Труды МАИ. 2024. № 138
Trudy MAI, 2024, no. 138

Научная статья
УДК 511.48+ 681.391
URL: https://trudymai.ru/published.php?ID=182673

ОБЕСПЕЧЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ КАНАЛА СВЯЗИ ЗА СЧЕТ ПРИМЕНЕНИЯ МЕТОДА ПОИСКА СЛОВ МАЛОГО ВЕСА В ЛИНЕЙНОМ БЛОЧНОМ ДВОИЧНОМ И ТЕРНАРНОМ КОДАХ

Василий Станиславович Усатюк[1], **Сергей Иванович Егоров**[2],
Эдуард Игоревич Ватутин[3], **Ирина Евгеньевна Чернецкая**[4]✉
[1,2,3,4]Юго-Западный государственный университет (ЮЗГУ),
Курск, Россия
[1] l@lcrypto.com
[2] sie58@mail.ru
[3] evatutin@rambler.ru
[4] white731@yandex.ru✉

Аннотация. Функциональность и надежность беспилотных летательных аппаратов во многом определяется используемым каналом передачи данных. Данные, в том числе видео, должны надежно передаваться в реальном времени с большой скоростью на возможно большее расстояние. Для этого необходимо применение продвинутых систем коррекции ошибок и шифрования. В контексте разработки таких систем возникает необходимость построения помехоустойчивых кодов с заданными свойствами, важнейшим из которых является минимальное кодовое расстояние.

Для оценки минимального расстояния кода в статье предложен новый метод поиска слов малого веса в линейном блочном двоичном, тернарном кодах на основе геометрии чисел с использованием семейства эвристик. Метод предусматривает выполнение следующих этапов: 1) вложение (Каннана) кода в решетку; 2) приведение базиса решетки; 3) ортогонализация базиса решетки методами QR-разложения; 4) поиск кратчайшего вектора в решетке по методу Каннана-Финке-Поста (КФП). Количество отличных от нуля компонент найденного вектора равняется искомому весу кодового слова, дающему оценку кодового расстояния.

Быстродействие предложенного метода поиска слов малого веса определяется быстродействием метода поиска кратчайшего вектора КФП. Быстродействие последнего значительно увеличивается с применением эвристик. В качестве эвристик использовались следующие: Гауссово отсечение веток; экстремальное отсечение веток, основанное на замене гиперсферы Гауссовой эвристики телом пересечения цилиндров; эвристики округления, основанные на сведении задачи поиска кратчайшего вектора к задаче поиска ближайшего вектора с использованием алгоритма Бабаи и эвристики плотности.

Предложенный метод имеет высокое быстродействие при решении задач приближенной оценки кодового расстояния. Этот метод на задаче поиска слова малого веса 228 продемонстрировал 3172.9 кратное ускорение по сравнению с алгоритмом Брауэра-Циммермана, реализованном в пакете MAGMA V2.22-3. Кодовое слово малого веса 212 было найдено на основе предложенного метода за 4 147 201 секунд с использованием процессора Intel 7700K 64 ГБ и видеокарты 1070

8 ГБ. Нахождение этого кодового слова позволило занять первое место в международном конкурсе поиска слов малого веса, проводимом Французским национальным центром научных исследований (CNRS), Национальным институтом исследований в области цифровых наук и технологий (Inria, Paris) и Национальным исследовательским институтом математики и информатики в Нидерландах (CWI).

Ключевые слова: Геометрия чисел, помехоустойчивый код, оценка кодового расстояния, поиск кратчайшего вектора, поиск кратчайшего базиса, наиполнейшие решетки, вложение Каннана

Для цитирования: Усатюк В.С., Егоров С.И., Ватутин Э.И., Чернецкая И.Е. Обеспечение помехоустойчивости канала связи за счет применения метода поиска слов малого веса в линейном блочном двоичном и тернарном кодах // Труды МАИ. 2024. № 138. URL: https://trudymai.ru/published.php?ID=182673

Original article

ENSURING NOISE IMMUNITY OF A COMMUNICATION CHANNEL BY USING A METHOD OF SEARCHING FOR SMALL-WEIGHT WORDS IN LINEAR BLOCK BINARY AND TERNARY CODES

Vasily S. Usatjuk[1], Sergey I. Egorov[2], Eduard I. Vatutin[3], Irina E. Chernetskaya[4]✉

[1,2,3,4] Southwest State University,

Kursk, Russia

[1] l@lcrypto.com

[2] sie58@mail.ru

[3] evatutin@rambler.ru

[4] white731@yandex.ru✉

Abstract. The functionality and reliability of unmanned aerial vehicles is largely determined by the data transmission channel used. Data, including video, must be transmitted reliably in real time at high speed over the greatest possible distance. This requires the use of advanced error correction and encryption systems. In the context of the development of such systems, there is a need to construct error-resistant codes with specified properties, the most important of which is the minimum code distance.

For estimating the minimum code distance, the article proposes a new method for searching for words of small weight in linear block binary and ternary codes based on the geometry of numbers using a family of heuristics. The method involves the following steps: 1) embedding (Kannan) code into a lattice; 2) reduction of the lattice basis; 3) orthogonalization of the lattice basis using QR decomposition methods; 4) search for the shortest vector in the lattice using the Kannan-Finke-Post (KFP) method. The number of non-zero components of the found vector is equal to the desired codeword weight, which gives an estimate of the code distance.

The performance of the proposed method for searching for words of small weight is determined by the performance of the KFP method for searching for the shortest vector. The performance of the latter increases significantly with the use of heuristics. The following heuristics were used: Gaussian branch pruning; extreme branch cutting based on replacing the hypersphere of the Gaussian heuristic with the body of the intersection of cylinders; rounding heuristics based on reducing the problem of finding the shortest vector

to the problem of finding the nearest vector using the Babai algorithm and lattice density heuristics.

The proposed method has high performance when solving problems of approximate estimation of the code distance. This method on the task of searching for a word of small weight 228 demonstrated 3172.9 times the speedup compared to the Brouwer-Zimmerman algorithm implemented in the MAGMA V2.22-3 package. The low weight codeword 212 was found based on the proposed method in 4 147 201 seconds using an Intel 7700K 64GB processor and a 1070 8GB graphics card. Finding this code word won first place in the international low-weight word search competition run by the French National Center for Scientific Research (CNRS), the National Institute for Research in Digital Sciences and Technologies (Inria Paris), and the National Research Institute for Mathematics and Informatics in the Netherlands (CWI).

Keywords: Number Geometry, Error Correction Code, Hamming distance estimation, Shortest Vector Problem, Shortest Basis Problem, Extremal lattices, Kannan embedding

For citation: Usatjuk V.S., Egorov S.I., Vatutin E.I., Chernetskaya I.E. Ensuring Noise Immunity of a Communication Channel by Using a Method of Searching for Small-Weight Words in Linear Block Binary and Ternary Codes. *Trudy MAI*, 2024, no. 138. URL: https://trudymai.ru/eng/published.php?ID=182673

Введение

В настоящее время значительное внимание уделяется разработке и внедрению беспилотных летательных аппаратов (БПЛА) различного назначения.

Функциональность и надежность БПЛА во многом определяется используемым каналом передачи данных [1-4]. Данные, в том числе видео, должны надежно передаваться в реальном времени с большой скоростью на возможно большее расстояние. Также необходимо обеспечить защиту данных, передаваемых в эфире, от их перехвата. Для этого необходимо применение продвинутых систем коррекции ошибок (FEC – forward error correction) и шифрования.

В контексте разработки продвинутых систем FEC и шифрования возникает необходимость построения помехоустойчивых кодов с заданными свойствами [5], важнейшим из которых является минимальное кодовое расстояние [6].

Эта задача эффективно может быть решена с использованием математического аппарата геометрии чисел, математические методы которой получили признание за пределами специализированных кругов только недавно. Приложение методов геометрии чисел позволило осуществить упрощение эквалайзера приемника по критерию максимального правдоподобия с использованием сферических декодеров для применяемых на практике модуляционных созвездий, [7-8]. Ранее эта задача считалась NP-полной и не разрешимой на практике даже для сравнительно малой размерности.

Задача поиска минимального кодового расстояния эквивалентна задаче поиска кодового слова минимального веса, и является NP-полной, [9]. В статье предложен метод, позволяющий с малой сложностью находить слова малого веса в линейных блочных кодах без использования циклических, квазициклических и иных свойств симметрии (блочной структуры).

Решетки

Решетка – дискретная абелева подгруппа, заданная в пространстве R^m.

Пусть базис $B = \{\bar{b}_1, ..., \bar{b}_m\}$ задан линейно-независимыми векторами в R^n. Тогда под решеткой будем понимать множество целочисленных линейных комбинаций этих векторов:

$$L(\bar{b}_1, ..., \bar{b}_m) = \{\sum_{i=1}^{m} x_i \bar{b}_i : (x_1, ..., x_m) \in Z^m\},$$

где n и m, размерность и ранг решетки, соответственно, $n \geq m$. Решетки, для которых $n = m$, называются полными.

Площади (объемы в многомерном случае) фундаментальных параллелепипедов, образованных всевозможными базисами одной решетки L, будут равны det(L) (инварианту решетки), см. рис. 1.

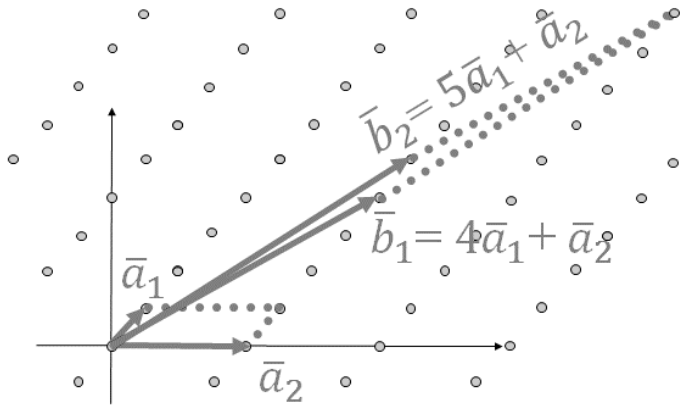


Рис. 1. Фундаментальные параллелепипеды, образованные разными базисами решетки

Важными задачами геометрии чисел являются: задача поиска короткого вектора, задача поиска короткого базиса решетки и задача поиска ближайшего вектора.

Задача поиска короткого вектора (ε-short vector problem, $\mathrm{SVP}_{\varepsilon}(n)$). Пусть дана n-мерная решетка $L(B)$ и вещественное ε>1. Найти нетривиальный вектор длины $\lambda_1(L)$ в ε-раз больший кратчайшего вектора в решетке $\bar{b} \in L : \left\|\bar{b}\right\| \le \varepsilon \cdot \lambda_1(L)$. При $\varepsilon = 1$ решается задача поиска кратчайшего вектора в решетке, при $\varepsilon > 1$ – короткого вектора.

Задача поиска короткого базиса решетки (ε-short basis problem, $\mathrm{SBP}_{\varepsilon}(n)$). Пусть дан базис полной решетки B и вещественное $\varepsilon > 1$. Найти базис $A = \{\bar{a}_1, \bar{a}_2, ..., \bar{a}_n\} : L(B) = L(A), \prod_{i=1}^{n} \left\|\bar{a}_i\right\| \le \varepsilon \cdot \prod_{i=1}^{n} \left\|\bar{b}_i^{\perp}\right\|$, где $\bar{b}_i^{\perp}$ – ортогональные вектора, полученные из базиса B.

Задача поиска ближайшего вектора (closest vector problem, $\mathrm{CVP}_{\varepsilon}(n)$). В решетке с базисом B найти вектор $\bar{b} \in L(B)$, ближайший к заданному вектору $\bar{j} \notin L(B)$. Эта задача является неоднородным (гетерогенным) вариантом SVP-задачи, (см. рис. 2).

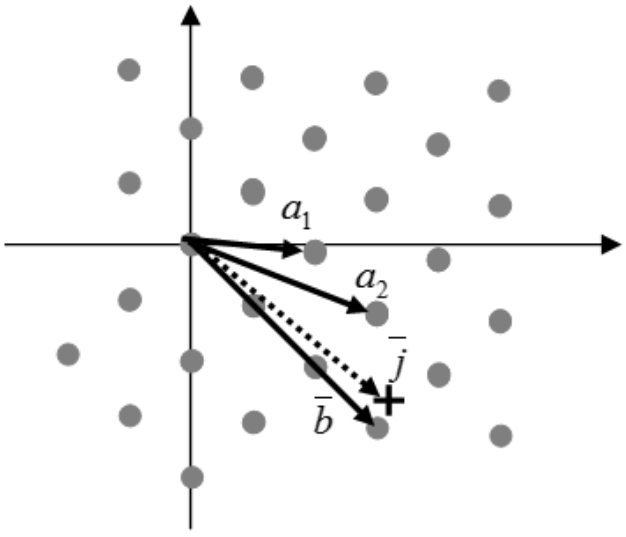


Рис. 2 Пример CVP-задачи в $\boldsymbol{R}^2$, $\bar{b} = CVP(L(\bar{a}_1, \bar{a}_2))$

Под плотностью решетки понимают величину равную отношению объема, занимаемого плотной упаковкой *n*-мерными шарами (не пересекающимися) радиуса, равного половине длины кратчайшего вектора решетки, к объему этой решетки:

$$\Delta(L) = V_n(\frac{\lambda_1}{2}) \cdot (\det(L))^{-1}.$$

Минковский в своей неопубликованной работе 1905 г. неконструктивно доказал, что существуют решетки с плотностью $\Delta \geq 2^{-n+1}$. В теореме Минковского-Главки результат был уточнен $\Delta \geq \frac{\zeta(n)}{2^{n-1}}$, где $\zeta(n)$ – Дзета-функция Римана, стремящаяся к 1 при $n \to \infty$, [10].

Под относительной плотностью решетки будем понимать скалярную величину:

$$rd(L) = \lambda_1 \cdot \gamma_n^{\frac{-1}{2}} (\det(L))^{\frac{-1}{n}},$$

где γ_n – константа Эрмита.

Эта величина демонстрирует во сколько раз кратчайший вектор в решетке L меньше по сравнению с наибольшим из кратчайших векторов в решетках такой же размерности: $rd(L) = \frac{\lambda_1(L)}{\max \lambda_1'(L')}$, $\det(L') = \det(L)$. Величина принадлежит полуотрезку $0 < rd(L) \leq 1$, причем $rd(L) = 1$ только для наиплотнейших (экстремальных) решеток. Такие решетки и точные значения константы Эрмита известны для размерностей *n* = 1, 2, …, 8; 24, (см. табл. 1).

Таблица 1

Параметры наиплотнейших решетчатых упаковок, [10]

Размерность решетки, n	2	3	4	5	6	7	8	24
Плотность решетки, $\Delta\ (L)$	0.9069	0.74	0.62	0.46	0.373	0.295	0.254	0.0019
Константа Эрмита, γ_n	$\frac{2}{\sqrt{3}}$	$\sqrt[3]{2}$	$\sqrt[4]{4}$	$\sqrt[5]{8}$	$\frac{2}{\sqrt[6]{3}}$	$\sqrt[7]{64}$	2	4

Диаграмма Вороного, также известная как многоугольник Вороного (с вершиной и ребрами) или ячейка Делоне, $V(x)$ – это геометрическая область вокруг каждого узла решетки, содержащая все точки решетки, находящиеся ближе к этому узлу решетки, чем к любой другой точке решетки. Пусть L – решетка в n-мерном евклидовом пространстве, и пусть $x \in L$ – точка решетки, принадлежащая этой решетке. Ячейка Вороного $V(x)$, связанная с точкой решетки x, определяется как совокупность всех точек y в евклидовом пространстве, для которых выполняется следующее условие, рис. 3:

$$V(x) = \{y \in R^n : ||y - x|| <= ||y - y'|| \forall y' \in L, y' \neq x\}.$$

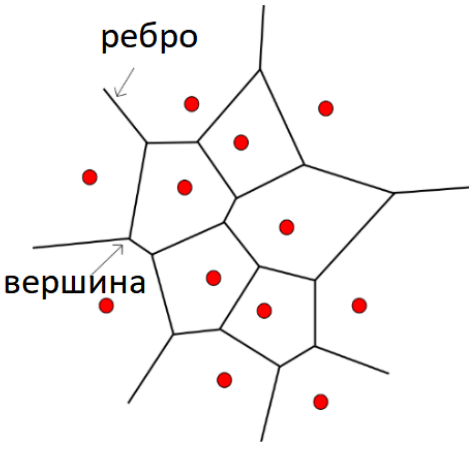


Рис. 3 Пример многоугольника Вороного с ребром и вершиной, образованного точкой (узлом) решетки

Эти ячейки (многоугольники) делят пространство на непересекающиеся области, и каждый узел решетки связан с одной такой областью.

Решения задач геометрии чисел: поиска кратчайшего вектора, поиска ближайшего вектора, поиска короткого (кратчайшего) вектора, тем сложнее, чем плотнее решетка. Ассимптотически сложными для поиска кратчайшего вектора (в том числе вероятностными методами) являются «плотные решетки»: сложные по Айтаю решетки, сложные по Гольдштейну-Майеру решетки [11], решетки Лагариса-Одлузко-Шнора (порождаемые задачей о рюкзаке с плотностью близкой к 1). Также существуют наиплотнейшие решетки, для которых нет алгоритмов построения.

Базис $B = \{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n\}$ решётки $L \subset R^n$ приведён по длине, если в результате ортогонализации решетки методом Грамма-Шмидта выполняется следующее неравенство:

$$\left|\mu_{i,j}\right| \le \frac{1}{2}, 1 \le j < i \le n,$$

где $\mu_{i,j}$ – коэффициенты Грамма-Шмидта.

Коркин и Золотарев в своей работе [12,13] представили алгоритм минимизации положительных квадратичных форм и верхнюю оценку точности приведения базиса решетки $c(n) = \sqrt{\gamma_n^n \prod_{i=1}^{n} \frac{i+3}{4}}$. При этом в алгоритме приведения решетки появляется вариативный параметр β – размер рассматриваемой подрешетки $L^{(\beta)}$, выбор которого позволяет получить алгоритм со сложностью, варьирующейся

от *полиномиальной до экпоненциальной (от субэкспоненциальной до экспоненциальной)*. Впоследствие именно на основе работ Коркина и Золотарева Шнором и Эхлером был предложен блочный алгоритм Коркина-Золотарева, [14].

Упорядоченный по длине базис $B = \{\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n\}$ решётки $L \subset R^n$ приведён блочным методом Коркина-Золотарева с размером блока $\beta \in [2, n]$ и точностью $\delta \in \left(\frac{1}{2}; 1\right]$, если:

– базис B приведён по длине;

– $\delta^2 \cdot \left\|\bar{b}_i^{\perp}\right\|^2 \le \lambda_1^2(L_i), i = 1, \ldots, n,$ где $\lambda_1(L_i)$ – длина кратчайшего вектора в решётке L_i, образованной ортогональным дополнением векторного пространства с базисом $\bar{b}_i, \ldots, \bar{b}_{\min(i+\beta-1, n)}$.

Базис решетки приведен по Ленстра-Ленстра-Ловасу (LLL-алгоритмом), если он приведен блочным методом Коркина-Золотарева с размером блока $\beta = 2$ и точностью ортогонализации $\delta \in \left(\frac{1}{2}; 1\right)$, [15].

Метод поиска кодовых слов минимального веса

Предлагаемый в работе метод поиска кодовых слов минимального (малого) веса требует построения решетки на основе порождающей матрицы систематического кода (вложение Каннана, [16-19]):

$$B_c = \begin{pmatrix} G^T & qI_n \\ I_k & 0 \end{pmatrix}, \qquad (1)$$

где n – длина кода, k – его размерность, q – размерность алфавита, I_k – единичная матрица размера $k \times k$, G – порождающая матрица, $G \in R^{k \times n}, B_c \in R^{(n+k)\times(k+n)}$.

В случае несистематического кода:

$$B_c = \begin{pmatrix} N \cdot G' & N \cdot qI_n \\ I_k & 0 \end{pmatrix}, \quad (2)$$

где N – масштабирующий коэффициент, G' – порождающая матрица несистематического кода.

После построения решетки и ее приведения в ней ищется вектор $\|x\|_\infty = 1,\ x \in L,\quad rank(L) = n$ с минимальным числом отличных от нуля координатных компонент, представляющий собой кодовое слово минимального веса. Кодовые слова двоичного $q = 2$, $-1 \equiv 1 \bmod 2$ и троичного кодов $q = 3, -1 \equiv 2 \bmod 3$ будут представлены векторами решетки, с координатными компонентами, принимающими значения из множества $\{-1, 0, 1\}$.

Особенностью метода является использование при поиске вектора x набора эвристических стратегий.

Метод поиска слова малого (минимального) веса в коде предусматривает выполнение следующих этапов.

1. *Вложение (Каннана) кода в решетку.* Вычисляется базис решетки B_c по формулам (1) или (2).

2. *Приведение базиса решетки*. Для приведения решетки используется блочный метод Коркина-Золотарева с размером блока β. После удаления линейно

зависимых строк и столбцов получается некоторый короткий базис решетки с рангом, равным размерности кода $m = k$.

3. *Ортогонализация базиса решетки* B_c *методами QR-разложения* с целью получения ортогонального базиса решетки $\bar{b}_1^{\perp},\ldots,\bar{b}_m^{\perp}$ и коэффициентов Грама-Шмидта.

Ортогонализация базиса по Граму-Шмидту выполняется следующим образом:

$$\bar{b}_1^{\perp} = \bar{b}_1,\ \bar{b}_i^{\perp} = \bar{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\bar{b}_j^{\perp}, i = 2,3,\ldots,m,$$

где $\mu_{i,j}$ – коэффициенты Грама-Шмидта, вычисляемые по формуле

$$\mu_{i,j} = \frac{\left\langle \bar{b}_i, \bar{b}_j^{\perp} \right\rangle}{\left\langle \bar{b}_j^{\perp}, \bar{b}_j^{\perp} \right\rangle} = \frac{\left\langle \bar{b}_i, \bar{b}_j^{\perp} \right\rangle}{\left\| \bar{b}_j^{\perp} \right\|^2}.$$

Коэффициенты Грама-Шмидта образуют верхнюю треугольную матрицу с $m \times (m-1)/2$ ненулевыми элементами.

Для ускорения ортогонализации базиса, предложено применять вместо модифицированного метода Грамма-Шмидта, параллельные методы QR-разложения матриц: блочный метод Хаусхолдера при использовании многоядерных процессоров и метод поворота Гивенса при использовании видеокарт.

4. *Поиск кратчайшего вектора в решетке*. После чего в решетке ищется вектор с минимальным числом отличных от нуля координатных компонент. Количество отличных от нуля компонент найденного вектора равняется искомому кодовому расстоянию.

Задача поиска кратчайшего вектора x в решетке сводится к целочисленному решению системы неравенств:

$$\begin{cases} x_m^2 \left\| \bar{b}_m^{\perp} \right\|^2 \le A^2, \\ (x_{m-1} + \mu_{m,m-1} x_n) \left\| \bar{b}_{m-1}^{\perp} \right\|^2 \le A^2 - x_m^2 \left\| \bar{b}_m^{\perp} \right\|^2, \\ \dots \\ (x_1 + \sum_{i=2}^{m} x_i \mu_{i,j})^2 \left\| \bar{b}_1^{\perp} \right\|^2 \le A^2 - \sum_{j=2}^{m} l_j \end{cases}$$

где A – верхняя оценка кодового расстояния (начальная норма $A = (m+1) \times r_{\max}^2$), x_i – координатная компонента искомого вектора $l_j = (x_j + \sum_{i=j+1}^{m} x_i \mu_{i,j})^2 \left\| \bar{b}_j^{\perp} \right\|^2$ – частичная сумма.

Для этой цели используется метод Каннана-Финке-Поста (КФП).

Метод КФП представляет собой вариант метода ветвей и границ и заключается в переборе линейных комбинаций базисных векторов решётки, дающих вектор с нормой, ограниченной сверху оценкой A, которая может уменьшаться в процессе поиска.

Решение задачи поиска кратчайшего вектора в решетке по методу КФП заключается в полном переборе всех линейных комбинаций векторов базиса решетки $\|x\|^2 = \left\| \sum_{i=1}^{m} x_i \bar{b}_i \right\|^2 \le A^2, x_i \in Z$, где A – норма искомого кратчайшего вектора. В качестве нормы берётся верхняя оценка длины кратчайшего вектора, $A = \sqrt{\gamma_m} \det(L)^{\frac{1}{m}}$, где γ_m – константа Эрмита. В тех случаях, когда наименьший из векторов в базисе решетки превосходит оценку $\left\| \bar{b}_1 \right\| > \sqrt{\gamma_m} \det(L)^{\frac{1}{m}}$ используется более

плотная верхняя оценка $A = d_{min}\big(C(H)\big)$, [20-22]. Предварительное приведение базиса решетки позволяет уменьшить пространство перебора x_i .

Эту задачу можно решить путем обхода дерева от корня к листьям, в каждой из вершин которого решается соответствующее линейное уравнение. Из корня этого дерева выходит $2 \cdot \left\lceil \frac{A}{\|\bar{b}_m^{\perp}\|} \right\rceil$ ветвей. В силу симметричности дерева (по свойствам нормы) для получения искомого кратчайшего вектора необходимо перебрать только половину его вершин, см. рис. 4.

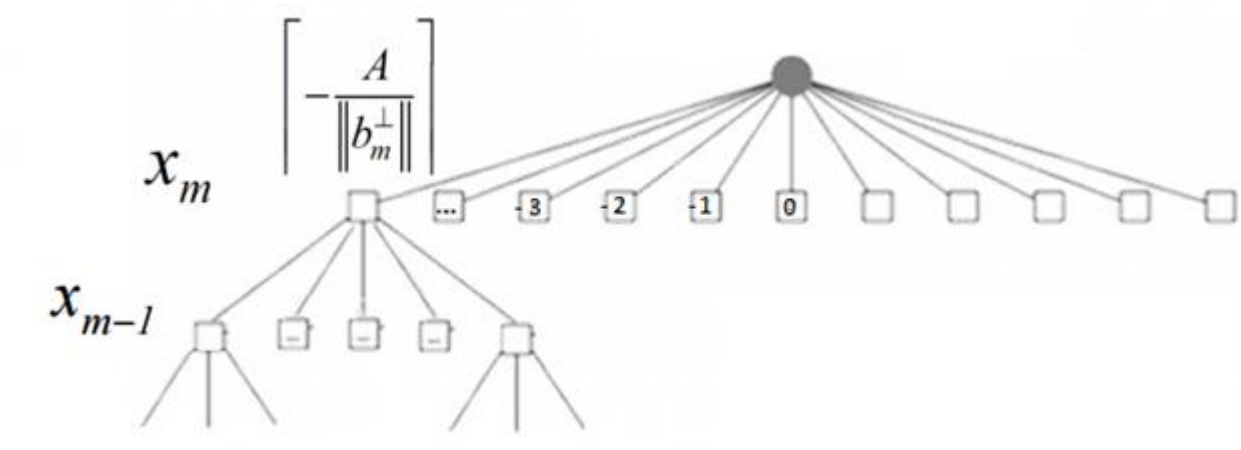


Рис. 4 Дерево перебора в методе Каннана-Финке-Поста

В результате полного обхода дерева от корня к листьям, будет получен предполагаемый кратчайший вектор *x* с нормой, меньше либо равной искомой. Если норма полученного вектора будет меньше заданной ранее, целесообразно обновить ее с целью уменьшения пространства перебора. Остановка алгоритма осуществляется, когда завершен обход вершин дерева, или когда получен вектор с достаточной нормой в случае поиска короткого вектора.

На втором этапе метода (приведение базиса решетки) для его ускорения используются следующие эвристики.

Эвристики на основе перестановок базиса решетки с последующим приведением базиса решетки (вставка подпространства). Метод BKZ (блочный метод Коркина-Золотарева) улучшает качество базиса и ускоряет поиск кратчайшего вектор в нем, [23-25].

Эвристики поиска в двойственном пространстве (двойственной решетке). Алгоритмы поиска кратчайшего базиса применяются в двойственном пространстве (в пространстве смежных классов, в двойственной решетке), [26-28].

Эвристики, основанные на сведение поиска оптимального отсечения к методам линейного программирования. В некоторых случаях подпространства решеток (подрешеток малых размерностей, определенных плотностей) может быть эффективно ограничено наименьшим числом гиперплоскостей, выбор которых может быть осуществлен путем решения задач целочисленного программирования в пакетах CPLEX и Gurobi, [29-32].

На четвертом этапе метода (поиск кратчайшего вектора в решетке) для его ускорения используются следующие эвристики.

Эвристики на основе длин векторов (отсечение веток в дереве перебора).

Гауссово отсечение веток [33] – это метод, используемый в алгоритмах приведения решеток, таких как алгоритм LLL (Lenstra-Lenstra-Lovász) для уменьшения глубины дерева перебора. Он основан на предположении о числе веток на каждом из уровней дерева перебора, $H_k = \frac{1}{2} \times \frac{V_k(A_k)}{\prod_{i=m+1-k}^{m} \left\| \bar{b}_i^{\perp} \right\|}$, ($k$ – номер уровня) и в

случае отклонения от этого числа, такие ветки считаются маловероятно содержащими кратчайший (короткий) вектор.

Линейная функция отсечения веток, [33]. Эта функция применяется для вычисления нормы кратчайшего вектора на каждом из $k \in [m, m-1, \ldots, 1]$ уровней:

$$A_k = \left(\frac{k}{m}\right) \times A^2, 1 \leq k \leq m.$$

Кусочно-линейная функция отсечения веток [33] предусматривает использование параметра $\alpha > \frac{1}{2}$:

$$\mathrm{A_k} = \alpha \times \mathrm{A^2}: 1 \leq \mathrm{k} \leq \frac{\mathrm{m}}{2}; \mathrm{A_k} = \mathrm{A^2}: \mathrm{k} > \frac{\mathrm{m}}{2}.$$

В работе [33] было показано для $\alpha \approx \frac{1}{2}$, что ускорение поиска кратчайшего вектора достигает величины $2^{\frac{\mathrm{m}}{4}} \approx 1.189^{\mathrm{m}}$, при этом вероятность ошибочного отсечения кратчайшего вектора меньше 5%.

Шаговая функция отсечения веток, [33] предусматривает использование параметра $0 < \alpha < \frac{1}{4}$:

$$\mathrm{A_k} = \left(\frac{2k}{m}\right) \times \alpha \times \mathrm{A^2}: 1 \leq \mathrm{k} \leq \frac{\mathrm{m}}{2}; \mathrm{A_k} = \left(2\alpha - 1 + \frac{2k(1-\alpha)}{m}\right) \times \mathrm{A^2}: \mathrm{k} > \frac{\mathrm{m}}{2}.$$

Экстремальное отсечения веток (Extream pruning) основывается на замене гиперсферы Гауссовой эвристики телом пересечения цилиндров, [34]:

$$H_k = \sum_{k=1}^{m} \frac{1}{2} \times \frac{V_k(C_{A_k})}{\prod_{i=m+1-k}^{m} \left\| \bar{b}_i^{\perp} \right\|}.$$

Тело пересечения цилиндров описывается следующей формулой:

$$\mathrm{C}_k = \left\{ x_i \in A^k, \forall j \leq k, \sum_{l=1}^{j} x_l^2 \leq R_j^2 \right\},$$

где R_j – радиус цилиндра на j-уровне.

Короткие векторы часто находятся вблизи края диаграммы Вороного и могут иметь более короткие нормы по сравнению с другими векторами. Тело пересечения цилиндров лучше приближает диаграммы Вороного. В частности, этот метод для 90-мерной решетки позволил найти кратчайший вектор за несколько дней вместо 8710 лет.

Эвристики округления основаны на сведении задачи поиска кратчайшего вектора к задаче поиска ближайшего вектора с использованием алгоритма Бабаи (Babai, Closest Vector Problem method), [35, 36]. Эти эвристики определяют, насколько хорошо вектор можно округлить до ближайшей точки решетки. Вектор, который трудно округлить, скорее всего, будет коротким (кратчайшим).

Эвристика плотности: меры плотности решетки показывают, насколько плотно точки решетки распределены в области вокруг вектора. Области с низкой плотностью с большей вероятностью будут содержать кратчайшие вектора, Эвристика плотности приводит к вероятностному методу поиска [37].

Реализация и экспериментальное исследование метода

Быстродействие предложенного метода поиска слов малого веса зависит от быстродействия метода поиска кратчайшего вектора КФП. Быстродействие последнего можно значительно увеличить с применением эвристик.

Метод КФП может быть реализован в ЭВМ на процессоре или видеокарте. Первый вариант предпочтителен для решеток небольшой размерности. Для малых

размерностей затраты на пересылку данных в память видеокарты превышают выигрыш от ускорения обработки [38,39].

Поиск кратчайшего вектора в решетке большой размерности ($n > 30 \dots 40$) целесообразно выполнять при помощи видеокарты на программной модели NVIDIA CUDA - варпа (warp - 32 последовательно идущих треда (потока), выполняющихся физически одновременно). Планировщик варпа выполняет декомпозицию дерева перебора метода КФП на составляющие, выделяя ту часть, которую он будет обрабатывать самостоятельно и ту, которую будет выполнять видеокарта (или возможно ПЛИС [40]) в соответсвие с *набором эвристик, рассмотренных ранее*.

Дерево перебора для не полностью приведенного базиса решетки (с размером блока $\beta << m$) крайне несбалансированно, эффективность работы алгоритма будет зависить от качества декомпозиции дерева перебора на поддеревья. Еще одним важным фактором, влияющим на эффективность поиска кратчайшего вектора является частота обновления значения нормы предполагаемого кратчайшего вектора. В случае слишком частого обновления задержка на обновление может превысить совокупное ускорение работы алгоритма за счет отсечения веток новой нормой. Таким образом эффективность работы алгоритма зависит от качества декомпозиции и частоты обновления нормы.

При реализации декомпозиции использовался гибридный подход, сочетающий стратегии поиска по дереву в ширину и в глубину. Выполнение каждым потоком видеокарты независимого поиска в глубину привело бы к ветвлению и неэффективному доступу к памяти.

Планировщик варпа поддерживает список открытых узлов, представляющих поддеревья, которые предстоит обработать. Каждому потоку назначается узел из этого списка, и он вычисляет его дочерние элементы (обычно несколькими потоками для обработки большого количества дочерних элементов). Дочерние элементы затем добавляются в список.

Сначала обрабатываются узлы на текущем уровне дерева. Чтобы обеспечить эффективные механизмы доступа к памяти, все потоки фокусируются на узлах одного уровня, а открытые узлы организуются и сохраняются по соответствующим уровням.

Предложенный метод поиска кодового расстояния продемонстрировал более высокое быстродействие при решении задач приближенной оценки кодового расстояния, чем алгоритм Брауэра-Циммермана, реализованный в пакете MAGMA V2.22-3, [41].

Сравнение выполнялось на двоичном блочном коде длины 1280 и скорости 0,5, проверочная матрица которого без таких свойств симметрии, как цикличность или квазицикличность, была представлена на международном конкурсе [6]. Конкурс по поиску кодовых слов с малым весом организован Французским национальным центром научных исследований (CNRS), Национальным институтом исследований в области цифровых наук и технологий (Inria, Paris) и Национальным исследовательским институтом математики и информатики в Нидерландах (CWI).

Для верхней оценки кодового расстояния и получения кодового слова малого веса 228 алгоритму Брауэра-Циммермана из пакета MAGMA V2.22-3 потребовалось

бы 6 279 197 секунд. Для решения этой же задачи лучшей автономной реализации алгоритма Брауэра-Циммермана с векторизацией и распараллеливанием [42] потребовалось бы 1 779 123 секунд.

Для получения кодового слова малого веса 228 предложенному методу потребовалось менее 1 979 секунд, ускорение предложенного метода по сравнению с алгоритмом Брауэра-Циммермана из пакета MAGMA составляет 3172.9 раза, ускорение предложенного метода по сравнению с автономной реализацией алгоритма Брауэра-Циммермана [42] составляет 899 раз.

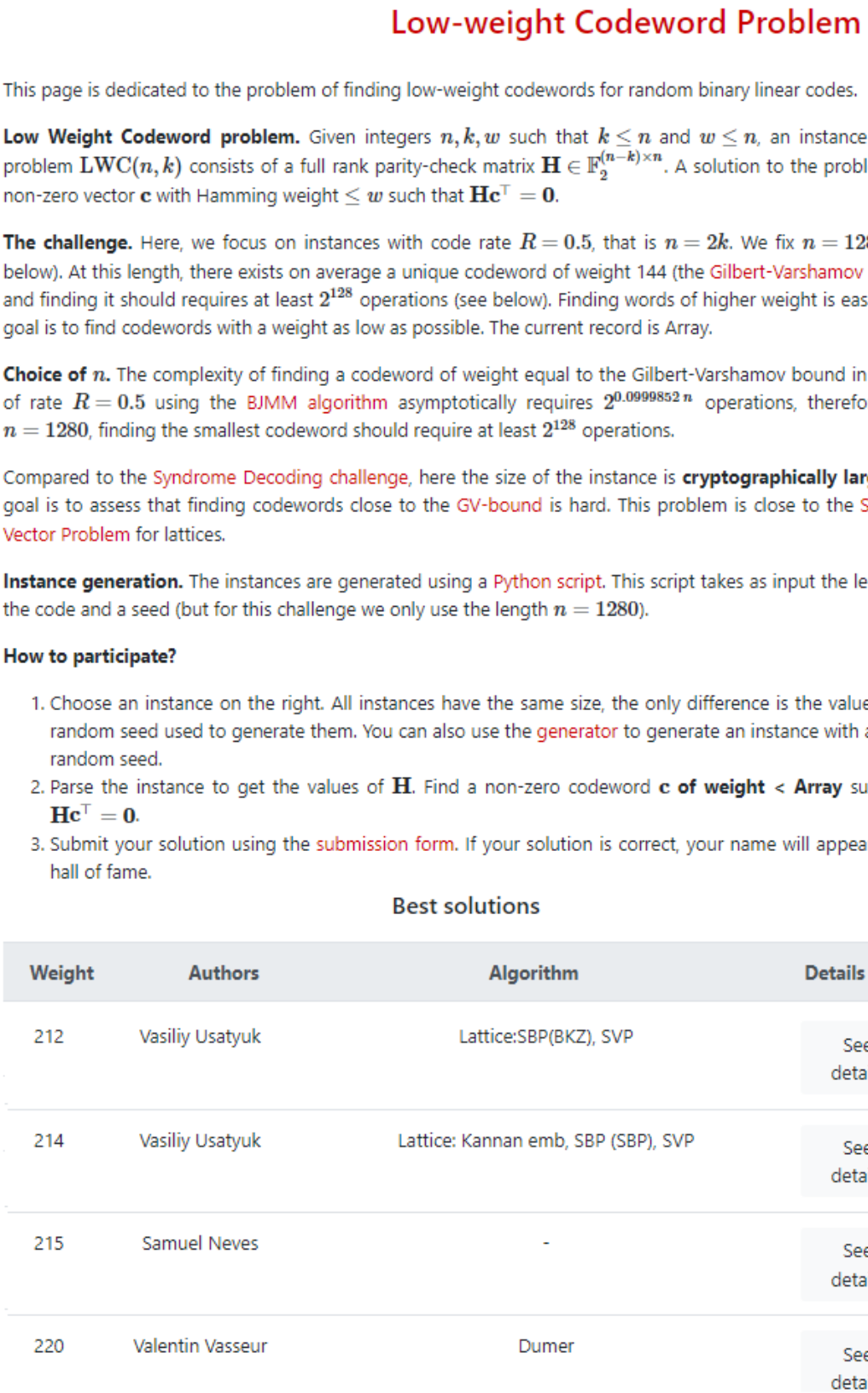
Для верхней оценки кодового расстояния и получения кодового слова малого веса 212 алгоритму Брауэра-Циммермана потребовалось бы 10^{121} секунд или 10^{114} лет [41]. Кодовое слово этого веса было найдено на основе предложенного метода за 4 147 201 секунд с использованием процессора Intel 7700K 64ГБ и видеокарты 1070 8ГБ.

Используемая методика предусматривала применение на подрешетке размерности $m \leq 32$ следующих наборов эвристик: эвристики приведения базиса в двойственном пространстве решетки, эвристики экстремального отсечения веток (вероятностного поиска в случае оптимизации матожидания и дисперсии кратчайшего вектора в решетке), эвристики плотности решетки.

Детали программной реализации предложенного метода представлены в [43].

Нахождение кодового слова малого веса 212 позволило занять первое место в международном конкурсе поиска слов малого веса [6], проводимом Французским национальным центром научных исследований (CNRS), Национальным институтом

исследований в области цифровых наук и технологий (Inria, Paris) и Национальным исследовательским институтом математики и информатики в Нидерландах (CWI) (рис. 5).



Low-weight Codeword Problem

This page is dedicated to the problem of finding low-weight codewords for random binary linear codes.

Low Weight Codeword problem. Given integers n, k, w such that $k \leq n$ and $w \leq n$, an instance of the problem $\mathbf{LWC}(n, k)$ consists of a full rank parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$. A solution to the problem is a non-zero vector $\mathbf{c}$ with Hamming weight $\leq w$ such that $\mathbf{Hc}^\top = \mathbf{0}$.

The challenge. Here, we focus on instances with code rate $R = 0.5$, that is $n = 2k$. We fix $n = 1280$ (see below). At this length, there exists on average a unique codeword of weight 144 (the Gilbert-Varshamov bound) and finding it should requires at least 2^{128} operations (see below). Finding words of higher weight is easier. The goal is to find codewords with a weight as low as possible. The current record is Array.

Choice of n. The complexity of finding a codeword of weight equal to the Gilbert-Varshamov bound in a code of rate $R = 0.5$ using the BJMM algorithm asymptotically requires $2^{0.0999852\,n}$ operations, therefore with $n = 1280$, finding the smallest codeword should require at least 2^{128} operations.

Compared to the Syndrome Decoding challenge, here the size of the instance is **cryptographically large**. The goal is to assess that finding codewords close to the GV-bound is hard. This problem is close to the Shortest Vector Problem for lattices.

Instance generation. The instances are generated using a Python script. This script takes as input the length of the code and a seed (but for this challenge we only use the length $n = 1280$).

How to participate?

1. Choose an instance on the right. All instances have the same size, the only difference is the value of the random seed used to generate them. You can also use the generator to generate an instance with another random seed.
2. Parse the instance to get the values of $\mathbf{H}$. Find a non-zero codeword $\mathbf{c}$ **of weight <** **Array** such that $\mathbf{Hc}^\top = \mathbf{0}$.
3. Submit your solution using the submission form. If your solution is correct, your name will appear in the hall of fame.

Best solutions

Weight	Authors	Algorithm	Details
212	Vasiliy Usatyuk	Lattice:SBP(BKZ), SVP	See details
214	Vasiliy Usatyuk	Lattice: Kannan emb, SBP (SBP), SVP	See details
215	Samuel Neves	-	See details
220	Valentin Vasseur	Dumer	See details

Рис. 5 Скриншот результатов международного конкурса, [6]

Выводы

В статье предложен новый метод поиска слов малого веса в линейном блочном двоичном и тернарном кодах на основе геометрии чисел с использованием семейства эвристик. Предложенный метод имеет высокое быстродействие при решении задач приближенной оценки кодового расстояния. Этот метод на задаче поиска слова малого веса 228 продемонстрировал 3172.9 кратное ускорение по сравнению с алгоритмом Брауэра-Циммермана, реализованном в пакете MAGMA V2.22-3. Предложенный метод поиска слов малого веса может быть использован для построения помехоустойчивых кодов для систем связи беспилотных летательных аппаратов.

Список источников

1. Бородин В.В., Петраков А.М., Шевцов В.А. Анализ эффективности передачи данных в сети связи группировки беспилотных летательных аппаратов // Труды МАИ. 2015. № 81. URL: https://trudymai.ru/published.php?ID=57894

2. Ананьев А.В., Иванников К.С., Филатов С.В. Основные принципы построения систем связи на базе беспилотных летательных аппаратов // Труды МАИ. 2022. № 125. URL: https://trudymai.ru/published.php?ID=168188. DOI: 10.34759/trd-2022-125-16

3. Титов К.Д. Принципы построения сверхширокополосного канала связи на беспилотном летательном аппарате вертолетного типа легкого класса // Труды МАИ.

2022. № 122. URL: https://trudymai.ru/published.php?ID=164250. DOI: 10.34759/trd-2022-122-12

4. Волков А.С. Разработка имитационной модели канала с группирующимися ошибками // Труды МАИ. 2023. № 128. URL: https://trudymai.ru/published.php?ID=171396. DOI: 10.34759/trd-2023-128-12

5. Усатюк В.С., Егоров С.И. Построение квазициклических недвоичных низкоплотностных кодов на основе совместной оценки их дистантных свойств и спектров связности // Телекоммуникации. 2016. № 8. С. 32-40.

6. Aragon N., Lavauzelle J., Lequesne M. Low-weight codewords problem challenge, 2019. URL: https://decodingchallenge.org/low-weight

7. Burg A., Wenk M., Zellweger M., Wegmueller M., Felber N., and Fichtner W. VLSI implementation of the sphere decoding algorithm // Proceedings of the 30th European Solid-State Circuits Conference, Leuven, Belgium, 2004, pp. 303-306.

8. Усатюк В.С. Приложение блочного метода Коркина-Золотарева для демодуляции сигналов MIMO // Обозрение прикладной и промышленной математики. 2015. № 5 (22). С. 600-602.

9. Dumer I., Micciancio D., and Sudan M. Hardness of approximating the minimum distance of a linear code // IEEE Transactions on Information Theory, 2003, vol. 49, no. 1, pp. 22-37. DOI: 10.1109/SFFCS.1999.814620

10. Конвей Дж., Слоэн Н. Упаковки шаров, решетки и группы: В 2-х т. Пер. с англ. – М.: Мир, 1990. Т. 2. - 367 с.

11. Goldstein D., Mayer A. On the equidistribution of Hecke points // Forum Mathematicum, 2003, vol. 15, no 2, pp. 165–189. DOI: 10.1515/form.2003.009

12. Korkine A., Zolotareff G. Sur les formes quadratiques // Mathematische Annalen, 1873, no. 6, pp. 366-389. DOI: 10.1007/BF01442912

13. Lagarias J.C., Jr. Lenstra H.W., Schnorr C.P. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice // Combinatorica, 1990, vol. 10 (4), pp. 333-348. DOI: 10.1007/BF02128669

14. Schnorr C-P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems // Fundamentals of Computation Theory, 1991, pp. 68-85.

15. Lenstra A., Lenstra H., Lovász L. Factoring polynomials with rational coefficients // Mathematische Annalen, 1982, vol. 261 (4), pp. 515-534. DOI: 10.1007/BF01457454

16. Kannan R. Minkowski's convex body theorem and integer programming // Mathematics of operations research, 1987, vol. 12 (3), pp. 415-440. DOI: 10.1287/MOOR.12.3.415

17. Betten A., Braun M., Fripertinger H. Error-Correcting Linear Codes Classification by Isometry and Applications, Berlin, Springer-Verlag, 2006, pp. 594-596.

18. Усатюк В.С. Определение кодового расстояния недвоичного LDPC-кода блочным методом Коркина-Золотарева // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2015. № 3 (16). С. 76-85.

19. Ivanova V.S. Lattice Basis Reduction in Infinity, Bachelor Thesis, Technische Universitat Darmstadt, 2010, 31 p.

20. MacKay J., Davey M. C. Evaluation of Gallager codes for short block length and high rate applications, IMA Workshop on Codes, System and Graphical Models, Springer-Verlag, 2001, pp. 113-130.

21. Smarandashe R., Vontobel P.O. Quasi-cyclic LDPC codes: influence of proto- and Tanner-graph structure on minimum hamming distance upper bounds // IEEE Transactions on Information Theory, 2012, vol. 58, no 2, pp. 585-607. DOI: 10.1109/TIT.2011.2173244

22. Butler B.K., Siegel P.H. Bounds on the minimum distance of punctured quasi-cyclic LDPC codes // IEEE Transactions on Information Theory, 2013, vol. 59, no 7, pp. 4584-4597. DOI: 10.1109/TIT.2013.2253152

23. Fontein F., Schneider M., Wagner U. PotLLL: a polynomial time version of LLL with deep insertions // Designs Codes and Cryptographym, 2014, vol. 73, pp. 355–368. DOI: 10.1007/s10623-014-9918-8

24. Yasuda M., Yamaguchi J. A new polynomial-time variant of LLL with deep insertions for decreasing the squared-sum of Gram–Schmidt lengths // Designs Codes and Cryptographym, 2019, vol. 87, pp. 2489–2505. DOI: 10.1007/s10623-019-00634-9

25. Одед Р., Миссиансио Д. Криптография на основе решеток / перевод Усатюк В.С., 2010, 78 с. URL: https://www.researchgate.net/publication/331047955

26. Micciancio D., Walter M. Practical predictable lattice basis reduction // Annual International Conference on Theory Applications of Cryptographic Techniques, Berlin, 2016, pp. 820–849. DOI: 10.1007/978-3-662-49890-3_31

27. Neumaier A. Bounding basis reduction properties // Designs Codes and Cryptographym, 2017, vol. 84, pp. 237-259. DOI: 10.1007/s10623-016-0273-9

28. Yamamura K., Wang Y. Fujisaki E. Improved lattice enumeration algorithms by primal and dual reordering methods // IET Information Security, 2023, vol. 17 (1), pp. 35-45. DOI: 10.1049/ise2.12083

29. Schnorr C.P. Fast Factoring Integers by SVP Algorithms // Cryptology ePrint Archive, Paper 2021/933. URL: https://eprint.iacr.org/2021/933

30. McGuire Gary, Robinson Oisin. A New Angle on Lattice Sieving for the Number Field Sieve, 2020. URL: https://arxiv.org/pdf/2001.10860

31. Gabrielle de Micheli, Pierrick Gaudry, Cécile Pierrot. Lattice Enumeration for Tower NFS: a 521- bit Discrete Logarithm Computation // 27th Annual International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2021, pp.67-96. DOI: 10.1007/978-3-030-92062-3_3

32. Robinson O. An Implementation of the Extended Tower Number Field Sieve using 4d Sieving in a Box and a Record Computation in Fp4, 2022. URL: https://arxiv.org/abs/2212.04999

33. Schnorr C.P., Hörner H.H. Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction // Advances in Cryptology, LNCS, 1995, vol. 921, pp 1-12. DOI: 10.1007/3-540-49264-X_1

34. Gamma N., Nguyen P. Q., Regev O. Lattice Enumeration Using Extreme Pruning // Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology – EUROCRYPT, 2010, pp. 257–278. DOI: 10.1007/978-3-642-13190-5_13

35. Babai L. On lovasz lattice reduction and the nearest lattice point problem // Combinatorica, 1986, vol. 6, pp. 1-13. DOI: 10.1007/BF02579403

36. Micciancio D. The shortest vector problem is NP-hard to approximate to within some constant // SIAM Journal on Computing, 2001, no. 30, pp. 2008-2035. DOI: 10.1137/S0097539700373039

37. Усатюк В.С. Вероятностный метод определения кодового расстояния линейного блочного кода // Proceedings of the III International conference "Engineering&Telecommunication - En&T 2016", Moscow, MIPT, 2016, pp. 43-46.

38. Кузьмин О.В., Усатюк В.С. Параллельные алгоритмы вычисления локальных минимумов целочисленных решеток // Программные продукты и системы. 2015. № 1 (109). С. 55-62.

39. Усатюк В.С. Реализация параллельных алгоритмов ортогонализации в задаче поиска кратчайшего базиса целочисленной решетки // Прикладная дискретная математика. Приложение. 2012. № 5. С. 120-122.

40. Усатюк В.С., Егоров С.И. Устройство для оценки кодового расстояния линейного блочного кода методом геометрии чисел // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2017. № 4 (25), С. 24-33.

41. Bosma W., Cannon J.J., Fieker C., Steel A. Handbook of Magma functions, 2019, 6129 p.

42. Hernando F., Igual F. D., Quintana-Orti G. Algorithm 994: Fast Implementations of the Brouwer-Zimmermann Algorithm for the Computation of the Minimum Distance of a

Random Linear Code // ACM Transactions on Mathematical Software, 2019, vol. 45, no. 2, pp. 1-28. DOI: 10.1145/3302389

43. Support material for Low weight codewords problem search method. URL: https://github.com/Lcrypto/Low-weight_Codeword_Problem V2.22-3

References

1. Borodin V.V., Petrakov A.M., Shevtsov V.A. *Trudy MAI*, 2015, no. 81. URL: https://trudymai.ru/eng/published.php?ID=57894

2. Anan'ev A.V., Ivannikov K.S., Filatov S.V. *Trudy MAI*, 2022, no. 125. URL: https://trudymai.ru/eng/published.php?ID=168188. DOI: 10.34759/trd-2022-125-16

3. Titov K.D. *Trudy MAI*, 2022, no. 122. URL: https://trudymai.ru/eng/published.php?ID=164250. DOI: 10.34759/trd-2022-122-12

4. Volkov A.S. *Trudy MAI*, 2023, no. 128. URL: https://trudymai.ru/eng/published.php?ID=171396. DOI: 10.34759/trd-2023-128-12

5. Usatyuk V.S., Egorov S.I. *Telekommunikatsii*, 2016, no. 8, pp. 32-40.

6. Aragon N., Lavauzelle J., Lequesne M. *Low-weight codewords problem challenge*, 2019. URL: https://decodingchallenge.org/low-weight

7. Burg A., Wenk M., Zellweger M., Wegmueller M., Felber N., and Fichtner W. VLSI implementation of the sphere decoding algorithm, *Proceedings of the 30th European Solid-State Circuits Conference*, Leuven, Belgium, 2004, pp. 303-306.

8. Usatyuk V.S. *Obozrenie prikladnoi i promyshlennoi matematiki*, 2015, no. 5 (22), pp. 600-602.

9. Dumer I., Micciancio D., and Sudan M. Hardness of approximating the minimum distance of a linear code, *IEEE Transactions on Information Theory*, 2003, vol. 49, no. 1, pp. 22-37. DOI: 10.1109/SFFCS.1999.814620

10. Konvei Dzh., Sloen N. *Upakovki sharov, reshetki i gruppy* (Sphere Pakings, Lattices and Groups. Vol. II.) Moscow, Mir, 1990, 367 p.

11. Goldstein D., Mayer A. On the equidistribution of Hecke points, *Forum Mathematicum*, 2003, vol. 15, no 2, pp. 165–189. DOI: 10.1515/form.2003.009

12. Korkine A., Zolotareff G. Sur les formes quadratiques, *Mathematische Annalen*, 1873, no. 6, pp. 366-389. DOI: 10.1007/BF01442912

13. Lagarias J.C., Jr. Lenstra H.W., Schnorr C.P. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica*, 1990, vol. 10 (4), pp. 333-348. DOI: 10.1007/BF02128669

14. Schnorr C-P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems, *Fundamentals of Computation Theory*, 1991, pp. 68-85.

15. Lenstra A., Lenstra H., Lovász L. Factoring polynomials with rational coefficients, *Mathematische Annalen*, 1982, vol. 261 (4), pp. 515-534. DOI: 10.1007/BF01457454

16. Kannan R. Minkowski's convex body theorem and integer programming, *Mathematics of operations research*, 1987, vol. 12 (3), pp. 415-440. DOI: 10.1287/MOOR.12.3.415

17. Betten A., Braun M., Fripertinger H. *Error-Correcting Linear Codes Classification by Isometry and Applications*, Berlin, Springer-Verlag, 2006, pp. 594-596.

18. Usatyuk V.S. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie*. 2015, no. 3 (16), pp. 76-85.

19. Ivanova V.S. *Lattice Basis Reduction in Infinity, Bachelor Thesis*, Technische Universität Darmstadt, 2010, 31 p.

20. MacKay J., Davey M. C. *Evaluation of Gallager codes for short block length and high rate applications, IMA Workshop on Codes, System and Graphical Models*, Springer-Verlag, 2001, pp. 113-130.

21. Smarandashe R., Vontobel P.O. Quasi-cyclic LDPC codes: influence of proto- and Tanner-graph structure on minimum hamming distance upper bounds, *IEEE Transactions on Information Theory*, 2012, vol. 58, no 2, pp. 585-607. DOI: 10.1109/TIT.2011.2173244

22. Butler B.K., Siegel P.H. Bounds on the minimum distance of punctured quasi-cyclic LDPC codes, *IEEE Transactions on Information Theory*, 2013, vol. 59, no 7, pp. 4584-4597. DOI: 10.1109/TIT.2013.2253152

23. Fontein F., Schneider M., Wagner U. PotLLL: a polynomial time version of LLL with deep insertions, *Designs Codes and Cryptographym*, 2014, vol. 73, pp. 355–368. DOI: 10.1007/s10623-014-9918-8

24. Yasuda M., Yamaguchi J. A new polynomial-time variant of LLL with deep insertions for decreasing the squared-sum of Gram–Schmidt lengths, *Designs Codes and Cryptographym*, 2019, vol. 87, pp. 2489–2505. DOI: 10.1007/s10623-019-00634-9

25. Oded R., Missiansio D. *Kriptografiya na osnove reshetok* (Lattice-based Post-Quantum Cryptography), 2010, 78 p. URL: https://www.researchgate.net/publication/331047955

26. Micciancio D., Walter M. Practical predictable lattice basis reduction, *Annual International Conference on Theory Applications of Cryptographic Techniques*, Berlin, 2016, pp. 820–849. DOI: 10.1007/978-3-662-49890-3_31

27. Neumaier A. Bounding basis reduction properties, *Designs Codes and Cryptographym*, 2017, vol. 84, pp. 237-259. DOI: 10.1007/s10623-016-0273-9

28. Yamamura K., Wang Y. Fujisaki E. Improved lattice enumeration algorithms by primal and dual reordering methods, *IET Information Security*, 2023, vol. 17 (1), pp. 35-45. DOI: 10.1049/ise2.12083

29. Schnorr C.P. Fast Factoring Integers by SVP Algorithms, *Cryptology ePrint Archive*, Paper 2021/933. URL: https://eprint.iacr.org/2021/933

30. McGuire Gary, Robinson Oisin. *A New Angle on Lattice Sieving for the Number Field Sieve*, 2020. URL: https://arxiv.org/pdf/2001.10860

31. Gabrielle de Micheli, Pierrick Gaudry, Cécile Pierrot. Lattice Enumeration for Tower NFS: a 521- bit Discrete Logarithm Computation, *27th Annual International Conference on the Theory and Application of Cryptology and Information Security*, Singapore, 2021, pp.67-96. DOI: 10.1007/978-3-030-92062-3_3

32. Robinson O. *An Implementation of the Extended Tower Number Field Sieve using 4d Sieving in a Box and a Record Computation in Fp4*, 2022. URL: https://arxiv.org/abs/2212.04999

33. Schnorr C.P., Hörner H.H. Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction, *Advances in Cryptology, LNCS*, 1995, vol. 921, pp 1-12. DOI: 10.1007/3-540-49264-X_1

34. Gamma N., Nguyen P. Q., Regev O. Lattice Enumeration Using Extreme Pruning, *Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology – EUROCRYPT*, 2010, pp. 257–278. DOI: 10.1007/978-3-642-13190-5_13

35. Babai L. On lovasz lattice reduction and the nearest lattice point problem, *Combinatorica*, 1986, vol. 6, pp. 1-13. DOI: 10.1007/BF02579403

36. Micciancio D. The shortest vector problem is NP-hard to approximate to within some constant, *SIAM Journal on Computing*, 2001, no. 30, pp. 2008-2035. DOI: 10.1137/S0097539700373039

37. Usatyuk V.S. Veroyatnostnyi metod opredeleniya kodovogo rasstoyaniya lineinogo blochnogo koda, Proceedings of the III International conference *"Engineering&Telecommunication - En&T 2016"*, Moscow, MIPT, 2016, pp. 43-46.

38. Kuz'min O.V., Usatyuk V.S. *Programmnye produkty i sistemy*, 2015, no. 1 (109), pp. 55-62.

39. Usatyuk V.S. *Prikladnaya diskretnaya matematika. Prilozhenie*, 2012, no. 5, pp. 120-122.

40. Usatyuk V.S., Egorov S.I. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie*. 2017, no. 4 (25), pp. 24-33.

41. Bosma W., Cannon J.J., Fieker C., Steel A. *Handbook of Magma functions*, 2019, 6129 p.

42. Hernando F., Igual F. D., Quintana-Orti G. Algorithm 994: Fast Implementations of the Brouwer-Zimmermann Algorithm for the Computation of the Minimum Distance of a Random Linear Code, *ACM Transactions on Mathematical Software*, 2019, vol. 45, no. 2, pp. 1-28. DOI: 10.1145/3302389

43. *Support material for Low weight codewords problem search method*. URL: https://github.com/Lcrypto/Low-weight_Codeword_Problem V2.22-3

Статья поступила в редакцию 01.07.2024
Одобрена после рецензирования 14.07.2024
Принята к публикации 25.10.2024
The article was submitted on 01.07.2024; approved after reviewing on 14.07.2024; accepted for publication on 25.10.2024