Симметрическо-групповая закономерность в распределении значений минимумов положительных квадратичных форм, приведенных по Коркину-Золотарёву

М.А. Лялин

***Аннотация* — Создание криптографических систем, основанных на теории решеток является перспективным направлением в области постквантовой криптографии. Целью настоящей работы является получение новых свойств решёток и связанных с ними объектов. В результате выявлена закономерность в распределении значений минимумов положительных квадратичных форм, приведенных по Коркину-Золотарёву. Установлено их соответствие высотам фундаментальных параллелепипедов n-мерных решеток. Полученный результат имеет практическое значение при построении плотных решетчатых упаковок шаров, при решении задач теории решеток, исследованиях постоянной Эрмита. Результат целесообразно учитывать при создании новых криптографических систем, основанных на теории решеток.**

***Ключевые слова* — Постквантовая криптография, теория решеток, положительные квадратичные формы, приведение по Коркину-Золотареву, решетчатые упаковки шаров, задачи теории решеток, постоянная Эрмита.**

I. Введение

Криптографическое сообщество, не полагаясь на большое число физических проблем по разработке квантовых вычислительных систем, заранее озаботилось задачей борьбы с будущими квантовыми компьютерами и создало направление – постквантовая криптография [1]. Это направление разрабатывает криптографические системы, которые окажутся трудными для будущих квантовых компьютеров.

В настоящее время выделяют четыре основных направления исследований в постквантовой криптографии:

криптография, основанная на кодах, исправляющих ошибки [2];

криптография, основанная на многочленах в конечных полях [3];

криптография, основанная на решетках [4];

криптография, основанная на представлении хэш функций для больших данных [5].

[1] Статья получена 07.03.2024

Статья подготовлена в рамках диссертационной работы соискателя ученой степени кандидата физико-математических наук по научной специальности 1.2.2 Математическое моделирование, численные методы и комплексы программ.

М.А. Лялин, Балтийский федеральный университет имени И. Канта, г. Калининград, РФ (e-mail: maxi2704@yandex.ru).

В настоящей статье авторы представляют аналитическое исследование полученных ранее результатов из теории положительных квадратичных форм, теории решеток, геометрической теории чисел, которые имеют практическое значение при анализе существующих криптосистем, основанных на решетках, а также при создании и улучшении существующих. Полученный результат представляет интерес при решении таких задач теории решеток, как поиск кратчайшего вектора и задач решетчатых упаковок шаров в R^n.

Первая теория приведения для положительных квадратичных форм двух переменных была построена Лагранжем [6].

Дирихле сформулировал проблему поиска кратчайшего ненулевого вектора решетки в форме проблемы о совместных диофантовых приближениях. Теорема Дирихле является верхней оценкой кратчайшего вектора в частном классе решеток, заданных на R^n [7].

Минковским опубликована теорема о выпуклом теле, симметричном относительно начала координат, также являющаяся оценкой длины кратчайшего ненулевого вектора (по отношению к норме, заданной выпуклым телом) [8].

Вороной опубликовал метод приведения по совершенным формам, разбиения пространства на основе «диаграмм Вороного», положенных в основу детерминированного алгоритма решения задач поиска кратчайшего и ближайшего векторов [9].

Боас доказал NP-сложность для алгоритмов решения задачи поиска кратчайшего вектора в решетке (Shortest Vector Problem) и задачи нахождения ближайшего вектора в решетке (Closest Vector Problem) для равномерных норм [10].

Ленстра, Ленстра и Ловас предложили полиномиальный по времени выполнения алгоритм редукции базиса LLL, который находит вектора в произвольной решетке, чья длина не превосходит $2^{(n-1)/2}sh(L)$ [11].

Айтай опубликовал результаты своей работы о трудности задачи поиска короткого вектора в решетке. Ему удалось доказать, что можно построить такую случайную решетку с коротким вектором в ней, что любой алгоритм нахождения этого вектора в данной

случайной решетке можно конвертировать в эффективный алгоритм нахождения достаточно короткого вектора в любой решетке [12].

Миссиансио и Реджев показали, что криптография на основе решеток криптоустойчива к квантовым компьютерам. Их работа в большей степени посвящена описанию практических аспектов криптографии на основе решеток и в меньшей степени описанию способов ее защищенности [4].

Впервые, алгоритмы решения задачи приведения положительных квадратичных форм (ПКФ) от n-переменных, были опубликованы в совместных работах Коркина и Золотарёва о минимумах положительных квадратичных форм, в которых они рассматривали все возможные положительные квадратичные формы с целочисленными коэффициентами [13-17]: $f = a_{11}{x_1}^2 + a_{22}{x_2}^2 + \cdots + a_{nn}{x_n}^2 + a_{12}x_1x_2 + a_{21}x_2x_1 + \cdots + a_{n-1,n}x_{n-1}x_n + a_{n,n-1}x_nx_{n-1} = \sum a_{ik}x_ix_k$

с данным определителем:

$$D = \begin{vmatrix} a_{11} & a_{12} \dots & a_{1n} \\ a_{21} & a_{22} \dots & a_{2n} \\ a_{n1} & a_{n2} \dots & a_{nn} \end{vmatrix}$$

и любыми вещественными коэффициентами: $a_{ik} = a_{ki}$.

В силу эквивалентности ПКФ решеткам, результат автоматически применим и для них.

Решетка Г – класс эквивалентности {f} ПКФ;

ПКФ из класса {f} – основной базис решетки Г;

квадратичная форма – точка евклидова пространства E^N, где $N = n(n+1)/2$.

Благодаря этим соответствиям всякий факт геометрии ПКФ может быть рассмотрен в зависимости от удобства его исследования:

либо как геометрический факт пространства E^n с заданной в нем решеткой;

либо аналитически, как некоторое свойство на множестве ПКФ;

либо как геометрический факт в пространстве E^N [18].

Задача о плотнейшей возможной упаковке равных шаров в евклидовом пространстве – часть восемнадцатой проблемы Гильберта. Ограничив рассмотрение и потребовав, чтобы центры шаров образовывали аддитивную подгруппу (решетку) – приходим к классической задаче теории чисел о минимумах унимодулярных квадратичных форм и об их классификации [19].

II. Обозначения и основные сведения

Пусть задана n-мерная решетка $\Gamma \in E^n$ и множество n-мерных шаров одного и того же радиуса с центрами в точках решетки, причем эти шары образуют упаковку, т.е. попарно не имеют общих внутренних точек. Максимальный радиус шаров такой упаковки назовем радиусом упаковки, соответствующей решетке Г, и обозначим r(Г).

$$r(\Gamma) = \frac{1}{2}\min \Gamma,$$

где $\min \Gamma$ – длина минимального вектора решетки.

Плотностью решетчатой упаковки, т.е. упаковки шаров радиуса r(Г) с центрами в точках решетки Г, назовем величину

$$d(\Gamma) = \Omega_n \frac{r^n(\Gamma)}{V(\Gamma)},$$

где V(Г) – объем основного параллелепипеда решетки Г, а Ω_n - объем n-мерного единичного шара. Задача о плотнейших решетчатых упаковках в пространстве E^n состоит в том, чтобы на множестве n-мерных решеток найти значение $d_n = \sup d(\Gamma)$ и те решетки, на которых они достигаются. Поскольку плотность d(Г) не меняется при преобразованиях подобия пространства E^n , то при решении задачи о плотнейших решетчатых упаковках исследуемое множество решеток можно нормировать, потребовав, например, V(Г) = 1 или r(Г) = 1.

Пусть $\{f\}$ - класс эквивалентности ПКФ, соответствующий решетке Г, и $f \in \{f\}$ – некоторый представитель этого класса. Тогда, имеем:

$$d(\Gamma) = \frac{\Omega_n}{2^n}\left[\min f/(\det f)^{1/n}\right]^{n/2}$$

Задача о плотнейшей решетчатой упаковке в пространстве E^n, эквивалентна задаче об отыскании верхней грани отношения $\min f/(\det f)^{1/n}$ на множестве ПКФ от n переменных: $\gamma_n = \sup[\min f/(\det f)^{1/n}] = \sup[(\min \Gamma_f)^2/(V(\Gamma_f))^{2/n}]$

Величина γ_n называется постоянной Эрмита. Постоянная γ_n и плотность плотнейшей решетчатой упаковки связаны формулой:

$$d_n = 2^{-n}\,\Omega_n\,\gamma^{n/2}$$

При отыскании постоянной Эрмита можно рассматривать не все множество ПКФ от n переменных, а взять по одному представителю от каждого класса эквивалентности и пронормировать его, положив $\min f = 1$ или $det\, f = 1$.

Теория приведения ПКФ произвольного числа переменных была изложена во втором мемуаре Коркина и Золотарева [14] и там же использована как метод получения значений и оценок постоянной Эрмита, а тем самым и решения задачи о плотнейших упаковках.

Рассмотрим разложение по Лагранжу для произвольной ПКФ:

$$f = A_1(x_1 - \sum_{k=2}^{n} a_{1k}x_k)^2 + A_2(x_2 - \sum_{k=3}^{n} a_{2k}x_k)^2 + \cdots + A_l(x_l - \sum_{k=l+1}^{n} a_{lk}x_k)^2 + \cdots + A_n\left(x_{n-1} - a_{n-1,n}x_n\right)^2 + A_n x_n^2$$

ПКФ называется приведенной по Коркину – Золотарёву, если в ее разложении при $l = 1,\ 2,\ \dots,\ n-1$ и $q = l+1,\ l+2,\ \dots,\ n$ коэффициенты A_l суть соответственно значения минимумов форм:

$$\phi_1 = f(x_1, x_2, \dots, x_n), \phi_{l+1}(x_{l+1}, x_{l+2}, \dots, x_n) = \phi_l(x_l, x_{l+1}, \dots, x_n) - A_l(x_l - \sum_{k=l+1}^{n} a_{lk}x_k)^2$$

Для каждого разложения по Коркину – Золотарёву справедливо равенство $\det f = A_1A_2 \dots A_n$ (1) и «Первое неравенство Коркина – Золотарёва»:

$$A_{k+1} \geq \frac{3}{4} A_k$$

«Второе неравенство Коркина – Золотарёва»:

$$A_{i+1} \geq \frac{2}{3} A_i$$

Согласно определению постоянной Эрмита γ_n и равенству (1), представляя каждый класс эквивалентности ПКФ разложением по Коркину – Золотарёву, имеем:

$$\gamma_n = \sup A_1(A_1A_2 \dots A_n)^{-1/n} \quad (2)$$

Оценка постоянной Эрмита γ_n :

$$\gamma_n \leq (4/3)^{(n-1)/2}$$

Имеют место следующие равенства для значений постоянной Эрмита и плотностей плотнейших решетчатых упаковок (таблица I) [6, 16, 20, 21]:

Таблица I.

		Лагранж	Гаусс	Коркин - Золотарёв		Блихфельдт			Кох-Кумар
Размерность, n	1	2	3	4	5	6	7	8	24
Значение постоянной Эрмита, γ_n	1	$\frac{2}{\sqrt{3}}$	$\sqrt[3]{2}$	$\sqrt{2}$	$\sqrt[5]{8}$	$\sqrt[6]{64/3}$	$\sqrt[7]{64}$	2	4
Плотность плотнейшей решетчатой упаковки, d_n	1	$\frac{\pi}{2\sqrt{3}}$	$\frac{\pi}{3\sqrt{2}}$	$\frac{\pi^2}{16}$	$\frac{\pi^2}{15\sqrt{2}}$	$\frac{\pi^3}{48\sqrt{3}}$	$\frac{\pi^3}{105}$	$\frac{\pi^4}{384}$	$\frac{\pi^{12}}{12!}$

Блихфельдт в работах, опубликованных в 1925-1935 годах вычислил значения постоянной Эрмита при n=6,7,8 и указал среди предельных форм, найденных Коркиным и Золотарёвым, те, на которых эти значения достигаются, т.е. решил задачу о плотнейших решетчатых упаковках в пространствах E^6, E^7, E^8. Все вычисления и доказательства Блихфельдта базируются только на неравенствах разложений Коркина – Золотарёва форм данного числа измерений, без привлечения каких-либо дополнительных понятий [20].

III. Основные результаты

Из равенства (2), получены значения коэффициентов A_n (таблица II):

Таблица II.

Размерность, n	1	2	3	4	5	6	7	8
Значение постоянной Эрмита, γ_n	1	$\frac{2}{\sqrt{3}}$	$\sqrt[3]{2}$	$\sqrt{2}$	$\sqrt[5]{8}$	$\sqrt[6]{64/3}$	$\sqrt[7]{64}$	2
Значение коэффициентов, A_n	1	3/4	2/3	1/2	1/2	3/8	1/3	1/4

Из формул $d(\Gamma) = \Omega_n \frac{r^n(\Gamma)}{V(\Gamma)}$ и $d_n = 2^{-n}\,\Omega_n\,\gamma^{n/2}$, при r(Γ) = 1, получены значения V(Γ).

По формуле объема параллелепипеда $V_n = V_{n-1}h_n$, получены значения высот, h_n (таблица III).

Таким образом, в размерностях 1 – 8 наблюдается возможность построения плотнейшей упаковки размерности n из плотнейшей решетчатой упаковки размерности n-1 путем определения нового значения высоты и построения фундаментального параллелепипеда в старшей размерности с минимальным объемом.

Таблица III.

Размерность, n	1	2	3	4	5	6	7	8
Объем фундаментального параллелепипеда решетки, V(Γ)	2	$2\sqrt{3}$	$4\sqrt{2}$	8	$8\sqrt{2}$	$8\sqrt{3}$	16	16
Значения высот фундаментальных параллелепипедов, h_n	2	$\sqrt{3}$	$2\sqrt{2/3}$	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{3/2}$	$\frac{2}{\sqrt{3}}$	1

Соответствие значений высот фундаментального параллелепипеда решетки Γ значениям коэффициентов A_n ПКФ, приведенных по Коркину – Золотарёву представлено в таблице IV. При выборе минимальной

нормы решётки $\mu_n = 4$, т.е. $\min \Gamma = 2$, имеет место следующее равенство: $h_n = 2\sqrt{A_n}$ (3).

Таблица IV.

Размерность, n	1	2	3	4	5	6	7	8
Значение коэффициентов A_n	1	3/4	2/3	1/2	1/2	3/8	1/3	1/4
Значения высот фундаментальных параллелепипедов, h_n	2	$\sqrt{3}$	$2\sqrt{2/3}$	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{3/2}$	$\frac{2}{\sqrt{3}}$	1

Для размерностей 1 – 8, имеют место следующие равенства:

$$h_1 h_8 = h_2 h_7 = h_3 h_6 = h_4 h_5 = 2$$
$$A_1 A_8 = A_2 A_7 = A_3 A_6 = A_4 A_5 = \tfrac{1}{4}$$

Используя известные значения центральных плотностей решетчатых упаковок (таблица V) [22], получаем равенства для размерностей 9 – 24.

Таблица V.

Размерность	Центральная плотность	Решетка
9	0.04419	LAMBDA9
10	0.03608	LAMBDA10
11	0.03208	KAPPA11
12	0.03704	KAPPA12 = K12
13	0.03208	KAPPA13
14	0.03608	LAMBDA14
15	0.04419	LAMBDA15
16	0.06250	LAMBDA16
17	0.06250	LAMBDA17
18	0.07217	LAMBDA18
19	0.08839	LAMBDA19
20	0.12500	LAMBDA20
21	0.17678	LAMBDA21
22	0.28868	LAMBDA22
23	0.50000	LAMBDA23
24	1	LAMBDA24

Для размерностей 9 – 16, имеют место следующие равенства:

$$h_9 h_{16} = h_{10} h_{15} = h_{11} h_{14} = h_{12} h_{13} = 1$$
$$A_9 A_{16} = A_{10} A_{15} = A_{11} A_{14} = A_{12} A_{13} = \frac{1}{16}$$

Для размерностей 17 – 24, имеют место следующие равенства:

$$h_{17} h_{24} = h_{18} h_{23} = h_{19} h_{22} = h_{20} h_{21} = \frac{1}{2}$$
$$A_{17} A_{24} = A_{18} A_{23} = A_{19} A_{22} = A_{20} A_{21} = \frac{1}{64}$$

IV. Заключение

Установлено соответствие значений минимумов ПКФ значениям высот фундаментальных параллелепипедов плотнейших решетчатых упаковок.

В размерностях 1 – 24 установлены симметрии в распределении значений минимумов положительных квадратичных форм, приведенных по Коркину-Золотарёву и значений высот фундаментальных параллелепипедов решеток Г, распределенные по группам размерностей 1 – 8, 9 – 16, 17 – 24.

Полученный результат имеет практическое значение при построении плотных решетчатых упаковок шаров, при решении задач теории решеток, исследований постоянной Эрмита, а также может использоваться для улучшения алгоритмов поиска коротких векторов в решетках. Результат целесообразно учитывать при анализе существующих и создании новых криптографических систем, основанных на теории решеток.

При построении новых решетчатых упаковок шаров, имеющих бóльшую плотность, чем известные упаковки, необходимо проверять отсутствие векторов, короче удвоенного радиуса упаковки на большом количестве точек решетки.

Стоит также отметить, что в размерностях 1 – 24, получены результаты, в которых наблюдается симметрия значений объемов фундаментальных параллелепипедов с разницей в том, что симметрия распространяется на всю группу размерностей 1 – 24.

Благодарности

М.А. Лялин выражает благодарность научному руководителю А.В. Шокурову (Институт системного программирования им. В.П. Иванникова Российской академии наук, г. Москва, РФ) за ценные замечания при подготовке статьи, а также М.А. Цфасману (Институт проблем передачи информации им. А.А. Харкевича Российской академии наук, г. Москва, РФ) за проявленный интерес и обсуждение работы.

Библиография

[1] Bernstein D.J., Buchmann J., Dahmen E., «Introduction to post-quantum cryptography» Post-Quantum Cryptography, pp. 1-14, 2009.

[2] Berlekamp, Elwyn R., Robert J. McEliece, Henk C. A. van Tilborg, «On the inherent intractability of certain coding problems» IEEE Transactions on Information Theory, № 24 (3), p. 384–386, 1978.

[3] Ding, Jintai & Schmidt, Dieter, «Multivariable public-key cryptosystems» IACR Cryptology ePrint Archive, p. 350, 2004.

[4] Micciancio D. Regev O., «Lattice-based Cryptography» Post-Quantum Cryptography, 2009.

[5] Buchmann J., Dahmen E., Szydlo M., «Hash-based digital signature schemes» Post-quantum cryptography, pp. 35-93, 2009.

[6] Lagrange J.L., «Arithmetic research» Nouveaux Memoires de l'Academie royal des Sciences et Belles-Lettres de Berlin, pp. 265-312, 1773.

[7] Dirichlet L.G.P., «Generalization of a theorem from the doctrine of continued fractions» S. B. Preuss. Akad. Wiss., pp. 93-95, 1842.

[8] Minkovski H., «Geometry of numbers», Teubner, 1896.

[9] Вороной Г. Ф., «Собр. соч., том 2,» 1952.

[10] Boas P. van E., «Another NP-complete problem and the complexity of computing short vectors in a lattice» Technical Report 81-04, 1981.

[11] Lenstra A.K. Lenstra H.W. Lovász L., «Factoring polynomials with rational coefficients» № 261, pp. 515-534, 1982.

[12] Ajtai M., «Generating Hard Instances of Lattice Problem» Proc. of 28th ACM Symp. on Theory of Comp, pp. 99-108, 1996.

[13] Korkin A. Zolotaryov E., «On quaternary positive quadratic forms» № 5, pp. 581-583, 1872.

[14] Korkin A. Zolotaryov E., «Quadratic shapes» № 6, p. 366-389, 1873.

[15] Korkin A. Zolotaryov E., «On positive quadratic forms» № 11, p. 242-292, 1877.

[16] Золотарёв Е.И., Полное собр. соч., вып. 1, Изд-во АН, 1931.

[17] Делоне Б.Н., Петербургская школа теории чисел, Ленинград: Изд-во АН СССР, 1947.

[18] Ryshkov S.S. Baranovskii E.P., «Classical metthods in the theory of lattice packings» т. 34, № 4, pp. 1-68, 1979.

[19] Конвэй Д. Слоэн Н., Упаковки шаров, решетки и группы, пер. с англ. - М., т. 1, Москва: Мир, 1990.

[20] Blichfeldt H.F., The minimum values of positive quadratic formes in six, seven and eight variables, Math. Z. 39, 1934-1935, pp. 1-15.

[21] Cohn H. and Kumar A., «The densest lattice in twenty-four dimensions» pp. 58-67, 2004.

[22] Gabriele N. Sloane N.J.A., «Table of Densest Packings Presently Known» Available: https://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/density.html.

Symmetric-group Regularity in the Distribution of Minima of Positive Quadratic Forms Reduced By Korkin-Zolotarev

M.A. Lyalin

***Abstract* — Creation of cryptographic systems based on lattice theory is a promising direction of postquantum cryptography. The purpose of this work is to obtain new properties of lattices and related objects. As a result, a regularity in the distribution of the minima of positive quadratic forms, reduced by Korkin-Zolotaryov, was revealed. Their correspondence to the heights of fundamental parallelepipeds of n-dimensional lattices has been established. The obtained result is of practical importance in the construction of dense lattice packs of balls, in solving problems of the lattice theory, researching of Hermit's constant. The result should be taken into account when creating new cryptographic systems based on lattice theory.**

***Keywords* — Postquantum cryptography, lattice (group), positive quadratic forms, Korkin-Zolotarev reduction, lattice packing of balls, lattice problems, Hermit's constant.**

REFERENCES

[1] Bernstein D.J., Buchmann J., Dahmen E., «Introduction to post-quantum cryptography» Post-Quantum Cryptography, pp. 1-14, 2009.
[2] Berlekamp, Elwyn R., Robert J. McEliece, Henk C. A. van Tilborg, «On the inherent intractability of certain coding problems» IEEE Transactions on Information Theory, № 24 (3), p. 384–386, 1978.
[3] Ding, Jintai & Schmidt, Dieter, «Multivariable public-key cryptosystems» IACR Cryptology ePrint Archive, p. 350, 2004.
[4] Micciancio D. Regev O., «Lattice-based Cryptography» Post-Quantum Cryptography, 2009.
[5] D. E. S. M. Buchmann J., «Hash-based digital signature schemes» Post-quantum cryptography, pp. 35-93, 2009.
[6] Lagrange J.L., «Arithmetic research» Nouveaux Memoires de l'Academie royal des Sciences et Belles-Lettres de Berlin, pp. 265-312, 1773.
[7] Dirichlet L.G.P., «Generalization of a theorem from the doctrine of continued fractions» S. B. Preuss. Akad. Wiss., pp. 93-95, 1842.
[8] Minkovski H., «Geometry of numbers», Teubner, 1896.
[9] Voronoi G.F., «Collected Works, vol. 2» 1952.
[10] Boas P. van E., «Another NP-complete problem and the complexity of computing short vectors in a lattice» Technical Report 81-04, 1981.
[11] Lenstra A.K. Lenstra H.W. Lovász L., «Factoring polynomials with rational coefficients» № 261, pp. 515-534, 1982.
[12] Ajtai M., «Generating Hard Instances of Lattice Problem» Proc. of 28th ACM Symp. on Theory of Comp, pp. 99-108, 1996.
[13] Korkin A. Zolotaryov E., «On quaternary positive quadratic forms» № 5, pp. 581-583, 1872.
[14] Korkin A. Zolotaryov E., «Quadratic shapes» № 6, p. 366-389, 1873.
[15] Korkin A. Zolotaryov E., «On positive quadratic forms» № 11, p. 242-292, 1877.
[16] Zolotaryov E.I., Complete Collected Works, vol. 1, Academy of Sciences, 1931.
[17] Delaunay B.N., Petersburg School of Number Theory, Leningrad: Academy of Sciences USSR, 1947.
[18] Ryshkov S.S. Baranovskii E.P., «Classical metthods in the theory of lattice packings» т. 34, № 4, pp. 1-68, 1979.
[19] Conway, D., Sloan, N., Packings of balls, lattices and groups, per. from Engl. - M., vol. 1, Moscow: Mir, 1990.
[20] Blichfeldt H.F., The minimum values of positive quadratic formes in six, seven and eight variables, Math. Z. 39, 1934-1935, pp. 1-15.
[21] Cohn H. and Kumar A., «The densest lattice in twenty-four dimensions» pp. 58-67, 2004.
[22] Gabriele N. Sloane N.J.A., «Table of Densest Packings Presently Known» Available: https://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/density.html.