Задача Чэпмена о “зловещем определителе”

Максим Всемирнов

Казанский федеральный университет
22 июня 2017

Символы Лежандра и определители

Строки и столбцы всех матриц нумеруются, начиная с 0.

Пусть p — нечетное простое. Рассмотрим матрицу $C(n,p) = (C_{ij})$ размера $n \times n$, где

$$C_{ij} = \left(\frac{j-i}{p}\right), \qquad 0 \le i,j \le n-1.$$

Символы Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv 0 \pmod p, \\ 1, & \text{если } a \equiv x^2 \pmod p \text{ разрешимо}, \\ -1, & \text{если } a \equiv x^2 \pmod p \text{ неразрешимо}. \end{cases}$$

Символы Лежандра и определители

Строки и столбцы всех матриц нумеруются, начиная с 0.

Пусть p — нечетное простое. Рассмотрим матрицу $C(n,p) = (C_{ij})$ размера $n \times n$, где

$$C_{ij} = \left(\frac{j-i}{p}\right), \qquad 0 \le i,j \le n-1.$$

Символы Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv 0 \pmod p, \\ 1, & \text{если } a \equiv x^2 \pmod p \text{ разрешимо}, \\ -1, & \text{если } a \equiv x^2 \pmod p \text{ неразрешимо}. \end{cases}$$

Далее рассматриваем случай $n = (p+1)/2$.

Пример матриц $C(n,p)$, $n=(p+1)/2$:

$$p=3,\ n=2 \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$p=5,\ n=3 \qquad \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}$$

$$p=7,\ n=4 \qquad \begin{pmatrix} 0 & 1 & 1 & -1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & 0 & 1 \\ 1 & -1 & -1 & 0 \end{pmatrix}$$

Гипотезы Чэпмена

В 2003–2004 годах Робин Чэпмен выдвинул несколько гипотез о поведении $\det C((p+1)/2, p)$.

Мотивировка:
эти и аналогичные определители возникли в связи с изучением некоторых унимодулярных решеток в $\mathbb{R}^n$, рассматриваемых как модули над квадратичными кольцами.

Гипотезы Чэпмена

В 2003–2004 годах Робин Чэпмен выдвинул несколько гипотез о поведении $\det C((p+1)/2, p)$.

Мотивировка:
эти и аналогичные определители возникли в связи с изучением некоторых унимодулярных решеток в $\mathbb{R}^n$, рассматриваемых как модули над квадратичными кольцами.

Ответ для аналогичных задач для матриц размера $p-1$ хорошо известен (вычисление гауссовых сумм). В этих случаях можно найти не только определитель, но и собственные числа.

Сложность задачи Чэпмена

Для матриц $C((p+1)/2, p)$ размера $(p+1)/2 \times (p+1)/2$, вопрос о нахождении собственных чисел, по-видимому, безнадежен.

Сложность задачи Чэпмена

Для матриц $C((p+1)/2, p)$ размера $(p+1)/2 \times (p+1)/2$, вопрос о нахождении собственных чисел, по-видимому, безнадежен.

$\chi_{C(10,19)}(t) = g(t^2)$,
$g(t) = t^5 + 45t^4 + 690t^3 + 4114t^2 + 7437t + 1$,
$\mathrm{Gal}(g) = \mathrm{Sym}(5)$.

$\chi_{C(12,23)}(t) = g(t^2)$,
$g(t) = t^6 + 66t^5 + 1583t^4 + 16476t^3 + 66479t^2 + 40322t + 1$,
$\mathrm{Gal}(g) = \mathrm{Sym}(6)$.

$\chi_{C(9,17)}(t) = g_1(t)g_2(t)$,
$g_1(t) = t^4 + 2t^3 - 16t^2 - 34t - 1$,
$g_2(t) = t^5 - 2t^4 - 16t^3 + 38t^2 - t - 4$,
$\mathrm{Gal}(g_2) = \mathrm{Sym}(5)$.

Характеристический многочлен

Открытый вопрос

Можно ли явно вычислить все коэффициенты характеристического многочлена матрицы $C((p+1)/2, p)$?

Характеристический многочлен

Открытый вопрос

Можно ли явно вычислить все коэффициенты характеристического многочлена матрицы $C((p+1)/2, p)$?

Открытый вопрос (А. Устинов)

Как распределены корни характеристического многочлена матрицы $C((p+1)/2, p)$?

Характеристический многочлен

Открытый вопрос

Можно ли явно вычислить все коэффициенты характеристического многочлена матрицы $C((p+1)/2, p)$?

Открытый вопрос (А. Устинов)

Как распределены корни характеристического многочлена матрицы $C((p+1)/2, p)$?

По-видимому,

$$\frac{|\lambda_{max}|}{\sqrt{p}} \to 1, \text{ при } p \to \infty.$$

Гипотеза Чэпмена: $p \equiv 3 \pmod 4$

Случай $p \equiv 3 \pmod 4$.

p	3	7	11	19	23	31	43	47	59	67	71	79	83
$\det C$	1	1	1	1	1	1	1	1	1	1	1	1	1

Гипотеза Чэпмена: $p \equiv 3 \pmod 4$

Случай $p \equiv 3 \pmod 4$.

p	3	7	11	19	23	31	43	47	59	67	71	79	83
$\det C$	1	1	1	1	1	1	1	1	1	1	1	1	1

Гипотеза (Чэпмен)

Если $p \equiv 3 \pmod 4$, то $\det C((p+1)/2, p) = 1$.

Чэпмен проверил ее для всех $p < 1000$.

Гипотеза Чэпмена: $p \equiv 3 \pmod 4$

Случай $p \equiv 3 \pmod 4$.

p	3	7	11	19	23	31	43	47	59	67	71	79	83
$\det C$	1	1	1	1	1	1	1	1	1	1	1	1	1

Гипотеза (Чэпмен)

Если $p \equiv 3 \pmod 4$, то $\det C((p+1)/2, p) = 1$.

Чэпмен проверил ее для всех $p < 1000$.

Доказана в: M.A.Vsemirnov. On the evaluation of R.Chapman's "evil determinant". Linear Algebra and its Applications, 436 (2012), no. 11, 4101–4106; doi:10.1016/j.laa.2011.08.039.

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Случай $p \equiv 1 \pmod 4$.

p	5	13	17	29	37	41	53	61
$\det C$	-2	-18	-4	-70	-882	-32	-182	-29718

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Случай $p \equiv 1 \pmod 4$.

p	5	13	17	29	37	41	53	61
$\det C$	-2	-18	-4	-70	-882	-32	-182	-29718

p	73	89	97	101	109	113
$\det C$	-1068	-500	-5604	-4030	-8890182	-776

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Случай $p \equiv 1 \pmod 4$.

p	5	13	17	29	37	41	53	61
$\det C$	-2	-18	-4	-70	-882	-32	-182	-29718

p	73	89	97	101	109	113
$\det C$	-1068	-500	-5604	-4030	-8890182	-776

p	137	...	229	...	257	...
$\det C$	-1744	...	-20000849130	...	-16432	...

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Случай $p \equiv 1 \pmod 4$.

p	5	13	17	29	37	41	53	61
$\det C$	-2	-18	-4	-70	-882	-32	-182	-29718

p	73	89	97	101	109	113
$\det C$	-1068	-500	-5604	-4030	-8890182	-776

p	137	...	229	...	257	...
$\det C$	-1744	...	-20000849130	...	-16432	...

Эта последовательность включена в On-line Encyclopedia of Integer Sequences (www.oeis.org) под номером A179073.

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

p	5	13	17	29	37	41	53	61
$\det C$	-2	-18	-4	-70	-882	-32	-182	-29718
$(\det C^2+1)/p$	1^2	5^2	1^2	13^2	145^2	5^2	25^2	3805^2

p	73	89	97	101	109	113
$\det C$	-1068	-500	-5604	-4030	-8890182	-776
$(\det C^2+1)/p$	125^2	53^2	569^2	401^2	851525^2	73^2

p	137	$\ldots$	229	$\ldots$	257	$\ldots$
$\det C$	-1744	$\ldots$	-20000849130	$\ldots$	-16432	$\ldots$
$(\det C^2+1)/p$	149^2	$\ldots$	1321693313^2	$\ldots$	1025^2	$\ldots$

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Пусть $\mathcal{O}$ — кольцо целых в $\mathbb{Q}(\sqrt{p})$, ε — фундаментальная единица в $\mathcal{O}$, а $h = h(p)$ — число классов.

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Пусть $\mathcal{O}$ — кольцо целых в $\mathbb{Q}(\sqrt{p})$, ε — фундаментальная единица в $\mathcal{O}$, а $h = h(p)$ — число классов.
Положим

$$a + b\sqrt{p} = \begin{cases} \varepsilon^h, & \text{если } p \equiv 1 \pmod 8, \\ \varepsilon^{3h}, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Пусть $\mathcal{O}$ — кольцо целых в $\mathbb{Q}(\sqrt{p})$, ε — фундаментальная единица в $\mathcal{O}$, а $h = h(p)$ — число классов.
Положим

$$a + b\sqrt{p} = \begin{cases} \varepsilon^h, & \text{если } p \equiv 1 \pmod 8, \\ \varepsilon^{3h}, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

Гипотеза (Чэпмен)

Если $p \equiv 1 \pmod 4$, то $\det C = -a$.

Гипотеза Чэпмена: $p \equiv 1 \pmod 4$

Пусть $\mathcal{O}$ — кольцо целых в $\mathbb{Q}(\sqrt{p})$, ε — фундаментальная единица в $\mathcal{O}$, а $h = h(p)$ — число классов.
Положим

$$a + b\sqrt{p} = \begin{cases} \varepsilon^h, & \text{если } p \equiv 1 \pmod 8, \\ \varepsilon^{3h}, & \text{если } p \equiv 5 \pmod 8, \end{cases}$$

Гипотеза (Чэпмен)

Если $p \equiv 1 \pmod 4$, то $\det C = -a$.

Доказана в: M.A.Vsemirnov. On R. Chapman's "evil determinant": case p=1 (mod 4). Acta Arithmetica 159 (2013), no.4, 331–344.

Матричные факторизации: $p \equiv 3 \pmod 4$

Пусть ζ — первообразный корень из 1 степени p, $\tau = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^{2k}$.

Матричные факторизации: $p \equiv 3 \pmod 4$

Пусть ζ — первообразный корень из 1 степени p,
$\tau = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^{2k}$.

Теорема

Пусть $p \equiv 3 \pmod 4$. Тогда
$C((p+1)/2, p) = -\tau\zeta^{-(p+1)/4} \cdot VDUDV$, где

Матричные факторизации: $p \equiv 3 \pmod 4$

Пусть ζ — первообразный корень из 1 степени p,
$\tau = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^{2k}$.

Теорема

Пусть $p \equiv 3 \pmod 4$. Тогда
$C((p+1)/2, p) = -\tau\zeta^{-(p+1)/4} \cdot VDUDV$, где

$$U_{ij} = \frac{\left(\frac{i}{p}\right)\zeta^{-j-2i} - \left(\frac{j}{p}\right)\zeta^{-2j-i}}{\zeta^{-i-j} - \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)}, \quad 0 \le i,j \le (p-1)/2,$$

$$V_{ij} = \zeta^{2ij}, \quad 0 \le i,j \le (p-1)/2,$$

$$D_{ii} = \prod_{\substack{0 \le k \le n \\ k \ne i}} \frac{1}{\zeta^{2i} - \zeta^{2k}}, \quad 0 \le i \le (p-1)/2,$$

Вычисление определителя: $p \equiv 3 \pmod 4$

Пусть G — диагональная матрица:

$$G_{00} = 1, \quad G_{ii} = \left(\frac{i}{p}\right)\zeta^i, \quad i = 1, \ldots, (p-1)/2.$$

Положим $W = -GUG$. Тогда W — частный случай кососимметирической матрицы Шура

$$Z(x_0, \ldots, x_{n-1}) = (Z_{ij}) = \left(\frac{x_i - x_j}{1 - x_i x_j}\right).$$

соответствующий выбору $x_0 = 1$, $x_i = \left(\frac{i}{p}\right)\zeta^i$, $i = 1, \ldots, (p-1)/2$.

Вычисление определителя: $p \equiv 3 \pmod 4$

Пусть G — диагональная матрица:

$$G_{00} = 1, \quad G_{ii} = \left(\frac{i}{p}\right)\zeta^i, \quad i = 1, \ldots, (p-1)/2.$$

Положим $W = -GUG$. Тогда W — частный случай кососимметирической матрицы Шура

$$Z(x_0, \ldots, x_{n-1}) = (Z_{ij}) = \left(\frac{x_i - x_j}{1 - x_i x_j}\right).$$

соответствующий выбору $x_0 = 1$, $x_i = \left(\frac{i}{p}\right)\zeta^i$, $i = 1, \ldots, (p-1)/2$.

Лемма (Stembridge; Laksov—Lascoux—Thorup)

$$\det(Z(x_0, \ldots, x_{n-1})) = \prod_{0 \le i < j \le n-1} \left(\frac{x_i - x_j}{1 - x_i x_j}\right)^2.$$

Вычисление определителя: $p \equiv 3 \pmod 4$

Напомним:

$$\begin{aligned} C((p+1)/2, p) &= -\tau\zeta^{-(p+1)/4} \cdot VDUDV, \\ U &= -G^{-1}WG^{-1}, \\ \det W &= \prod_{1 \le i < j \le n} \left(\frac{\left(\frac{i}{p}\right)\zeta^i - \left(\frac{j}{p}\right)\zeta^j}{1 - \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)\zeta^{i+j}} \right)^2 \end{aligned}$$

Отсюда уже можно вывести, что $\det C = 1$.

Матричные факторизации: $p \equiv 1 \pmod 4$

Теперь удобнее фиксировать выбор ζ: $\zeta = \exp(2\pi i/p)$.

$$
\begin{aligned}
U_{ij} &= \frac{\left(\frac{i}{p}\right)\zeta^{-j-2i} + \left(\frac{j}{p}\right)\zeta^{-2j-i}}{\zeta^{-i-j} + \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)}, \quad 0 \le i,j \le (p-1)/2, \\
V_{ij} &= \zeta^{2ij}, \quad 0 \le i,j \le (p-1)/2, \\
D_{ii} &= \prod_{\substack{0 \le k \le n \\ k \ne i}} \frac{1}{\zeta^{2i} - \zeta^{2k}}, \quad 0 \le i \le (p-1)/2,
\end{aligned}
$$

Матричные факторизации: $p \equiv 1 \pmod 4$

Теперь удобнее фиксировать выбор ζ: $\zeta = \exp(2\pi i/p)$.

$$
\begin{aligned}
U_{ij} &= \frac{\left(\frac{i}{p}\right)\zeta^{-j-2i} + \left(\frac{j}{p}\right)\zeta^{-2j-i}}{\zeta^{-i-j} + \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)}, \quad 0 \le i,j \le (p-1)/2, \\
V_{ij} &= \zeta^{2ij}, \quad 0 \le i,j \le (p-1)/2, \\
D_{ii} &= \prod_{\substack{0 \le k \le n \\ k \ne i}} \frac{1}{\zeta^{2i} - \zeta^{2k}}, \quad 0 \le i \le (p-1)/2,
\end{aligned}
$$

Теорема

$$C((p+1)/2, p) = \tau\zeta^{(p-1)/4} \cdot VDUDV = \left(\frac{2}{p}\right)\sqrt{p}\zeta^{(p-1)/4} \cdot VDUDV.$$

Вычисление определителей: $p \equiv 1 \pmod 4$

Сводится к вычислению определителей матриц

$$Z = (Z_{ij}) = \left(\frac{u_i + v_j}{1 + u_i v_j} \right).$$

Вычисление определителей: $p \equiv 1 \pmod 4$

Сводится к вычислению определителей матриц

$$Z = (Z_{ij}) = \left(\frac{u_i + v_j}{1 + u_i v_j} \right).$$

Этот определитель, в свою очередь, сводится к вычислению определителя Коши:

$$\det \left(\frac{1}{1 + u_i v_j} \right)_{0 \le i,j \le m-1} = \prod_{0 \le i < j \le m-1} \left((u_i - u_j)(v_j - v_i) \right) \times \prod_{0 \le i,j \le m-1} (u_i + v_j)^{-1}.$$

Вычисление определителей: $p \equiv 1 \pmod 4$

$$\det W = -\frac{(-1)^{(n-1)(n-2)/2}}{2}\left(\prod_{j=1}^{n-1}\left(1+\left(\frac{j}{p}\right)\zeta^j\right)^2 - \prod_{j=1}^{n-1}\left(1-\left(\frac{j}{p}\right)\zeta^i\right)^2\right)$$

$$\times \prod_{1\le i<j\le n-1}\left(\left(\frac{i}{p}\right)\zeta^i - \left(\frac{j}{p}\right)\zeta^j\right)^2 \prod_{1\le i<j\le n-1}\left(1+\left(\frac{i}{p}\right)\left(\frac{j}{p}\right)\zeta^{i+j}\right)^{-2}$$

$$\times \prod_{j=1}^{n-1}(1+\zeta^{2j})^{-1}.$$

Вычисление определителей: $p \equiv 1 \pmod 4$

$$\prod_{j=1}^{n-1} \left(1 + \left(\frac{j}{p}\right)\zeta^j\right)^2 = (-1)^{(n-1)/2}\zeta^{n(n-1)/2}\sqrt{p}\left(\frac{\prod \sin\frac{\pi j}{p}}{\prod \sin\frac{\pi k}{p}}\right)^{2-(2/p)}$$

где j пробегает квадратичные невычеты, а k пробегает ненулевые квадратичные вычеты.

Вычисление определителей: $p \equiv 1 \pmod 4$

$$\prod_{j=1}^{n-1} \left(1 + \left(\frac{j}{p}\right)\zeta^j\right)^2 = (-1)^{(n-1)/2}\zeta^{n(n-1)/2}\sqrt{p}\left(\frac{\prod \sin \frac{\pi j}{p}}{\prod \sin \frac{\pi k}{p}}\right)^{2-(2/p)}$$

где j пробегает квадратичные невычеты, а k пробегает ненулевые квадратичные вычеты.

Формула Дирихле:

$$\frac{\prod \sin \frac{\pi j}{p}}{\prod \sin \frac{\pi k}{p}} = \epsilon^h.$$

Открытые вопросы

$$C(n,p) = (C_{ij}) = \left(\left(\frac{j-i}{p} \right) \right)_{0 \le i,j \le n-1}.$$

Открытые вопросы

$$C(n,p) = (C_{ij}) = \left(\left(\frac{j-i}{p} \right) \right)_{0 \le i,j \le n-1}.$$

- $p \equiv 3 \pmod 4$, $n = (p-3)/2$, $p > 3$. Верно ли, что $\det C((p-3)/2, p) = 1$?

Открытые вопросы

$$C(n,p) = (C_{ij}) = \left(\left(\frac{j-i}{p} \right) \right)_{0 \le i,j \le n-1}.$$

- $p \equiv 3 \pmod 4$, $n = (p-3)/2$, $p > 3$. Верно ли, что $\det C((p-3)/2, p) = 1$?
- $p \equiv 3 \pmod 4$, $n = (p+5)/2$, $p > 3$. Верно ли, что $\det C((p+5)/2, p) = p^2 \left(\frac{p-3+\left(\frac{3}{p}\right)}{3} \right)^2$?

Открытые вопросы

Гипотеза

Для всякого $r \geq 0$ существует целое $N = N(r)$ и набор многочленов $H_{r,a}^{(1)}$, $1 \leq a \leq N$, $(a, N) = 1$, таких, что для всех достаточно больших $p \equiv 3 \pmod 4$ выполнено

$$\det C((p-1)/2 - 2r, p) = H_{r,a}^{(1)}(p).$$

если $p \equiv a \pmod N$.

Гипотеза

Для всякого $r \geq 0$ существует целое $N = N(r)$ и набор многочленов $H_{r,a}^{(2)}$, $1 \leq a \leq N$, $(a, N) = 1$, таких, что для всех достаточно больших $p \equiv 3 \pmod 4$ выполнено

$$\det C((p+1)/2 + 2r, p) = p^{2r} H_{r,a}^{(2)}(p)$$