

Сведение задачи декодирования с ограниченным расстоянием к задаче Изинга с использованием редукции базиса двойственной решетки

И. В. Лысаков

Аннотация—Рассматривается сведение задачи декодирования с ограниченным расстоянием (BDD) в целочисленных решетках к задаче минимизации функционала Изинга. Предложенный метод использует редукцию базиса двойственной решетки для получения верхних оценок координат искомого вектора. Это позволяет улучшить известные оценки количества переменных в функционале Изинга до $\frac{1}{2}n^2 + O(n \cdot \log n)$ при LLL-редукции двойственного базиса и до $\frac{3}{2}n \cdot \log n + O(n)$ при редукции по Коркину—Золотареву. Указанные оценки определяют количество кубитов, достаточное для решения задачи на квантовом адиабатическом вычислителе.

Ключевые слова—целочисленная решетка, задача поиска ближайшего вектора (CVP), задача декодирования с ограниченным расстоянием (BDD), задача Изинга, квантовый адиабатический вычислитель, квантовый отжиг.

1. ВВЕДЕНИЕ

Модель квантовых гейтовых вычислений, предложенная Д. Дойчем в 80-х годах прошлого века, является развитием теории вычислений А. Тьюринга. Известно, что в квантовой модели вычислений существуют эффективные алгоритмы решения сложных математических задач, для которых эффективные классические алгоритмы неизвестны. Важнейшие для криптографии примеры — алгоритмы факторизации и дискретного логарифмирования: на сложности этих задач основана стойкость большинства современных асимметричных схем, например RSA [1] и схемы Эль-Гамала [2].

Некоторые из вычислительных устройств, функционирование которых основано на принципах квантовой механики, могут быть использованы для решения задач оптимизации на дискретных множествах. Например, адиабатический вычислитель [3] или алгоритм QAOA [4], реализованный на квантовом гейтовом компьютере, предназначены для решения так называемой задачи Изинга [5]. Последняя предполагает нахождение минимума функционала

$$I(\mathbf{s}) = \sum_{p=1}^N h_p s_p + \sum_{i=1}^N \sum_{j=i+1}^N J_{i,j} s_i s_j,$$

где $h_p \in \mathbb{R}$, $p = \overline{1, n}$, $J_{i,j} \in \mathbb{R}$, $i = \overline{1, N}$, $i < j \leq N$, над множеством переменных $s_k \in \{-1, 1\}$, $k = \overline{1, n}$. Параметр N , задающий количество переменных в функционале, играет важную роль в определении сложностных характеристик алгоритма. В случае адиабатического вычислителя он

устанавливает количество логических кубитов, необходимых для проведения вычислений. Поэтому в нашей работе исследуется сведение ряда задач, имеющих важное криптографическое применение, к задаче Изинга.

Считается [6], что семейство криптографических схем, безопасность которых основана на задачах из теории решеток, устойчиво к атакам с использованием квантового вычислителя. В качестве таких задач обычно используются задачи поиска кратчайшего вектора (SVP) и ближайшего вектора (CVP). У последней существует ослабленная версия — задача декодирования с ограниченным расстоянием (BDD). В некоторых случаях для вскрытия криптосистемы достаточно решить именно ее.

В статье [7] авторы представили два способа сведения поиска кратчайшего вектора к задаче Изинга [5], для решения которой предназначен квантовый адиабатический компьютер. Первый из них требует для этого меньшего числа кубитов по сравнению со вторым. Однако второй более устойчив к квантовому шуму.

В [8] алгоритм из [7] был обобщен на задачи поиска ближайшего вектора и декодирования с ограниченным расстоянием с помощью сведения к задаче квадратичной бинарной оптимизации без ограничений (QUBO, [9]), которая эквивалентна задаче Изинга. Кроме этого, в упомянутой статье была дана оценка количества кубитов, достаточного для решения задачи декодирования с ограниченным расстоянием на квантовом адиабатическом вычислителе в решетках, обеспечивающих безопасность криптосистемы NTRUEncrypt [10]. В [11] была дана оценка времени работы адиабатического алгоритма, достаточного для решения задачи декодирования с ограниченным расстоянием, а в [12] исследовалась возможность улучшения сложностных характеристик квантового адиабатического алгоритма при использовании методов предобработки базиса решетки и точки пространства.

В [13] был предложен метод оценки координат вектора решетки через нормы векторов двойственного базиса. Было показано, что при редукции базиса двойственной решетки по Коркину-Золотареву [14] в предположении гауссовой эвристики задача SVP может быть сведена к поиску минимума функционала Изинга, определенного над $\frac{3}{2}n \log n + O(n)$ переменными.

В настоящей работе рассматривается сведение решения задачи декодирования с ограниченным расстоянием к задаче Изинга. Использование подхода из [13] в рамках решения задачи BDD позволило получить строгие оценки без эвристических предположений. Были доказаны верхние оценки количества переменных в функционалах Изинга, требуемых для подобного сведения, при использовании разных алгоритмов предобработки базиса решетки. В случае декодирования с ограниченным расстоянием для произвольной решетки ранга n в $\mathbb{R}^n$ потребуется не более $\frac{1}{2}n^2 + O(n)$ и $\frac{3}{2}n \cdot \log n + O(n)$ переменных, если двойственный базис решетки был LLL-редуцирован [15] или редуцирован по Коркину-Золотареву [14] соответственно.

II. ОСНОВНЫЕ ПОНЯТИЯ

Пусть $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$ линейно независимы. Решеткой ранга n в $\mathbb{R}^m$ называется множество

$$\mathcal{L} = \left\{ \sum_{i=1}^n z_i \mathbf{b}_i \mid z_i \in \mathbb{Z} \right\}.$$

При этом матрица $B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$, составленная из векторов $\mathbf{b}_i$ как из столбцов, называется *базисом решетки*. Если $n = m$, то будем называть $\mathcal{L}$ — *решеткой полного ранга*.

Таким образом, решетка $\mathcal{L}$, заданная базисом B , может быть определена равенством

$$\mathcal{L} = \mathcal{L}(B) = \{ \mathbf{z} \in \mathbb{R}^m : \mathbf{z} = B \mathbf{s}, \mathbf{s} \in \mathbb{Z}^n \}.$$

Каждая решетка $\mathcal{L}$, определяет так называемую *двойственную решетку* $\mathcal{L}^*$. Двойственной решеткой к $\mathcal{L} \subset \mathbb{R}^m$ называется такое множество $\mathcal{L}^*$, что

$$\mathcal{L}^* = \{ \mathbf{z} \in \text{span}(\mathcal{L}) \mid \forall \mathbf{x} \in \mathcal{L} \langle \mathbf{z}, \mathbf{x} \rangle \in \mathbb{Z} \}$$

Для множества, определенного выше, выполнены следующие свойства [16].

1. Множество $\mathcal{L}^*$ — решетка.
2. Решетка, двойственная к $\mathcal{L}^*$, совпадает с $\mathcal{L}$.
3. Пусть решетка $\mathcal{L}$ определена базисом $B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$. Тогда существует единственный базис $B^* = (\mathbf{b}_1^*, \mathbf{b}_2^*, \dots, \mathbf{b}_n^*)$, определяющий $\mathcal{L}^*$, для которого выполнено

$$\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = \delta_{ij},$$

где δ_{ij} — символ Кронекера. Он равен

$$B^* = B (B^T B)^{-1}.$$

Одна и та же решетка может быть определена несколькими базисами. Базисы $B_1 \in \mathbb{Z}^{m \times n}$ и $B_2 \in \mathbb{Z}^{m \times n}$ задают одну и ту же решетку тогда и только тогда, когда $B_1 = B_2 U$, где $U \in \mathbb{Z}^{n \times n}$ — унимодулярная матрица, т. е. $|\det(U)| = 1$.

Основываясь на приведенном выше утверждении, можно ввести понятие определителя решетки. *Определителем решетки $\mathcal{L}(B)$* называется $\det(\mathcal{L}) = \sqrt{\det(B^T B)}$.

Определитель решетки и двойственной ей решетки связаны соотношением $\det(\mathcal{L}^*) = \frac{1}{\det(\mathcal{L})}$.

В каждой решетке существует вектор с минимальной ненулевой евклидовой нормой. Длина такого вектора для решетки $\mathcal{L}$ называется *первым минимумом решетки* и обозначается

$$\lambda_1(\mathcal{L}) = \min\{\|\mathbf{v}\| \mid \mathbf{v} \in \mathcal{L}, \mathbf{v} \neq \mathbf{0}\}.$$

Таким образом, первый минимум можно задать как минимальный радиус шара с центром в начале координат, содержащего хотя бы один ненулевой вектор решетки. Это определение можно обобщить для последовательности параметров $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n$, получивших название *последовательных минимумов решетки*.

Для решетки $\mathcal{L}$ ранга n в $\mathbb{R}^m$ и целого $k \leq n$ ее k -м *последовательным минимумом* $\lambda_k(\mathcal{L})$ называется минимальный радиус шара с центром в начале координат, содержащего k линейно независимых векторов $\mathcal{L}$.

Для первого минимума решетки $\mathcal{L}$ ранга n в $\mathbb{R}^n$ доказана так называемая *граница Минковского* [17]

$$\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}.$$

Последовательные минимумы решетки $\mathcal{L}$ и двойственной ей решетки $\mathcal{L}^*$ связаны соотношением, определенным *теоремой Банашица* [18]:

$$1 \leq \lambda_i(\mathcal{L}) \cdot \lambda_{n-i+1}(\mathcal{L}^*) \leq n.$$

Еще одна характеристика решетки $\mathcal{L}$ — *радиус покрытия* $\mu(\mathcal{L})$, значение которого равно такому минимальному числу r , что шары $\mathcal{B}(\mathbf{v}, r) = \{ \mathbf{x} \in \mathbb{R}^m \mid \|\mathbf{x} - \mathbf{v}\| \leq r \}$ радиуса r с центрами в векторах $\mathbf{v}$ решетки $\mathcal{L}$ покрывают все линейное подпространство, определенное базисными векторами $\mathcal{L}$:

$$\mu(\mathcal{L}) = \inf \left\{ r \geq 0 \mid \text{span}(\mathcal{L}) \subseteq \bigcup_{\mathbf{v} \in \mathcal{L}} \mathcal{B}(\mathbf{v}, r) \right\}.$$

Для решетки $\mathcal{L}$ ранга n в $\mathbb{R}^m$ справедлива оценка [16] $\mu(\mathcal{L}) \leq \frac{\sqrt{n}}{2} \lambda_n(\mathcal{L})$.

Синтез криптографических алгоритмов на основе теории решеток использует наличие в ней ряда вычислительно сложных задач. Одна из них — *задача поиска кратчайшего вектора* (Shortest Vector Problem, или SVP). Для ее решения необходимо найти в решетке $\mathcal{L}$ такой вектор $\mathbf{v} \in \mathcal{L}$, что $\|\mathbf{v}\| = \lambda_1(\mathcal{L})$.

Рассмотрим один из способов приближенного решения задачи SVP. Пусть решетка $\mathcal{L} \subseteq \mathbb{R}^n$ определена базисом $B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$. В результате применения процесса ортогонализации Грама–Шмидта к базису B получим набор ортогональных базисных векторов $\tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_2, \dots, \tilde{\mathbf{b}}_n$, заданных следующим образом

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\mathbf{b}}_j, \quad \mu_{i,j} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\|\tilde{\mathbf{b}}_j\|^2}.$$

Базис $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathbb{R}^m$ называется δ -LLL-редуцированным [15] для $\delta \in \left(\frac{1}{4}, 1\right)$, если выполнено

1. $\forall i, j: 1 \leq i, j \leq n, j < i, |\mu_{i,j}| \leq \frac{1}{2};$
2. $\forall i: 1 \leq i < n, \delta \|\tilde{\mathbf{b}}_i\|^2 \leq \|\mu_{i+1,i} \tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2.$

При $\delta = \frac{3}{4}$ подобный базис будем называть просто LLL-редуцированным.

В силу ортогональности векторов $\tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_2, \dots, \tilde{\mathbf{b}}_n$ условие 2 в определении можно преобразовать следующим образом:

$$\delta \|\tilde{\mathbf{b}}_i\|^2 \leq \mu_{i+1,i}^2 \|\tilde{\mathbf{b}}_i\|^2 + \|\tilde{\mathbf{b}}_{i+1}\|^2.$$

Что, с учетом $|\mu_{i,j}| \leq \frac{1}{2}$, при $j < i$ позволяет получить

$$\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq (\delta - \mu_{i+1,i}^2) \|\tilde{\mathbf{b}}_i\|^2 \geq \left(\delta - \frac{1}{4}\right) \|\tilde{\mathbf{b}}_i\|^2.$$

Если $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathbb{R}^n$ — δ -LLL-редуцированный базис решетки L , тогда выполнены следующие утверждения [15].

1. $\|\tilde{\mathbf{b}}_1\| \leq \left(\delta - \frac{1}{4}\right)^{-\frac{i-1}{2}} \|\tilde{\mathbf{b}}_i\|;$
2. $\|\mathbf{b}_i\| \leq \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1} \lambda_i(L).$

Для любой решетки можно построить LLL-редуцированный базис за полиномиальное число шагов от размерности решетки. Подобный алгоритм представлен в [15]. Будем обозначать его применение к базису решетки B через $\text{LLL}_\delta(B)$.

Рассмотрим другие способы редукции базиса решетки. Для $1 \leq i \leq n$ обозначим через π_i ортогональную проекцию на ортогональное дополнение к $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})$:

$$\pi_i(\mathbf{x}) = \sum_{j=i}^n \frac{\langle \mathbf{x}, \tilde{\mathbf{b}}_j \rangle}{\|\tilde{\mathbf{b}}_j\|^2} \tilde{\mathbf{b}}_j.$$

Для $1 \leq i \leq j \leq n$ положим

$$B_{[i,j]} = (\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_j))$$

$$\mathcal{L}_{[i,j]} = \mathcal{L}(B_{[i,j]})$$

Базис B редуцирован по Коркину–Золотареву (КЗ-базис) [14], если

1. $|\mu_{i,j}| \leq 1/2$ при $1 \leq j < i \leq n$;
2. для каждого $i = 1, \dots, n$ вектор $\pi_i(\mathbf{b}_i) = \tilde{\mathbf{b}}_i$ — кратчайший ненулевой вектор решетки $\mathcal{L}_{[i,n]}$.

Для базиса Коркина–Золотарева выполнено следующее свойство [14]. Пусть $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n \in \mathbb{R}^n$ базис решетки L , редуцированный по Коркину–Золотареву. Тогда выполнено

$$\frac{4}{i+3} \leq \left(\frac{\|\mathbf{b}_i\|}{\lambda_i(L)}\right)^2 \leq \frac{i+3}{4}.$$

Для любой решетки можно построить базис, редуцированный по Коркину–Золотареву [14]. Однако для этого требуется нахождение кратчайшего вектора в решетке ранга n , что делает это вычислительно сложной задачей.

Рассмотрим другую важную задачу из теории решеток — задачу поиска ближайшего вектора (Closest Vector Problem, или CVP). Для ее решения необходимо по заданной

точке $\mathbf{t} \notin L$ найти такой вектор $\mathbf{v} \in L$, что $\mathbf{v} = \underset{\mathbf{u} \in L}{\operatorname{argmin}}(\|\mathbf{u} - \mathbf{t}\|)$.

У задачи CVP существует ослабленная версия — задача декодирования с ограниченным расстоянием (Bounded Distance Decoding, или BDD $_\gamma$). Тут требуется по $\mathbf{t} \notin L$ найти ближайший вектор $\mathbf{v} \in L$, если известно, что $\|\mathbf{v} - \mathbf{t}\| \leq \gamma \cdot \lambda_1(L)$, $0 < \gamma < 1/2$. Условие $0 < \gamma < 1/2$ гарантирует единственность решения задачи BDD $_\gamma$.

Метод нахождения приближенного решения $\mathbf{u}$ этих задач был предложен Ласло Бабаи в работе [19]. Для его нахождения достаточно покомпонентно округлить к ближайшему целому вектор координат точки $\mathbf{t}$ в базисе B , задающем решетку

$$\mathbf{u} = B[B^{-1} \mathbf{t}].$$

В дальнейшем будем называть этот алгоритм алгоритмом округления Бабаи. Полученный после его завершения вектор решетки обладает следующим свойством [19]

$$\mathbf{u} - \mathbf{t} \in \left\{ \sum_{i=1}^n a_i \mathbf{b}_i \mid |a_i| \leq \frac{1}{2} \right\}.$$

Если решетка L задана LLL-редуцированным базисом, то установлено [19], что вектор $\mathbf{u}$ удовлетворяет условию

$$\|\mathbf{u} - \mathbf{t}\| \leq \left(1 + 2n \left(\frac{9}{2}\right)^{n/2}\right) \operatorname{dist}(\mathbf{t}, L).$$

Применение алгоритма округления Бабаи к базису решетки B и точке $\mathbf{t}$ обозначим $\text{BabaiRounding}(B, \mathbf{t})$.

III. СВЕДЕНИЕ ЗАДАЧ SVP И CVP К ЗАДАЧАМ ИЗИНГА И QUBO

Рассмотрим следующий функционал $I(\mathbf{s})$:

$$I(\mathbf{s}) = \sum_{p=1}^N h_p s_p + \sum_{i=1}^N \sum_{j=i+1}^N J_{i,j} s_i s_j,$$

$$h_p \in \mathbb{R}, p = \overline{1, N}, J_{i,j} \in \mathbb{R}, i = \overline{1, N}, i < j \leq N$$

$$s_k \in \{-1, 1\}, k = \overline{1, N},$$

Будем называть его функционалом Изинга. Задача нахождения вектора, на котором достигается минимум $I(\mathbf{s})$, получила название задачи Изинга [5].

Параметр N из определения имеет важное значение для определения сложностных характеристик алгоритма, запускаемого на квантовом адиабатическом вычислителе [3]. Он совпадает с количеством логических кубитов, достаточных для завершения работы алгоритма. Подробнее см. [3].

Замена переменных $s_i = 2x_i - 1, i = \overline{1, N}$, в функционале $I(\mathbf{s})$ позволяет определить последний над множеством $\{0, 1\}^N$. Задача минимизации так преобразованного функционала называется задачей QUBO (quadratic unconstrained binary optimization problem) [9].

Рассмотрим решетку $\mathcal{L}(B)$, $B \in \mathbb{Z}^{n \times n}$. Известно, что решение SVP может быть сведено к нахождению минимума положительно определенной квадратичной формы

$$\|\mathbf{v}\|^2 = \|B \mathbf{x}\|^2 = \sum_{i,j=1}^n g_{ij} x_i x_j,$$

где $g_{ij} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle$ — элемент матрицы Грама $B^T B = \{g_{ij}\}$. Поэтому для определения кратчайшего вектора решетки достаточно минимизировать следующий функционал на множестве всех ненулевых целочисленных векторов:

$$f(\mathbf{x}) = \sum_{i,j=1}^n g_{ij} x_i x_j = \mathbf{x}^T G \mathbf{x} = \mathbf{x}^T B^T B \mathbf{x}.$$

На основе вышеприведенного факта, в [7] был предложен способ сведения задачи SVP к поиску второго минимума функционала Изинга. В предположении ограниченности абсолютного значения переменных в квадратичной форме $f(\mathbf{x})$: $|x_j| \leq 2^k$, $j = \overline{1, n}$, замены

$$x_j = \sum_{p=0}^k 2^p y_{pj} - 2^k, y_{pj} \in \{0, 1\},$$

$$x_j = - \sum_{\ell=0}^k 2^{\ell-1} s_{\ell j} - \frac{1}{2}, s_{\ell j} \in \{-1, 1\},$$

позволяют преобразовать $f(\mathbf{x})$ в функционалы QUBO и Изинга соответственно.

Аналогично, для решения задач CVP и BDD относительно фиксированной точки $\mathbf{t} \in \mathbb{Z}^m$ достаточно найти минимум функционала, представленного ниже

$$g(\mathbf{x}) = \|B \mathbf{x} - \mathbf{t}\|^2 = \|B \mathbf{x}\|^2 - 2(B \mathbf{x}, \mathbf{t}) + \|\mathbf{t}\|^2 = \mathbf{x}^T B^T B \mathbf{x} - 2 \mathbf{x}^T B^T \mathbf{t} + \mathbf{t}^T \mathbf{t}.$$

В [12] исследовалась возможность решения задач BDD и CVP через их сведение к задаче Изинга с помощью замены переменных вида $x_j = - \sum_{\ell=0}^k 2^{\ell-1} s_{\ell j} - \frac{1}{2}$, $s_{\ell j} \in \{-1, 1\}$, в функционале $g(\mathbf{x})$ в предположении $|x_j| < 2^k$, $j = \overline{1, n}$. Отметим, что в отличие от случая поиска кратчайшего вектора здесь для решения исходной задачи требовалось найти непосредственно минимум функционала Изинга. Также в работе получена верхняя оценка количества переменных в упомянутом выше функционале, достаточных для решения BDD_γ.

Пусть D — базис решетки $\mathcal{L}$; обозначим через $[D]$ множество всех ее базисов

$$[D] = \{D' \mid D' = D \cdot U, U \in \mathbb{Z}^{n \times n}, \det U = \pm 1\}.$$

Также пусть $F: [D] \rightarrow [D]$ и $G: \mathbb{Z}^n \setminus \mathcal{L} \rightarrow \mathcal{L}$ — функции преобразования базиса решетки L и приближения точки пространства ее вектором соответственно. Тогда определим матрицу B и вектор $\mathbf{u}$ равенствами

$$B = F(D), \mathbf{u} = G(\mathbf{t}_0).$$

Пусть $\mathbf{z}_0$ — ближайший вектор к $\mathbf{t}_0$, а $\mathbf{z}$ — ближайший к точке $\mathbf{t} = \mathbf{t}_0 - \mathbf{u}$. Заметим, что так как $\mathbf{u} \in L$, то $\mathbf{z}_0 = \mathbf{z} + \mathbf{u}$. Таким образом, нахождение $\mathbf{z} \in \mathbb{Z}^n$ позволит решить исходную задачу.

Для координат $\mathbf{z} \in \mathbb{Z}^n$ в базисе B справедливо представление

$$B^{-1} \mathbf{z} = \arg \min_{\mathbf{x} \in \mathbb{Z}^n} (\|B \mathbf{x} - \mathbf{t}\|^2)$$

$$= \arg \min_{\mathbf{x} \in \mathbb{Z}^n} (\mathbf{x}^T B^T B \mathbf{x} - 2 \mathbf{x}^T B^T \mathbf{t} + \mathbf{t}^T \mathbf{t}) = \arg \min_{\mathbf{x} \in \mathbb{Z}^n} (g(\mathbf{x})).$$

Сведем нахождение минимума функционала $g(\mathbf{x})$ к задаче Изинга в предположении $|x_i| \leq 2^k$, $i = 1, \dots, n$. Для этого выполним замену переменных вида

$$x_j = - \sum_{\ell=0}^k 2^{\ell-1} s_{\ell j} - \frac{1}{2}, s_{\ell j} \in \{-1, 1\}, j = 1, \dots, n.$$

Ее можно переписать в терминах операций с матрицами (см. [12]): $\mathbf{x} = P \mathbf{s} - \mathbf{d}$, где $P \in \mathbb{R}^{n \times (n \cdot (k+1))}$, $\mathbf{s} \in \{-1, 1\}^{(n \cdot (k+1))}$ и $\mathbf{d} \in \mathbb{R}^{(n \cdot (k+1))}$.

Замена переменных позволяет придать функционалу $g(\mathbf{x})$ вид

$$g(\mathbf{s}) = \mathbf{s}^T J \mathbf{s} + H \mathbf{s} + c,$$

$$J = P^T B^T B P, H = -2 \mathbf{d}^T B^T B P - 2 \mathbf{t}^T B P,$$

$$c = \mathbf{d}^T B^T B \mathbf{d} + 2 \mathbf{d}^T B^T \mathbf{t} + \mathbf{t}^T \mathbf{t}, \mathbf{s} \in \{-1, 1\}^{n \cdot (k+1)}.$$

Пусть $J = \{J_{i,j}\}_{i,j=1, n \cdot (k+1)}$, $H = \{h_i\}_{i=1, n \cdot (k+1)}$. Так как $s_i^2 = 1$, функционал

$$I(\mathbf{s}) = \sum_{i=1}^{n \cdot (k+1)} \sum_{j=i+1}^{n \cdot (k+1)} 2 J_{i,j} s_i s_j + \sum_{p=1}^{n \cdot (k+1)} h_p s_p =$$

$$\mathbf{s}^T J \mathbf{s} + H \mathbf{s} - \sum_{i=1}^{n \cdot (k+1)} J_{i,i} = g(\mathbf{s}) - c - \sum_{i=1}^{n \cdot (k+1)} J_{i,i} = g(\mathbf{s}) - c - c',$$

где $c' = \sum_{i=1}^{n \cdot (k+1)} J_{i,i}$, является функционалом Изинга, определенным над $n \cdot (k+1)$ переменными.

Нахождение вектора $\mathbf{s}$ дает возможность восстановить вектор $\mathbf{z}$, а значит, и вектор $\mathbf{z}_0 = \mathbf{z} + \mathbf{u}$, причем $\|\mathbf{z}_0 - \mathbf{t}_0\| = \text{dist}(\mathbf{t}_0, \mathcal{L})$, что и требуется для решения задачи поиска ближайшего вектора.

В работе [12] рассматривался случай $F = \text{LLL}_{\frac{3}{4}}$. Для задачи BDD было доказано, что решение относительно точки $\mathbf{t}_0$, не принадлежащей $\mathcal{L}$, может быть сведено к задаче минимизации функционала Изинга, определенного над $(\frac{1}{2} + \log 3) n^2 - (1 + \log 3) n$ переменными.

IV. РЕШЕНИЕ ЗАДАЧИ BDD

В данной работе исследуется возможность сведения задачи BDD к задаче Изинга для решеток произвольного вида. В частности, доказаны верхние оценки количества переменных в функционале Изинга, необходимых для решения BDD в решетках, чьи двойственные базисы редуцированы по LLL и Коркину–Золотареву. Полученные оценки улучшают результат из [12].

Пусть заданы $\mathcal{L}$ — произвольная решетка ранга n в $\mathbb{Z}^n$, определенная базисом D , и $\mathbf{t}_0 \notin \mathcal{L}$ — точка пространства, не принадлежащая решетке.

Применим к $\mathcal{L}$ и $\mathbf{t}_0$ алгоритм из предыдущего раздела. Вычислим $D^* = (D^{-1})^T$, применим к нему алгоритм редукции и получим базис B^* решетки $\mathcal{L}^*$. От алгоритма редукции потребуем выполнения свойства

$$\|\mathbf{b}_i^*\| \leq \omega \lambda_i(\mathcal{L}^*), i = 1, \dots, n,$$

где $\omega = \omega(n)$ — некоторая величина, которая зависит от размерности решетки. Положим $B = F(D) = ((B^*)^{-1})^T$; по свойству 3 это базис решетки $\mathcal{L}$, двойственный к B^* .

Заметим, что подобное приведение действительно возвращает целочисленный базис исходной решетки. Алгоритм вычисляет базис B^* той же самой двойственной решетки $\mathcal{L}^*$, поэтому существует такая унимодулярная матрица $U \in \mathbb{Z}^{n \times n}$, что

$$B^* = D^* \cdot U.$$

В этом случае базис исходной решетки определяется как

$$B = ((D^* \cdot U)^{-1})^T = ((D^*)^{-1})^T \cdot (U^{-1})^T = D \cdot (U^{-1})^T.$$

Поскольку матрица, обратная к унимодулярной, также является унимодулярной, то базис B задает исходную решетку $\mathcal{L}$.

В качестве функции G возьмем алгоритм округления Бабаи.

$$G = \text{BabaiRounding}(B, \cdot)$$

Это позволяет вычислить точку $\mathbf{t}$:

$$\mathbf{t} = \mathbf{t}_0 - G(\mathbf{t}_0).$$

Покажем, что подобный подход улучшает оценку для BDD из [12]. Следующая теорема устанавливает ее вид для рассматриваемой задачи.

Теорема 1. Пусть решетка $\mathcal{L}$ ранга n в $\mathbb{Z}^n$ задана базисом $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$. Пусть также $B^* = (B^{-1})^T$ — базис двойственной к $\mathcal{L}$ решетки, для которого выполнено $\|\mathbf{b}_i^*\| \leq \omega \cdot \lambda_i(\mathcal{L}^*)$, $i = 1, \dots, n$. Тогда решение задачи BDD $_{\gamma}$ относительно точки $\mathbf{t}_0$, не принадлежащей $\mathcal{L}$, может быть сведено к задаче минимизации функционала Изинга, определенного над $(\log \omega + \log n) \cdot n + (3 + \log \gamma) \cdot n$ переменными.

Доказательство. Будем искать ближайший вектор к точке $\mathbf{t} = [t_1 t_2 \dots t_n]^T$, полученной в результате сдвига исходной точки $\mathbf{t}_0$ на вектор решетки $\mathbf{u}$, где $\mathbf{u}$ — результат работы алгоритма округления Бабаи. Пусть $\mathbf{x} = [x_1 x_2 \dots x_n]^T$ определяется равенством

$$\mathbf{x} = \operatorname{argmin}_{\mathbf{z} \in \mathbb{Z}^n} \|\mathbf{B} \mathbf{z} - \mathbf{t}\|.$$

Поскольку $B^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ — базис решетки, двойственной к $\mathcal{L}$, то заметим, что

$$\langle \mathbf{b}_i^*, \mathbf{B} \mathbf{x} \rangle = \left\langle \mathbf{b}_i^*, \sum_{j=1}^n x_j \mathbf{b}_j \right\rangle = \sum_{j=1}^n x_j \langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = x_i.$$

Оценим значение $|x_i - \langle \mathbf{b}_i^*, \mathbf{t} \rangle|$:

$$|x_i - \langle \mathbf{b}_i^*, \mathbf{t} \rangle| = |\langle \mathbf{b}_i^*, \mathbf{B} \mathbf{x} - \mathbf{t} \rangle| \leq \|\mathbf{B} \mathbf{x} - \mathbf{t}\| \cdot \|\mathbf{b}_i^*\| \leq \gamma \cdot \lambda_i(\mathcal{L}) \cdot \|\mathbf{b}_i^*\|.$$

Согласно условию теоремы $\|\mathbf{b}_i^*\| \leq \omega \cdot \lambda_i(\mathcal{L}^*)$, $i = 1, \dots, n$. С учетом теоремы Банашика имеем

$$\|\mathbf{b}_i^*\| \leq \omega \cdot \frac{n}{\lambda_{n-i+1}(\mathcal{L})} \leq \omega \cdot \frac{n}{\lambda_1(\mathcal{L})}.$$

Последнее позволяет переписать неравенство для $|x_i - \langle \mathbf{b}_i^*, \mathbf{t} \rangle|$ в виде

$$|x_i - \langle \mathbf{b}_i^*, \mathbf{t} \rangle| \leq \gamma \cdot \omega \cdot n.$$

В силу того, что $|x_i| - |\langle \mathbf{b}_i^*, \mathbf{t} \rangle| \leq |x_i - \langle \mathbf{b}_i^*, \mathbf{t} \rangle|$, получаем

$$|x_i| \leq \gamma \cdot \omega \cdot n + |\langle \mathbf{b}_i^*, \mathbf{t} \rangle|.$$

Осталось заметить, что согласно свойствам базиса двойственной решетки и алгоритма округления Бабаи

$$|\langle \mathbf{b}_i^*, \mathbf{t} \rangle| = \left| \left\langle \mathbf{b}_i^*, \sum_{j=1}^n \tau_j \mathbf{b}_j \right\rangle \right| = |t_i| \leq \frac{1}{2}.$$

Окончательно получаем

$$|x_i| \leq \gamma \cdot \omega \cdot n + \frac{1}{2}, i = 1, \dots, n,$$

откуда достаточно выбрать

$$k = \log \left(\gamma \cdot \omega \cdot n + \frac{1}{2} \right) + 1$$

Так как полученная оценка справедлива для любой координаты вектора $\mathbf{x}$, то для решения задачи BDD $_{\gamma}$ достаточно определить функционал Изинга над

$$n \cdot \left(\log \left(\gamma \cdot \omega \cdot n + \frac{1}{2} \right) + 2 \right) \leq (\log \omega + \log n) \cdot n + (3 + \log \gamma) \cdot n$$

переменными, **ч. т. д.**

Следствие 1. Пусть решетка $\mathcal{L}^*$, двойственная к решетке $\mathcal{L}$ ранга n в $\mathbb{Z}^n$, задана $\frac{3}{4}$ -LLL-редуцированным базисом B^* . Тогда решение задачи BDD $_{\gamma}$ в $\mathcal{L}$ относительно точки $\mathbf{t}_0$, не принадлежащей $\mathcal{L}$, может быть сведено к задаче минимизации функционала Изинга, определенного над $\frac{1}{2} n^2 + n \log n + \left(\frac{5}{2} + \log \gamma \right) \cdot n$ переменными.

Доказательство. Справедливость следствия следует из свойств $\frac{3}{4}$ -LLL-базиса, поскольку для двойственной решетки справедливо $\|\mathbf{b}_i^*\| \leq 2^{\frac{n-1}{2}} \cdot \lambda_i(\mathcal{L}^*)$, откуда $\omega = 2^{\frac{n-1}{2}}$, **ч. т. д.**

Следствие 2. Пусть решетка $\mathcal{L}^*$, двойственная к решетке $\mathcal{L}$ ранга n в $\mathbb{Z}^n$, задана редуцированным по Коркину–Золотареву базисом B^* . Тогда решение задачи BDD $_{\gamma}$ в $\mathcal{L}$ относительно точки $\mathbf{t}_0$, не принадлежащей $\mathcal{L}$, может быть сведено к задаче минимизации функционала Изинга, определенного над $\frac{3}{2} n \cdot \log n + (3 + \log \gamma) \cdot n$ переменными.

Доказательство. Справедливость следствия следует из свойств базиса, редуцированного по Коркину–Золотареву, поскольку для двойственной решетки справедливо $\|\mathbf{b}_i^*\| \leq \sqrt{\frac{n+3}{4}} \cdot \lambda_i(\mathcal{L}^*)$, откуда $\omega = \sqrt{\frac{n+3}{4}}$. Таким образом для определения функционала Изинга достаточно

$$\left(\frac{1}{2} \log \frac{n+3}{4} + \log n \right) \cdot n + (3 + \log \gamma) \cdot n$$

$$\leq \frac{3}{2} n \cdot \log n + (3 + \log \gamma) \cdot n$$

переменных, **ч. т. д.**

Результат, аналогичный результату теоремы 1, можно доказать для задачи поиска ближайшего вектора.

Теорема 2. Пусть решетка $\mathcal{L}$ ранга n в $\mathbb{Z}^n$ задана базисом $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$. Пусть также $B^* = (B^{-1})^T$ — базис двойственной к $\mathcal{L}$ решетки, для которого выполнено $\|\mathbf{b}_i^*\| \leq$

$\omega \cdot \lambda_i(\mathcal{L}^*)$, $i = 1, \dots, n$. Тогда поиск ближайшего вектора решетки к точке $\mathbf{t}_0$, не принадлежащей $\mathcal{L}$, может быть сведен к задаче минимизации функционала Изинга, определенного над $\left(\log \frac{\lambda_n(\mathcal{L})}{\lambda_1(\mathcal{L})} + \log \omega + \frac{3}{2} \log n\right) \cdot n + 2n$ переменными.

Доказательство. Теорема доказывается аналогично теореме 1, за исключением оценки

$$|x_i - \langle \mathbf{b}_i^*, \mathbf{t} \rangle| = |\langle \mathbf{b}_i^*, B\mathbf{x} - \mathbf{t} \rangle| \leq \|B\mathbf{x} - \mathbf{t}\| \cdot \|\mathbf{b}_i^*\| \leq \mu(\mathcal{L}) \cdot \|\mathbf{b}_i^*\|$$

С учетом $\mu(\mathcal{L}) \leq \frac{\sqrt{n}}{2} \lambda_n(\mathcal{L})$, получаем требуемое, **ч. т. д.**

Преобразование базиса двойственной решетки уменьшает константу при главном члене числа переменных по сравнению с редукцией исходного базиса решетки. Следствие 1 устанавливает оценку количества кубитов порядка $\frac{1}{2}n^2 + O(n)$, в то время как теорема из [12] — $\left(\frac{1}{2} + \log 3\right)n^2 + O(n)$. Более того, редукция базиса двойственной решетки по Коркину–Золотареву позволяет решить задачу декодирования с ограниченным расстоянием с использованием $\frac{3}{2}n \cdot \log n + O(n)$ кубитов. Однако последнее предполагает нахождение кратчайшего вектора в решетке размерности n , что предполагает решение NP-трудной задачи.

V. ОТКРЫТЫЕ ВОПРОСЫ

Результаты работы могут быть полезны в случае реализации атаки на рассматриваемые задачи с помощью квантового вычислителя. Однако в этом случае встает вопрос о влиянии квантового шума на работу алгоритма. При практической реализации он окажет влияние как на количество требуемых кубитов, так и на время работы.

Также остается открытым вопрос о возможности решения поставленной задачи с помощью функционала Изинга, определенного над $O(n \log n)$ переменными, без редукции по Коркину–Золотареву.

БИБЛИОГРАФИЯ

- [1] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [2] T. El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", in *Advances in Cryptology — CRYPTO'84*, vol. 196, *Lect. Notes Comput. Sci.* Springer, 1984, pp. 10–18.
- [3] T. Albash and D. A. Lidar, "Adiabatic quantum computation", *Rev. Mod. Phys.*, vol. 90, p. 015002, Jan. 2018.
- [4] E. Farhi, J. Goldstone, and S. Gutmann, "A Quantum Approximate Optimization Algorithm", *arXiv:1411.4028*, 2014.
- [5] T. Kadowaki and H. Nishimori, "Quantum annealing in the transverse Ising model", *Phys. Rev. E*, vol. 58, no. 5, pp. 5355–5363, 1998.
- [6] J.-F. Biasse, X. Bonnetain, E. Kirshanova, et al., "Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography", *IET Inf. Secur.*, vol. 16, no. 4, pp. 577–602, 2022.
- [7] D. Joseph, A. Callison, C. Ling, and F. Mintert, "Two quantum Ising algorithms for the Shortest Vector Problem: one for now and one for later", *arXiv:2006.14057*, 2021.

- [8] I. V. Lysakov, "Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method", *Mat. Vopr. Kriptogr.*, vol. 14, no. 2, pp. 111–122, 2023.
- [9] G. Kochenberger, J.-K. Hao, F. Glover, et al., "The unconstrained binary quadratic programming problem: A survey", *J. Comb. Optim.*, vol. 28, pp. 58–81, 2014.
- [10] NTRU NIST PQC submission, 2020. [Online]. Available: <https://ntru.org/release/NIST-PQSubmission-NTRU-20201016.tar.gz>
- [11] И. В. Лысаков, «Об оценке временной сложности адиабатических вычислений для одного класса целочисленных решёток», *Матем. вopr. криптогр.*, Т. 16, вып. 1, 121–143, 2025.
- [12] И. В. Лысаков, «Сведение задачи поиска ближайшего вектора для целочисленных решёток к задаче Изинга», *Дискрет. матем.*, Т. 37, вып. 3, 94–114, 2025.
- [13] M. R. Albrecht, M. Prokop, Y. Shen, and P. Wallden, "Variational quantum solutions to the Shortest Vector Problem", *Cryptology ePrint Archive, Paper 2022/233*, 2022.
- [14] J. C. Lagarias, H. W. Lenstra, and C. P. Schnorr, "Korkin–Zolotarev bases and successive minima of a lattice and its reciprocal lattice", *Combinatorica*, vol. 10, no. 3, pp. 281–312, 1990.
- [15] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients", *Math. Ann.*, vol. 261, pp. 515–534, 1982.
- [16] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Springer, 2002.
- [17] H. Minkowski, *Geometrie der Zahlen*, Leipzig: Teubner, 1910.
- [18] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers", *Math. Ann.*, vol. 296, no. 4, pp. 625–636, 1993.
- [19] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem", in *STACS 85*, K. Mehlhorn, Ed. Berlin: Springer, 1985, pp. 13–20.

On the reduction of the Bounded Distance Decoding problem to the Ising problem via dual lattice basis reduction

I.V. Lysakov

Abstract—We propose a method for reducing the Bounded Distance Decoding problem (BDD) to the Ising problem based on dual lattice basis reduction. We prove that $\frac{1}{2}n^2 + O(n \cdot \log n)$ Ising variables suffice when the dual basis is LLL-reduced, and $\frac{3}{2}n \cdot \log n + O(n)$ suffice for a Korkin—Zolotarev-reduced dual basis, improving previously known bounds. These results determine the qubit requirements for solving BDD on a quantum adiabatic computer.

Keywords—integer lattice, closest vector problem (CVP), bounded distance decoding (BDD), Ising problem, quantum adiabatic computer, quantum annealing.

REFERENCES

- [1] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [2] T. El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", in *Advances in Cryptology — CRYPTO'84*, vol. 196, Lect. Notes Comput. Sci. Springer, 1984, pp. 10–18.
- [3] T. Albash and D. A. Lidar, "Adiabatic quantum computation", *Rev. Mod. Phys.*, vol. 90, p. 015002, Jan. 2018.
- [4] E. Farhi, J. Goldstone, and S. Gutmann, "A Quantum Approximate Optimization Algorithm", *arXiv:1411.4028*, 2014.
- [5] T. Kadowaki and H. Nishimori, "Quantum annealing in the transverse Ising model", *Phys. Rev. E*, vol. 58, no. 5, pp. 5355–5363, 1998.
- [6] J.-F. Biance, X. Bonnetain, E. Kirshanova, et al., "Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography", *IET Inf. Secur.*, vol. 16, no. 4, pp. 577–602, 2022.
- [7] D. Joseph, A. Callison, C. Ling, and F. Mintert, "Two quantum Ising algorithms for the Shortest Vector Problem: one for now and one for later", *arXiv:2006.14057*, 2021.
- [8] I. V. Lysakov, "Solving some cryptanalytic problems for lattice-based cryptosystems with quantum annealing method", *Mat. Vopr. Kriptogr.*, vol. 14, no. 2, pp. 111–122, 2023.
- [9] G. Kochenberger, J.-K. Hao, F. Glover, et al., "The unconstrained binary quadratic programming problem: A survey", *J. Comb. Optim.*, vol. 28, pp. 58–81, 2014.
- [10] NTRU NIST PQC submission, 2020. [Online]. Available: <https://ntru.org/release/NIST-PQSubmission-NTRU-20201016.tar.gz>
- [11] I. V. Lysakov, "On the estimate of time complexity of adiabatic calculations on a class of integer lattices", *Mat. Vopr. Kriptogr.*, vol. 16, no. 1, pp. 121–143, 2025.
- [12] I. V. Lysakov, "On the reduction of the closest vector problem for integer lattices to the Ising problem", *Diskretn. Mat.*, vol. 37, no. 3, pp. 94–114, 2025.
- [13] M. R. Albrecht, M. Prokop, Y. Shen, and P. Wallden, "Variational quantum solutions to the Shortest Vector Problem", *Cryptography ePrint Archive*, Paper 2022/233, 2022.
- [14] J. C. Lagarias, H. W. Lenstra, and C. P. Schnorr, "Korkin—Zolotarev bases and successive minima of a lattice and its reciprocal lattice", *Combinatorica*, vol. 10, no. 3, pp. 281–312, 1990.
- [15] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients", *Math. Ann.*, vol. 261, pp. 515–534, 1982.
- [16] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Springer, 2002.
- [17] H. Minkowski, *Geometrie der Zahlen*, Leipzig: Teubner, 1910.
- [18] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers", *Math. Ann.*, vol. 296, no. 4, pp. 625–636, 1993.
- [19] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem", in *STACS 85*, K. Mehlhorn, Ed. Berlin: Springer, 1985, pp. 13–20.