Algebraic codes are good

Patrick Solé (France, Saint-Denis)
University of Paris 8
e-mail: sole@enst.fr

We survey the algebraic structure [3], and asymptotic performance of the self-dual and LCD classes of quasi-cyclic [1], quasi-twisted [2], and dihedral codes over finite fields and finite rings. Of special interest is the case of low index: double circulant codes and four circulant codes [4]. We show that additive cyclic codes are good [5], and give an alternative proof that dihedral codes are good [1].

REFERENCES

1. Adel Alahmadi, Funda Özdemir, Patrick Solé, *On self-dual double circulant codes*. Des. Codes Cryptography **86(6):** (2018), 1257–1265 .

2. Adel Alahmadi, Cem Güneri, Buket Özkaya, Hatoon Shohaib, Patrick Solé, *On self-dual double negacirculant codes*, Discrete Applied Mathematics, **222:** (2017),205–212 .

3. Cem Güneri, Funda Özdemir, Patrick Solé, *On the additive cyclic structure of quasi-cyclic codes*. Discrete Mathematics **341(10):**,(2018), 2735–2741 .

4. Minjia Shi, Hongwei Zhu, Liqin Qian, Patrick Solé, *On Self-Dual Four Circulant Codes*, Int. J. Found. Comput. Sci. **29(7):**, (2018), 1143–1150.

5. Minjia Shi, Rongsheng Wu, Patrick Solé, *Asymptotically Good Additive Cyclic Codes Exist*, IEEE Communications Letters **22(10):** (2018), 1980–1983 .

УДК 511.3

К программе И. М. Виноградова[1]

В. Н. Чубариков (Россия, г. Москва)
МГУ имени М. В. Ломоносова
e-mail: chubarik2009@live.ru

To the program of I. M. Vinogradov

V. N. Chubarikov (Russia, Moscow)
Lomonosov Moscow State University
e-mail: chubarik2009@live.ru

Введение

Настоящую работу автор посвящает светлой памяти профессора Механико-математического факультета Московского университета Геннадия Ивановича Архипова (12.12.1945 – 14.03.2013). Он внёс существенный и принципиальный вклад в развитие программы И. М. Виноградова в 1971 г.

[1]Работа выполнена при финансовой поддержке МГУ имени М. В. Ломоносова, грант ведущих научных школ

Сначала приведем список важнейших научных результатов И. М. Виноградова.

$$\left|\sum_{n\le x}\left(\frac{n}{p}\right)\right| < \sqrt{p}\ln p$$

$$n_p < p^{1/(2\sqrt{e})}\ln^2 p$$

$$p_1+p_2+p_3 = 2N+1$$

$$n < G(n) < 2n(\ln n + O(1))$$

$$\{f(p)\}$$

$$p_1^n + \cdots + p_k^n = N$$

$$\pi(x) = \mathrm{li}(x) + O\left(xe^{-(\ln x)^{0.6}(\ln\ln x)^{-0.2}}\right)$$

§1. Программа И. М. Виноградова

В своей монографии "Метод тригонометрических сумм в теории чисел" (Труды Матем. ин-та им. В. А. Стеклова АН СССР, 1947, т.23) И. М. Виноградов писал, что "одною из важнейших для теории чисел проблем является установление различного рода закономерностей в распределении значений функции $f(x_1,\ldots,x_r)$ от одной или более переменных. При этом рассматриваются лишь те значения функции, которые отвечают целым точкам $(x_1,\ldots,x_r)$ r-мерного пространства, принадлежащим заданной совокупности Ω." Для решения этой проблемы он сформулировал программу исследований, которая включает в себя "три достаточно достаточно большие и весьма важные для теории чисел проблемы".

§2. Проблема 1 И. М. Виноградова

Проблема распределения значений показательной функции

$$f(x_1,\ldots,x_r) = e^{2\pi i F(x_1,\ldots,x_r)},$$

где $F(x_1,\ldots,x_r)$ — вещественная функция.

Наиболее существенным здесь является установление верхней границы модуля суммы

$$S = \sum_{\Omega} e^{2\pi i F(x_1,\ldots,x_r)}.$$

Детальному изучению эти суммы подверглись в случае, когда Ω представляет собой параллелепипед $Q_s \le x < Q_s + P_s, s = 1,2,\ldots,r$, а $F(x_1,\ldots,x_r)$ — многочлен вида

$$F(x_1,\ldots,x_r) = \sum_{t_1=0}^{n_1}\cdots\sum_{t_r=0}^{n_r}\alpha(t_1,\ldots,t_r)x_1^{t_1}\ldots x_r^{t_r},$$

где $\alpha(t_1,\ldots,t_r)\in\mathbf{R}$.

Полные рациональные тригонометрические суммы вида

$$\sum_{x_1=0}^{q-1}\cdots\sum_{x_r=0}^{q-1} e^{2\pi i\frac{\Phi(x_1,\ldots,x_r)}{q}},$$

где

$$\Phi(x_1,\dots,x_r)=\sum_{t_1=0}^{n}\cdots\sum_{t_r=0}^{n}a(t_1,\dots,t_r)x_1^{t_1}\dots x_r^{t_r},a(t_1,\dots,t_r)\in\mathbf{Z}$$

являются наиболее изученными.

К. Ф. Гаусс нашёл величину суммы вида

$$\sum_{x=0}^{q-1}e^{2\pi i\frac{x^2}{q}}=\frac{1+i^{-q}}{1+i^{-1}}\sqrt{q}$$

(сумма Гаусса).

Л. Морделл для простого q, а Л.-К. Хуа для общего случая при $(a_n,\dots,a_1,q)=1$ получили оценку вида

$$S=\sum_{x=0}^{q-1}e^{2\pi i\frac{\Phi(x)}{q}}\ll q^{1-\nu},\nu=\frac{1}{n},$$

где постоянная в знаке $\ll$ зависит только от n.

Для кратных полных рациональных тригонометрических сумм докладчик нашёл оценку

$$\sum_{x_1=0}^{q-1}\cdots\sum_{x_r=0}^{q-1}e^{2\pi i\frac{\Phi(x_1,\dots,x_r)}{q}}\ll q^{r-\nu}(\ln q)^{r-1},$$

где постоянная в знаке $\ll$ зависит только от n,r.

Две последние оценки не могут быть существенно улучшены.

Более трудной задачей является оценка сумм Г. Вейля вида

$$S=\sum_{x=Q}^{Q+P-1}e^{2\pi iF(x)},F(x)=\sum_{m=1}^{n}\alpha_m x^m,\alpha_m\in\mathbf{R},P>1.$$

Оценки таких сумм зависят от приближения коэффициентов многочлена $F(x)$ рациональными дробями. В 1934 г. И. М. Виноградов разработал мощный метод оценок сумм Г. Вейля.

Все точки $(\alpha_n,\dots,\alpha_2,\alpha_1)$ единичного куба $E:0\leq\alpha_m<1,m=1,\dots,n$, разбиваются на два класса. К первому классу относятся окрестности точек с “малыми знаменателями”, все остальные точки куба E принадлежат второму классу. Для точек первого класса сумма Г. Вейля асимптотически с большой точностью приближается произведением полной рациональной тригонометрической суммы и тригонометрического интеграла. Для точек второго класса справедлива единообразна оценка

$$S\ll P^{1-\rho},\rho=\frac{\gamma}{n^2\ln n},$$

где $\gamma>0$ — абсолютная постоянная, а константы в знаке $\ll$ зависят только от n.

Удачные варианты метода И. М. Виноградова оценок сумм Г. Вейля были даны ван дер Корпутом (1936 г.), Ю. В. Линником (1942 г.), А. А. Карацубой (1963 г.). В основе оценок сумм лежит теорема И. М. Виноградова о среднем.

Теоремы о среднем для сумм произвольной кратности впервые были доказаны Г. И. Архиповым (1971 г.) (дальнейшее развитие: Г. И. Архипов, А. А. Карацуба и автор.)

Теорема *Пусть $\tau\geqslant 0$ — целое число и $n_1,\dots,n_r$ — натуральные числа. Тогда для $k\geqslant m\tau$ интеграл $J=J(\bar{P};k,\bar{n})$ удовлетворяет неравенству*

$$J=J(\bar{P};k,\bar{n})\leqslant k^{2m\tau}\kappa^{4\kappa^2\Delta(\tau)}2^{8m\kappa\tau}(P_1\dots P_r)^{2k}P^{-\kappa\Delta(\tau)},$$

где $\kappa = n_1\nu_1 + \cdots + n_r\nu_r$, $\gamma\kappa = 1$, $m = (n_1+1)\dots(n_r+1)$,

$$\Delta(\tau) = 0.5m(1-(1-\gamma)^\tau), \quad P = (P_1^{n_1}\dots P_r^{n_r})^\gamma.$$

Здесь $\nu_1, \dots, \nu_r$ *— натуральные числа такие, что*

$$-1 < \frac{\log P_s}{\log P_1} - \nu_s \leqslant 0,\ s = 1, \dots, r.$$

Отсюда следуют оценки кратных сумм Г. Вейля, подобные оценкам И. М. Виноградова.

Важным и интересным случаем проблемы 1 И. М. Виноградова являются суммы по простым числам с многочленом в экспоненте вида

$$\sum_{p \leq N} e^{2\pi i F(p)},$$

где p пробегает последовательность всех простых чисел.

Нетривиальные оценки таких сумм впервые были получены И. М. Виноградовым; по силе они такие же, как и по сплошному промежутку. Докладчик получил подобные оценки для сумм произвольной кратности

$$\sum_{p_1 \leq N_1} \cdots \sum_{p_r \leq N_r} e^{2\pi i F(p_1,\dots,p_r)},$$

где $p_1, \dots, p_r$ пробегают простые числа.

§3. Проблема 2 И. М. Виноградова

В этой проблеме изучается распределение значений дробной части $\{F(x_1, \dots, x_r)\}$ вещественной функции $F(x_1, \dots, x_r)$, ког да точки $(x_1, \dots, x_r)$ принадлежат конечному множеству Ω. Сначала рассматривается задача о точности приближения $\Delta = \Delta(F; \Omega; \alpha)$ функцией $\{F(x_1, \dots, x_r)\}$ к числу α, т.е. вывод неравенства

$$|\{F(x_1, \dots, x_r)\} - \alpha| \leq \Delta.$$

Часто можно установить равномерность распределения на промежутке $[0, 1)$ значений дробной части функции $\{F(x_1, \dots, x_r)\}$ на множестве Ω. Г. Вейль доказал, что для многочлена $F(x) = \alpha_n x^n + \cdots + \alpha_1 x$, у которого хотя бы один из коэффициентов иррационален, для любых $0 \leq \alpha < \beta \leq 1$ количество $N_P(\alpha, \beta)$ значений дробных частей $\{F(x)\}$, попадающих на промежуток $[\alpha\beta)$, удовлетворяет предельному соотношению

$$\lim_{P \to +\infty} \frac{N_P(\alpha, \beta)}{P} = \beta - \alpha.$$

Особый интерес представляет задача о равномерном распределении последовательности дробных частей значений многочлена $\{F(p)\}$, где p пробегает последовательность простых чисел, и хотя бы один из коэффициентов $F(x)$ является иррациональным числом. В этом случае $\{F(p)\}$ равномерно распределена по модулю единица.

И. М. Виноградов получил более точные результаты для отклонений от равномерного распределения, подобные оценкам тригонометрических сумм от многочленов с простыми числами.

Для дробных частей значений многочленов $\{F(p_1, \dots, p_r)\}$ подобные результаты получены докладчиком.

Распределение значений интересного класса очень коротких сумм Гаусса и их обобщений исследовали автор и его ученики.

§4. Проблема 3 И. М. Виноградова

Пусть $I(N)$ обозначает число решений диофантова уравнения вида

$$f(x_1,\dots,x_r)=N,$$

где функция $f(x_1,\dots,x_r)$ принимает целые значения для наборов $(x_1,\dots,x_r)$ из $\Omega\in\mathbf{R}$.

Здесь возникает несколько вопросов. Первый из них — о разрешимости уравнения, т.е. о справедливости неравенства $I(N)>0$; другой вопрос — об установлении асимптотической формулы для $I(N)$; иногда удаётся найти точную формулу для $I(N)$.

Г. Харди ввёл в рассмотрение символ $G(n)$, обозначающий целое число со следующими свойствами:

а) существует целое число $c>0$ такое, что $\forall N\ge c$ уравнение $x_1^n+\dots+x_r^n=N$ разрешимо для $r=G(n)$;

б) не существует $c_1>0$ такого, что $\forall N\ge c_1$ уравнение $x_1^n+\dots+x_r^n=N$ разрешимо при $r<G(n)$.

И. М. Виноградов (1958 г.) доказал, что

$$n+1\le G(n)\le 2n\ln n(1+o(1)).$$

Система диофантовых уравнений вида

$$\begin{cases} x_1+\dots+x_k &= N_1,\\ \dots\quad\dots &\dots\\ x_1^n+\dots+x_k^n &= N_n, \end{cases}$$

называется *системой Гильберта–Камке* (Г-К). Здесь $N_1,\dots,N_n$ — натуральные числа, и неизвестные $x_1,\dots,x_k$ принимают натуральные значения.

Г. И. Архипов (1980) нашёл необходимые арифметические условия разрешимости системы Г-К в следующем виде.

Система линейных уравнений

$$\begin{cases} t_1\cdot 1+\dots+t_n\cdot n &= N_1,\\ \dots\quad\dots &\dots\\ t_1\cdot 1^n+\dots+t_n\cdot n^n &= N_n, \end{cases}$$

имеет решение в целых числах $t_1,\dots,t_n$.

Далее будем рассматривать наборы натуральных чисел $\{N_1,\dots,N_n\}$, удовлетворяющие условиям

$$N_m=N_1^m(\gamma_m+O(N_1^{-\varepsilon})),$$

где $\gamma_1,\dots,\gamma_n$ — фиксированные положительные числа и $\varepsilon>0$ — сколь угодно малая постоянная.

Г. И. Архипов (1980) нашёл также необходимые условия вещественной разрешимости системы Г-К. Они имеют вид.

Пусть набор $\{N_1,\dots,N_n\}$ *принадлежит* $(\gamma_1,\dots,\gamma_n,\varepsilon)$*-конусу и пусть существует число* $P_0=P_0(\gamma_1,\dots,\gamma_n,\varepsilon)$ *такое, что для любого натурального* $N_1\ge P_0$ *система уравнений*

$$\begin{cases} x_1+\dots+x_k &= \gamma_1,\\ \dots\quad\dots &\dots\\ x_1^n+\dots+x_k^n &= \gamma_n, \end{cases}$$

имеет решение в вещественных числах $0\le x_1,\dots,x_k\le 1$ *и матрица Якоби вида*

$$\|rx_s^{r-1}\|\quad(1\le r\le n, 1\le s\le k)$$

решения $(x_1, \ldots, x_k)$ *имеет максимальный ранг.*

Система диофантовых уравнений Г-К разрешима тогда и только тогда, когда выполняются одновременно арифметические условия разрешимости и условия вещественной разрешимости. Пусть $G_1(n)$ обозначает наименьшее число переменных k, для которого эти необходимые и достаточные условия выполняются.

Г. И. Архипов (1980) доказал, что

$$2^n - 1 < G_1(n) \leq 3n^3 2^n - n.$$

Д. А. Митькин (1986) уточнил этот результат

$$G_1(n) \sim 2^n (n \to \infty).$$

Проблема Гильберта – Камке в простых числах была решена докладчиком (1984 г.).

Transformation and unimodality

Yaokun Wu (China, Shanghai)
Shanghai Jiao Tong University
e-mail: ykwu@sjtu.edu.cn

Abstract: Given a matroid lattice L of finite rank n and a semigroup acting on it, we call two elements of L of equal rank equivalent if each of them can be transformed to the other by the semigroup. We propose to look at the sequence $c_0, \ldots, c_n$, where c_i is the number of equivalence classes of rank i in L. Is this sequence unimodal? We analyze some examples related to this question. This is joint work with Yinfeng Zhu.
