $\mathbb{Z}_2^n$, 2013 (Cornell Univ. Libr. e-Print Archive, arXiv:1305.6849).

Ilnur M. Khuziev

Received
3 March 2014
Revised
26 August 2014