



# Math-Net.Ru

All Russian mathematical portal

I. D. Shkredov, On the  
multiplicative Chung-Diaconis-Graham process, *Mat. Sb.*,  
2023, Volume 214, Number 6, 136–154

DOI: 10.4213/sm9811

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have  
read and agreed to these terms of use  
<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 18.97.9.173

December 12, 2024, 17:56:45



И. Д. Шкрёдов

## О мультипликативном процессе Чанг–Диакониса–Грэма

Изучается ленивая цепь Маркова на  $\mathbb{F}_p$ , заданная формулой  $X_{n+1} = X_n$  с вероятностью  $1/2$  и в противном случае  $X_{n+1} = f(X_n) \cdot \varepsilon_{n+1}$ , где случайные величины  $\varepsilon_n$  равномерно распределены на  $\{\gamma, \gamma^{-1}\}$ . Здесь  $\gamma$  – первообразный корень и функция  $f(x) = x/(x-1)$  или же  $f(x) = \text{ind}(x)$ . Показано, что время перемешивания такой цепи  $X_n$  есть  $\exp(O(\log p \cdot \log \log \log p / \log \log p))$ . Также мы получаем приложение разработанной техники к одному аддитивно-комбинаторному вопросу о множествах Сидонова типа.

Библиография: 34 названия.

**Ключевые слова:** цепи Маркова, процесс Чанг–Диакониса–Грэма, время перемешивания, геометрия инцидентий, множества Сидона.

DOI: <https://doi.org/10.4213/sm9811>

### § 1. Введение

**1.1.** Процесс Чанг–Диакониса–Грэма (см. [6]) – это случайное блуждание на  $\mathbb{F}_p$  (в более общем случае на  $\mathbb{Z}/n\mathbb{Z}$  для составного  $n$ ), определенное как

$$X_{j+1} = aX_j + \varepsilon_{j+1}, \quad (1.1)$$

где  $a \in \mathbb{F}_p^*$  – фиксированный остаток, а случайные величины  $\varepsilon_j$  независимы и одинаково распределены (в оригинальной работе [6] величины  $\varepsilon_j$  были распределены равномерно на  $\{-1, 0, 1\}$  и  $a$  было равно двойке). Это случайное блуждание активно изучалось, например, в работах [4], [6]–[10] и др. В нашей статье мы изучаем следующую характеристику  $X_n$ , которая называется *временем перемешивания*:

$$t_{\text{mix}}(\varepsilon) := \inf \left\{ n : \max_{A \subseteq \mathbb{F}_p} \left| \mathbb{P}(X_n \in A) - \frac{|A|}{p} \right| \leq \varepsilon \right\}.$$

Обычно задается конкретное значение параметра  $\varepsilon$ , например,  $\varepsilon = 1/4$  и далее мы будем говорить о  $t_{\text{mix}} := t_{\text{mix}}(1/4)$ . Простое случайное блуждание на  $\mathbb{F}_p$  имеет время перемешивания  $t_{\text{mix}}$  порядка  $p^2$  (см. [16]), и, как было показано в [6] (см. также более позднюю работу [7]), время перемешивания процесса (1.1) не превосходит  $O(\log p \cdot \log \log p)$ . Таким образом процесс Чанг–Диакониса–Грэма дает пример явления ускорения, т.е. уменьшения времени сходимости. В [8]

---

Исследование выполнено за счет гранта Российского научного фонда № 19-11-00001, <https://rscf.ru/project/19-11-00001/>.

была рассмотрена более общая нелинейная версия процесса Чанг–Диакониса–Грэма, определенная как

$$X_{j+1} = f(X_j) + \varepsilon_{j+1}, \tag{1.2}$$

где  $f$  – биекция на  $\mathbb{F}_p$ . В частности, было доказано, что для рациональных функций ограниченной степени (корректно определенных в полюсах, см. [8]) время перемешивания равно

$$t_{\text{mix}}\left(\frac{1}{4}\right) = O(p^{1+\varepsilon}) \quad \forall \varepsilon > 0. \tag{1.3}$$

Вероятно, для процесса (1.2) правильным ответом является  $t_{\text{mix}} = O(\log p)$ , но такой результат было получено только для случая  $f(x) = 1/x$  при  $x \neq 0$  и  $f(0) = 0$ , см. [9]. Доказательство основано на методе  $\text{SL}_2(\mathbb{F}_p)$ -действий из работы [3]. В [4] был задан вопрос о нахождении других явных примеров марковских цепей с малым временем перемешивания.

Наша работа посвящена мультипликативной форме процесса Чанг–Диакониса–Грэма. Мультипликативные варианты процесса рассматривались в [1], [11], [12], [15] и в других работах. Рассмотрим семейство функций

$$f_*^{\alpha,\beta}(x) = \frac{x}{\alpha x + \beta}, \tag{1.4}$$

где  $\alpha, \beta \neq 0$ . Большинство приведенных ниже результатов не зависят от  $\alpha, \beta$ . В таких случаях мы не будем их указывать. В теоремах 1 и 7 нужно, чтобы функция  $f_*^{\alpha,\beta}(x)$  была биективна, поэтому полагаем  $f_*^{\alpha,\beta}(-\beta/\alpha) := 1/\alpha$ . Так как теоремы 1 и 7 не зависят от выбора  $(\alpha, \beta)$ , то можно положить  $\alpha = 1, \beta = -1$  и  $f_*(x) := f_*^{1,-1}(x)$ . Сформулируем частный случай нашего основного результата.

**ТЕОРЕМА 1.** Пусть  $p$  – простое число и  $\gamma \in \mathbb{F}_p^*$  – первообразный корень. Также пусть  $\varepsilon_j$  – случайные величины, равномерно распределенные на  $\{\gamma, \gamma^{-1}\}$ . Рассмотрим ленивую цепь Маркова  $0 \neq X_0, X_1, \dots, X_n, \dots$ ,

$$X_{j+1} = \begin{cases} f_*(X_j) \cdot \varepsilon_{j+1} & \text{с вероятностью } \frac{1}{2}, \\ X_j & \text{с вероятностью } \frac{1}{2}. \end{cases} \tag{1.5}$$

Тогда для любого  $c > 0$  и для любого  $n = c \exp(\log p \cdot \log \log \log p / \log \log p)$  имеем

$$\|P_n - U\| := \max_{A \subseteq \mathbb{F}_p^*} \left| \mathbb{P}(X_n \in A) - \frac{|A|}{p-1} \right| \leq K e^{-Kc},$$

где  $K > 0$  – абсолютная константа. То же верно и для  $X_{j+1} = f_*(X_j) \cdot \varepsilon_{j+1}$ , где  $\varepsilon_j$  – случайные величины, равномерно распределенные на  $\{1, \gamma^{-1}, \gamma\}$ .

Другими словами, время перемешивания нашей цепи Маркова есть  $n$ , где  $n$  задается формулой выше. Похожим методом мы получаем такую же оценку на время перемешивания для другой цепи с  $f_*(x) = \text{ind}(x)$  и для

цепи вида (1.2) с  $f(x) = \exp(x)$ , см. теорему 9 и формулы (3.21), (3.22) ниже (функции  $\text{ind}$ ,  $\exp$  определены в §2). Также мы рассмотрели и иные цепи (которые могут быть даже более интересны, чем (1.5)), а именно

$$X_{j+1} = \begin{cases} \text{ind}(X_j) \cdot \varepsilon_{j+1} & \text{с вероятностью } \frac{1}{2}, \\ X_j & \text{с вероятностью } \frac{1}{2} \end{cases} \quad (1.6)$$

( $X_0 \neq 0$ ) или как в (1.2) с  $f(x) = \exp(x)$ , т.е.

$$X_{j+1} = \begin{cases} \exp(X_j) + \varepsilon_{j+1} & \text{с вероятностью } \frac{1}{2} \\ X_j & \text{с вероятностью } \frac{1}{2}. \end{cases} \quad (1.7)$$

В качестве побочного результата мы получим, что в случае  $f(x) = x^2$  и  $p \equiv 3 \pmod{4}$ , где  $p$  – достаточно большое простое число, время перемешивания (1.2) есть в действительности  $O(p \log p)$ , см. замечание 2. Еще раз обратим внимание на то, что ожидаемый порядок  $t_{\text{mix}}$  во всех этих проблемах есть, вероятно,  $O(\log p)$ , но это может оказаться трудным вопросом (особенно с учетом некоторых специальных конструкций в аффинной группе, которые показывают на наличие семейства так называемых “богатых” преобразований, имеющих в точности субэкспоненциальные нижние границы на число инцидентностей, см. [17; теорема 15]).

Наш подход не аналитический, как в [8], а использует методы из аддитивной комбинаторики и геометрии инцидентности. В частности, мы применяем результаты про рост в аффинной группе  $\text{Aff}(\mathbb{F}_p)$ . Центральная часть нашей статьи имеет больше общего с работами [3], [27], чем с работой [8], но мы активно используем схему доказательства из последней статьи. С аддитивно-комбинаторной точки зрения основным новшеством является последовательность асимптотических формул для числа инцидентностей точек и прямых, которые были получены с помощью действия  $\text{Aff}(\mathbb{F}_p)$ , см. начало §3. Автор надеется, что эти формулы могут быть интересны сами по себе. Хорошо известно (см., например, [3], [17], [18], [22], [26]–[28], [30]), что геометрия инцидентности и феномен сумм-произведений иногда работают лучше, чем классические аналитические методы, и именно поэтому становится возможным преодолеть барьер квадратного корня, который соответствует естественной границе (1.3) (см. детали в теореме 8 и доказательствах теорем 7, 9).

Оказывается, что этот же метод применим к чисто аддитивно-комбинаторному вопросу о множествах Сидона. Множества Сидона – это классическая тема из комбинаторной теории чисел (см., например, обзор [19]). Напомним, что подмножество  $S$  абелевой группы  $\mathbf{G}$  с групповой операцией  $*$  называется  $g$ -множеством Сидона, если для любого  $z \neq 1$  уравнение  $z = x*y^{-1}$ , где  $x, y \in S$ , имеет не больше  $g$  решений. Если  $g = 1$ , тогда мы приходим к классическому определению множеств Сидона (см. [29]). Для произвольного множества  $A \subseteq \mathbf{G}$ , обозначим через  $\text{Sid}^*(A)$  размер максимального по мощности сидоновского подмножества множества  $A$  и через  $\text{Sid}_K^*(A)$  размер максимального

$K$ -сидоновского множества. Известно [14] (см. также [24]), что для любого подмножества  $A$  нашей абелевой группы  $\mathbf{G}$  имеет место следующая оценка:

$$\text{Sid}^*(A) \gg \sqrt{|A|}.$$

Клурман и Похоацэ, как указано в [13], спрашивают о возможности улучшить последнюю границу, имея две различные операции на кольце  $\mathbf{G}$ . В [28] автор доказал такой результат.

**ТЕОРЕМА 2.** Пусть  $A \subseteq \mathbb{F}$  – произвольное множество, где  $\mathbb{F} = \mathbb{R}$  или  $\mathbb{F} = \mathbb{F}_p$  (в случае простого поля положим дополнительно, что  $|A| < \sqrt{p}$ ). Тогда существуют абсолютные константы  $c > 0$ ,  $K \geq 1$  такие, что

$$\max\{\text{Sid}_K^+(A), \text{Sid}_K^\times(A)\} \gg |A|^{1/2+c}. \tag{1.8}$$

Относительно верхних границ для (1.8) мы отсылаем заинтересованного читателя к работам [20] и [28]. Отметим что  $\text{Sid}_K^\times(A) = \text{Sid}_K^+(\log(A))$  и  $\text{Sid}_K^+(A) = \text{Sid}_K^\times(\exp(A))$  для  $A \subset \mathbb{R}^+$ . Таким образом, возможно переписать неравенство (1.8) в терминах только одной операции. Рассмотрим общий вопрос, который был сформулирован А. Уорреном во время конференции SANTS’2021 (см. [34]).

**ПРОБЛЕМА 1.** Пусть  $f, g$  – некоторые “хорошие” (скажем, выпуклые или вогнутые) функции. Верно ли что для любого множества  $A \subset \mathbb{R}^+$  выполняется

$$\max\{\text{Sid}_K^+(A), \text{Sid}_K^+(f(A))\}, \quad \max\{\text{Sid}_K^\times(A), \text{Sid}_K^\times(g(A))\} \gg |A|^{1/2+c}?$$

Здесь  $c > 0$  и  $K \geq 1$  – некоторые абсолютные константы. Что можно сказать для  $K$ , равной в точности единице? Какое оптимальное значение константы  $c > 0$ ?

В этой работе мы получаем положительный ответ на вопрос выше для  $g(x) = x + 1$  и  $f(x) = \exp(x)$ , где в случае  $\mathbb{F}_p$  последняя функция определена как  $\exp(x) := g^x$  и  $g$  есть фиксированный первообразный корень.

**ТЕОРЕМА 3.** Пусть  $A \subseteq \mathbb{F}$  – произвольное множество, где  $\mathbb{F} = \mathbb{R}$  или  $\mathbb{F} = \mathbb{F}_p$  (в случае простого поля положим дополнительно, что  $|A| < \sqrt{p}$ ). Тогда существуют абсолютные константы  $c > 0$ ,  $K \geq 1$  такие, что

$$\max\{\text{Sid}_K^\times(A), \text{Sid}_K^\times(A + 1)\} \gg |A|^{1/2+c}, \tag{1.9}$$

$$\max\{\text{Sid}_K^+(A), \text{Sid}_K^+(\exp(A))\} \gg |A|^{1/2+c}. \tag{1.10}$$

С другой стороны, для любого целого  $k \geq 1$  существует  $A \subseteq \mathbb{F}$  такое, что

$$\max\{\text{Sid}_k^\times(A), \text{Sid}_k^\times(A + 1)\} \ll k^{1/2}|A|^{3/4}. \tag{1.11}$$

Мы благодарим Джимми Хе за очень полезные дискуссии и ценные предложения. Также мы благодарим рецензента за многочисленные комментарии и аккуратную вычитку нашей статьи.

## § 2. Основные определения

Обозначим через  $\mathbf{G}$  (абелеву) группу. Иногда мы указываем групповую операцию  $+$  или  $\times$  в рассматриваемых величинах (энергия, функция представления и т.п., см. ниже). Пусть  $\mathbb{F}$  – это поле  $\mathbb{R}$  или же  $\mathbb{F} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  для простого  $p$ . Пусть  $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ .

Мы используем ту же заглавную букву для обозначения множества  $A \subseteq \mathbb{F}$  и его характеристической функции  $A: \mathbb{F} \rightarrow \{0, 1\}$ , а в случае конечного  $\mathbb{F}$  мы пишем  $f_A(x) := A(x) - |A|/|\mathbb{F}|$  для *балансовой функции* множества  $A$ . Для двух множеств  $A, B \subseteq \mathbf{G}$  определим *множество сумм*  $A$  и  $B$  как

$$A + B := \{a + b : a \in A, b \in B\}.$$

Подобным образом определим *множество разностей* и *множествах старших сумм*, например,  $2A - A$  есть  $A + A - A$ . Обозначим через  $\dot{+}$  прямую сумму, т.е.  $A \dot{+} B = \{a + b : a \in A, b \in B\}$  и  $a + b = a' + b'$  влечет  $a = a'$  и  $b = b'$ . Также мы используем обозначение  $A \times B = \{(a, b) : a \in A, b \in B\} \subseteq \mathbf{G} \times \mathbf{G}$  для декартова произведения  $A$  и  $B$ . Для абелевой группы  $\mathbf{G}$  выполняется неравенство Плюннеке–Ружа (см., например, [32])

$$|nA - mA| \leq \left( \frac{|A + A|}{|A|} \right)^{n+m} |A|, \quad (2.1)$$

где  $n, m$  – любые положительные целые. Мы используем обозначения для функций представлений  $r_{A+B}(x)$  или  $r_{A-B}(x)$  и т.п., которые равняются числу способов, которыми  $x \in \mathbf{G}$  может быть выражено как сумма  $a + b$  или  $a - b$ , где  $a \in A, b \in B$ , соответственно. Например,  $|A| = r_{A-A}(0)$ . Подобным образом, для функций  $f_1, \dots, f_k: \mathbf{G} \rightarrow \mathbb{C}$  мы пишем  $r_{f_1 + \dots + f_k}(x) = \sum_{x_1 + \dots + x_k = x} f_1(x_1) \cdots f_k(x_k)$ .

Для любых двух множеств  $A, B \subseteq \mathbf{G}$  *аддитивная энергия*  $A$  и  $B$  определена как

$$E(A, B) = E^+(A, B) = |\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B : a_1 - b_1 = a_2 - b_2\}|.$$

Если  $A = B$ , то мы пишем  $E(A)$  вместо  $E(A, A)$ . В более общем случае для множеств  $A_1, \dots, A_{2k}$ , принадлежащих произвольной (некоммутативной) группе  $\mathbf{G}$ , и  $k \geq 2$  определим энергию  $T_k(A_1, \dots, A_{2k})$  как

$$T_k(A_1, \dots, A_{2k}) = \left| \left\{ (a_1, \dots, a_{2k}) \in A_1 \times \cdots \times A_{2k} : a_1 a_2^{-1} \cdots a_{k-1} a_k^{-1} = a_{k+1} a_{k+2}^{-1} \cdots a_{2k-1} a_{2k}^{-1} \right\} \right| \quad (2.2)$$

для четных  $k$  и для нечетных  $k$  как

$$T_k(A_1, \dots, A_{2k}) = \left| \left\{ (a_1, \dots, a_{2k}) \in A_1 \times \cdots \times A_{2k} : a_1 a_2^{-1} \cdots a_{k-1}^{-1} a_k = a_{k+1} a_{k+2}^{-1} \cdots a_{2k-1}^{-1} a_{2k} \right\} \right|. \quad (2.3)$$

Аналогично, имея вещественные функции  $f_1, \dots, f_{2k}: \mathbf{G} \rightarrow \mathbb{C}$  (например,  $k$  четно), мы полагаем

$$T_k(f_1, \dots, f_{2k}) = \sum_{a_1 a_2^{-1} \cdots a_{k-1} a_k^{-1} = a_{k+1} a_{k+2}^{-1} \cdots a_{2k-1} a_{2k}^{-1}} f_1(a_1) \cdots f_{2k}(a_{2k}).$$

Если мы хотим подчеркнуть групповую операцию  $+$ , то мы используем обозначение  $\Gamma_k^+(f_1, \dots, f_{2k})$ , так что (пусть  $k$  чётно)

$$\Gamma_k^+(f_1, \dots, f_{2k}) = \sum_{a_1 - a_2 + \dots + a_{k-1} - a_k = a_{k+1} - a_{k+2} + \dots + a_{2k-1} - a_{2k}} f_1(a_1) \cdots f_{2k}(a_{2k}).$$

Мы пишем  $\Gamma_k(f)$  вместо  $\Gamma_k(f, \dots, f)$ . В абелевом случае положим для  $k \geq 2$

$$E_k^+(A) := \sum_{x \in \mathbf{G}} r_{A-A}^k(x) = \sum_{\alpha_1, \dots, \alpha_{k-1} \in \mathbf{G}} |A \cap (A + \alpha_1) \cap \dots \cap (A + \alpha_{k-1})|^2 \quad (2.4)$$

(тождество выше может быть найдено, например, в [23]). Ясно, что  $|A|^k \leq E_k^+(A) \leq |A|^{k+1}$ . Также мы пишем  $\hat{E}_k^+(A) = \sum_x r_{A+A}^k(x)$ .

Конечно, данные выше определения зависят от групповой операции, которая будет понятна из контекста. Например, используя умножение (скажем, в  $\mathbb{R}$  или в  $\mathbb{F}_p$ ), мы запишем  $AB = \{ab : a \in A, b \in B\}$  для множества произведений множеств  $A$  и  $B$ , далее  $r_{AB}(x) = \sum_{ab=x} A(a)B(b)$  и т.п.

Обозначим через  $\text{ord}(x)$  мультипликативный порядок элемента  $x \in \mathbb{F}_p^*$  и пусть  $\text{ind}(x)$  будет определено как  $x = g^{\text{ind}(x)}$ , где  $g$  – фиксированный первообразный корень  $\mathbb{F}_p^*$ . Удобно полагать, что функция  $\text{ind}(x)$  принимает значения от 1 до  $p - 1$  и, таким образом,  $\text{ind}(x)$  определено на  $\mathbb{F}_p^*$ . Похожим образом мы обозначаем через  $\text{exp}(x) : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$  функцию  $\text{exp}(x) = g^x$ , где  $x \in \mathbb{F}_p^*$ . Пусть  $\text{Aff}(\mathbb{F})$  – группа преобразований  $x \rightarrow ax + b$ , где  $a \in \mathbb{F}^*$ ,  $b \in \mathbb{F}$ . Иногда мы пишем  $(a, b) \in \text{Aff}(\mathbb{F})$  для отображения  $x \rightarrow ax + b$ .

Символы  $\ll$  и  $\gg$  – это обычные символы Виноградова. Когда константы в знаках зависят от параметра  $M$ , мы пишем  $\ll_M$  и  $\gg_M$ . Все логарифмы в статье имеют основание 2. Для множества  $A$ ,  $|A| > 1$ , мы пишем  $a \lesssim b$  или  $b \gtrsim a$ , если  $a = O(b \log^c |A|)$ , где  $c > 0$  есть некоторая константа, которая может меняться от строчки к строчке. Обозначим через  $[n]$  множество  $\{1, 2, \dots, n\}$ .

Упомянем теперь несколько полезных результатов, к которым мы будем обращаться в тексте. Начнем с результата из [27].

**ЛЕММА 1.** Пусть  $f_1, \dots, f_{2k} : \mathbf{G} \rightarrow \mathbb{C}$  – произвольные функции. Тогда

$$\Gamma_k^{2k}(f_1, \dots, f_{2k}) \leq \prod_{j=1}^{2k} \Gamma_k(f_j). \quad (2.5)$$

Следующая лемма 2 о коллинеарный четверках в множестве  $A \times A$  (т.е. число 4-кортежей  $\{(x_1, l(x_1)), \dots, (x_4, l(x_4))\}$ , где  $x_1, x_2, x_3, x_4 \in A$ ,  $l \in \text{Aff}(\mathbb{F}_p)$  и  $l(x_1), l(x_2), l(x_3), l(x_4) \in A$ ) была доказана в [18; с. 604–607]. Обозначим через  $Q(A)$  число таких коллинеарных четверок и перепишем асимптотическую формулу для  $Q(A)$ , см. [18; теорема 11, (2)]

$$Q(A) = \frac{|A|^8}{p^2} + O(|A|^5 \log |A|) \quad (2.6)$$

в следующей удобной форме (2.7), которая может использоваться в дальнейших результатах. Наконец, отметим что аффинное преобразование  $\mathbb{F}_p$  может быть отождествлено с прямой в  $\mathbb{F}_p \times \mathbb{F}_p$  с помощью ее графика.

ЛЕММА 2. Пусть  $A \subseteq \mathbb{F}_p$  – произвольное множество и  $f_A(x) = A(x) - |A|/p$ . Тогда

$$Q(f_A) := \sum_{l \in \text{Aff}(\mathbb{F}_p)} \left| \sum_x f_A(x) f_A(lx) \right|^4 \ll |A|^5 \log |A|, \quad (2.7)$$

где суммирование по  $l$  в последней формуле берется по всеми аффинным преобразованиям (прямым), имеющим не меньше двух точек в  $A \times A$ .

Нам понадобится [2; теорема А], которую мы повторим ниже в теореме 4. Лучшая зависимость  $\delta'$  от  $\delta$  в виде  $\delta/(C_1 \log(C_2 r/\delta))^k$ , где  $C_1, C_2 > 0$  – некоторые константы, может быть найдена в [26; теорема 46, следствие 47]. Также мы показали в [26], что в действительности условие  $|A_j| \geq p^\delta$ ,  $j \in [k]$ , не требуется.

ТЕОРЕМА 4. Пусть  $k \geq 2$ ,  $A_1, \dots, A_k \subseteq \mathbb{F}_p$  – произвольные множества,  $|A_j| \geq p^\delta$ ,  $j \in [k]$ . Положим, что  $\prod_{j=1}^k |A_j| \geq p^{1+\delta}$ . Тогда для любого  $\lambda \neq 0$  выполняется

$$\sum_{x_1 \in A_1, \dots, x_k \in A_k} e^{2\pi i \lambda x_1 \dots x_k} \ll p^{-\delta'} |A_1| \dots |A_k|,$$

где  $\delta' > (\delta/k)^{Ck}$  и  $C > 0$  есть абсолютная константа. В частности, для любого  $l \geq 2$  и  $A_1 = \dots = A_k = A$  выполнено  $\Gamma_l^+(r_{f_A^k}) \leq |A|^{k(2l-1)} p^{-(2l-2)\delta'}$ .

Вспомним, что по определению  $r_{f_A^k}(x) = \sum_{x_1 \dots x_k = x} f_A(x_1) \dots f_A(x_k)$ , где  $f_A(x)$  есть балансовая функция множества  $A$ . Отметим, что возможно оценить  $\Gamma_l^+(r_{f_A^k})$  непосредственно, как было сделано в [25; теорема 5] (также см. [17]), чтобы улучшить неравенство  $\Gamma_l^+(r_{f_A^k}) \leq |A|^{k(2l-1)} p^{-(2l-2)\delta'}$ . Мы оставляем эти вычисления читателю, так как это усложнило бы доказательство, но улучшило бы оценку  $t_{\text{mix}}$  только на  $\log \log \log p$ . Тем не менее мы используем теорему 5, которая является упрощенной версией [25; теорема 5], в последней части статьи.

ТЕОРЕМА 5. Пусть  $A, B \subseteq \mathbb{F}_p$  – произвольные множества,  $|AB| \leq M|A|$ ,  $k \geq 2$ , и  $|B| \gtrsim_k M^{2^{k+1}}$ . Тогда

$$\Gamma_{2^k}^+(A) \lesssim_k M^{2^{k+1}} \left( \frac{|A|^{2^{k+1}}}{p} + |A|^{2^{k+1}-1} |B|^{-(k-1)/2} \right). \quad (2.8)$$

### § 3. Инциденции и время перемешивания

Начнем с нового считающего результата об инциденциях. Пусть  $\mathcal{P}, \mathcal{L} \subseteq \mathbb{F}_p \times \mathbb{F}_p$  – произвольные множество точек и множество прямых соответственно. Число инциденций между  $\mathcal{P}$  и  $\mathcal{L}$  есть

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) := |\{(q, l) \in \mathcal{P} \times \mathcal{L} : q \in l\}|. \quad (3.1)$$

Как и ранее, мы пишем  $f_{\mathcal{L}}(x) = \mathcal{L}(x) - |\mathcal{L}|/|\text{Aff}(\mathbb{F}_p)|$  для балансовой функции множества прямых  $\mathcal{L}$ .



**ПРЕДЛОЖЕНИЕ 1.** Пусть  $A, B \subseteq \mathbb{F}_p$  – произвольные множества и  $\mathcal{L}$  – некоторое множество аффинных преобразований. Тогда для любого положительного целого  $k$  выполнено

$$\begin{aligned} \mathcal{I}(A \times B, \mathcal{L}) &= \frac{|A||B||\mathcal{L}|}{p} \\ &\ll \sqrt{|A||B||\mathcal{L}|} \max \left\{ (\mathsf{T}_{2^k}(f_{\mathcal{L}})|A| \log |A|)^{1/2^{k+2}}, \sqrt{|\mathcal{L}||A|^{-2^{-k}}} \right\}. \end{aligned} \quad (3.2)$$

**ДОКАЗАТЕЛЬСТВО.** Имеем

$$\mathcal{I}(A \times B, \mathcal{L}) = \frac{|A||B||\mathcal{L}|}{p} + \sum_{x \in B} \sum_l f_{\mathcal{L}}(l) f_A(lx) = \frac{|A||B||\mathcal{L}|}{p} + \sigma. \quad (3.3)$$

Таким образом, мы можем использовать обе балансовые функции в (3.3) или можем выбрать только одну из них. Чтобы оценить величину остаточного члена  $\sigma$ , мы применяем неравенство Гёльдера несколько раз, как в [17], [22], и получаем (ниже мы используем обе балансовые функции)

$$\sigma^2 \leq |B| \sum_h r_{f_{\mathcal{L}-1} f_{\mathcal{L}}}(h) \sum_x f_A(x) f_A(hx),$$

и далее

$$\sigma^{2^k} \leq |B|^{2^{k-1}} |A|^{2^{k-1}-1} \sum_h r_{(f_{\mathcal{L}-1} f_{\mathcal{L}})^{2^{k-1}}}(h) \sum_x f_A(x) f_A(hx). \quad (3.4)$$

Здесь группа  $\mathbf{G}$  есть (некоммутативная) группа  $\text{Aff}(\mathbb{F}_p)$  и мы используем обозначение  $r_f(x)$  для  $f: \text{Aff}(\mathbb{F}_p) \rightarrow \mathbb{C}$  и  $x \in \text{Aff}(\mathbb{F}_p)$ . Вспомним, что  $r_{(f_{\mathcal{L}-1} f_{\mathcal{L}})^{2^{k-1}}}(h)$  означает величину

$$\sum_{x_1^{-1}x'_1 \cdots x_{2^{k-1}}^{-1}x'_{2^{k-1}} = h} f_{\mathcal{L}}(x_1) f_{\mathcal{L}}(x'_1) \cdots f_{\mathcal{L}}(x_{2^{k-1}}) f_{\mathcal{L}}(x'_{2^{k-1}})$$

в последней формуле. Разобьем сумму (3.4) на сумму  $\sigma_1$ , где суммирование берется над прямыми  $h$  (другими словами, элементами  $\text{Aff}(\mathbb{F}_p)$ ), имеющими не менее двух точек в  $A \times A$ , и, обозначая оставшиеся элементы  $\sigma_*$ , предположим, что  $\sigma_* \leq 2^{-1}\sigma$ . Тогда применяя неравенство Гёльдера еще раз, мы получим

$$\begin{aligned} \sigma^{2^{k+2}} &\ll |B|^{2^{k+1}} |A|^{2^{k+1}-4} \left( \sum_h |r_{(f_{\mathcal{L}-1} f_{\mathcal{L}})^{2^{k-1}}}(h)| \right)^3 \mathsf{Q}(f_A) \\ &\ll 2^{2^{k+1}} |B|^{2^{k+1}} |A|^{2^{k+1}-4} \mathsf{T}_{2^k}(f_{\mathcal{L}}) |\mathcal{L}|^{2^{k+1}} \mathsf{Q}(f_A), \end{aligned} \quad (3.5)$$

как и требовалось благодаря лемме 2. Осталось оценить  $\sigma_*$ . Имеем

$$\sum_x f_A(x) f_A(hx) = \sum_x A(x) A(hx) - \frac{|A|^2}{p},$$

как и

$$r_{(f_{\mathcal{L}-1} f_{\mathcal{L}})^{2^{k-1}}}(h) = r_{(\mathcal{L}-1)\mathcal{L})^{2^{k-1}}}(h) - \frac{|\mathcal{L}|^{2^k}}{p(p-1)}.$$

Конечно, произведение  $(\mathcal{L}^{-1}\mathcal{L})^{2^{k-1}}$  означает произведение в  $\text{Aff}(\mathbb{F}_p)$ . Обозначим через  $\Omega$  множество прямых, имеющих не более одной точки в  $A \times A$ . Мы можем предположить, что  $|A| \geq 2\sqrt{p}$ , так как иначе мы получим

$$\sigma_*^{2^{k+2}} \ll 2^{2^{k+2}} |B|^{2^{k+1}} |A|^{2^{k+1}-4} |\mathcal{L}|^{2^{k+2}}, \tag{3.6}$$

и это соответствует второй от максимума величине в (3.2). Далее, из основного результата [33] (также, см. [26] или просто формулу (3.20) ниже), мы видим что  $|\Omega| \ll p^3/|A|^2$ . Возвращаясь к (3.3), (3.4), находим

$$\sum_{h \in \Omega} r_{(f_{\mathcal{L}^{-1}} f_{\mathcal{L}})^{2^{k-1}}}(h) \sum_x f_A(x) f_A(hx) \ll 2^{2^k} |\mathcal{L}|^{2^k} + \frac{|\mathcal{L}|^{2^k} |A|^2 |\Omega|}{p^2(p-1)} \ll 2^{2^k} |\mathcal{L}|^{2^k}$$

и, таким образом, снова получаем (3.6). Предложение доказано.

Основное преимущество оценки (3.2) предложения 1 состоит в наличии асимптотической формулы для числа инцидентов  $\mathcal{I}(A \times B, \mathcal{L})$  (при этом множество  $\mathcal{L}$  может быть небольшим), а не только верхних неравенств для  $\mathcal{I}(\mathcal{P}, \mathcal{L})$ , как в [30]. Асимптотическая формула для величины  $\mathcal{I}(\mathcal{P}, \mathcal{L})$  была известна ранее для некоторых специальных случаев больших множеств (см. [33] или оценку (3.20) ниже) и для случая декартовых произведений, но больших множеств прямых (см. [26] и [30]).

В следующей лемме мы оцениваем энергию  $\mathsf{T}_k(\mathcal{L})$  для конкретного семейства прямых, которые возникнут в доказательствах результатов нашей работы.

**ЛЕММА 3.** Пусть  $A, B \subseteq \mathbb{F}_p^*$  – произвольные множества и  $\mathcal{L} = \{(a, b) : a \in A, b \in B\} \subseteq \text{Aff}(\mathbb{F}_p)$ . Тогда для любого  $k \geq 2$  выполняется

$$\mathsf{T}_k(f_{\mathcal{L}}) \leq |A|^{2^{k-1}} \mathsf{T}_k^+(f_B). \tag{3.7}$$

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим случай четного  $k$ , так как для нечетного  $k$  рассуждения аналогичны. Имеем  $\mathcal{L}^{-1}\mathcal{L} = \{(a/c, (b-d)/c) : a, c \in A, b, d \in B\}$ . Рассматривая величину  $\mathsf{T}_{2k}(f_{\mathcal{L}})$ , мы приходим к двум уравнениям. Первое уравнение есть

$$\frac{a_1 \cdots a_k}{c_1 \cdots c_k} = \frac{a'_1 \cdots a'_k}{c'_1 \cdots c'_k}. \tag{3.8}$$

Если мы зафиксируем в этом уравнении все переменные  $a_1, \dots, a_k, a'_1, \dots, a'_k, c_1, \dots, c_k, c'_1, \dots, c'_k \in A$ , тогда число решений второго уравнения будет  $\mathsf{T}_{2k}^+(\alpha_1 f_B, \dots, \alpha_{2k} f_B)$ , где  $\alpha_1, \dots, \alpha_{2k} \in \mathbb{F}_p^*$  – некоторые элементы  $A$ , зависящие от фиксированных переменных. Последняя величина не превосходит  $\mathsf{T}_{2k}^+(f_B)$  по лемме 1. Возвращаясь к (3.8), мы получаем необходимое неравенство. Лемма доказана.

Теперь мы готовы получить наш первый основной результат.

**ТЕОРЕМА 6.** Пусть  $A, B, X_1, Y_1, Z_1 \subseteq \mathbb{F}_p^*$  – произвольные множества,  $A = XY_1, B = XY_2, |A| = |X| |Y_1|/K_*$  и  $|B| = |X| |Y_2|/K_*$ . Пусть  $|Z| \geq p^\delta$  для данного  $\delta \gg \log \log \log p / \log \log p, M \geq 2\delta^{-1}$  и  $|XZ^M| \leq K|X|$ . Тогда для некоторой абсолютной константы  $C > 0$  выполнено

$$|\{(a, b) \in A \times B : a := f_*(b)\}| - \frac{K^2 K_*^2 |A| |B|}{p} \ll K K_* \sqrt{|A| |B|} \cdot p^{-\delta^{C/\delta}}. \tag{3.9}$$

ДОКАЗАТЕЛЬСТВО. Пусть  $\sigma$  – это величина из левой части (3.9) и  $k \geq 2$  – некоторый параметр. Также пусть  $Q_1 = AZ^M$ ,  $Q_2 = BZ^M$ . Тогда  $r_{Q_1 Z^{-M}}(a) = |Z|^M$  и  $r_{Q_2 Z^{-M}}(a) = |Z|^M$  для любого  $a \in A$ . Заметим, что  $|Q_1| \leq |XZ^M| |Y_1| \leq K|X| |Y_1| = KK_*|A|$  и подобная оценка верна для  $|Q_2|$ .

Имеем

$$|Z|^{2M} \sigma \leq \left| \left\{ (q_1, q_2, z_1, z_2) \in Q_1 \times Q_2 \times Z^M \times Z^M : \frac{q_1}{z_1} := f_* \left( \frac{q_2}{z_2} \right) \right\} \right|,$$

где  $z_1, z_2$  берутся с весами  $r_{Z^M}(z_1), r_{Z^M}(z_2)$ . Используя определение функции  $f_*^{\alpha, \beta}$ , мы приходим к уравнению

$$\frac{q_1}{z_1} = \frac{q_2}{\alpha q_2 + \beta z_2} \implies \frac{z_1}{q_1} - \frac{\beta z_2}{q_2} = \alpha. \tag{3.10}$$

Последнее уравнение может быть проинтерпретировано как инцидентии прямых и точек множества прямых  $\mathcal{L}$ , где любое  $l \in \mathcal{L}$  имеет вид  $l: z_1 X - \beta z_2 Y = \alpha$ , и множества точек  $\mathcal{P} = Q_1^{-1} \times Q_2^{-1}$ . Применяя предложение 1, мы получаем, что для любого  $k$

$$\sigma - \frac{|Q_1| |Q_2|}{p} \ll |Z|^{-M} \sqrt{|Q_1| |Q_2|} \cdot (T_{2^k}(f_{\mathcal{L}}) |Q_1|^4 p^{-2} \log pr)^{1/2^{k+2}}.$$

Используя наши оценки для размеров множеств  $Q_1, Q_2$  и совмещая их с леммой 3 и теоремой 4, получаем

$$\sigma - \frac{K^2 K_*^2 |A| |B|}{p} \lesssim KK_* \sqrt{|A| |B|} \cdot (p^{2-\delta'(2^k-2)} \log p)^{1/2^{k+2}}.$$

Взяв  $k$  такое, что  $\delta'(2^k - 2) \geq 3.1$ , получим

$$\sigma - \frac{K^2 K_*^2 |A| |B|}{p} \ll KK_* \sqrt{|A| |B|} p^{-\delta'/100}.$$

Теорема доказана.

ЗАМЕЧАНИЕ 1. Повторим, что если использовать улучшенную формулу для  $\delta'$  (см. замечание перед теоремой 4) вида  $\delta/(C_1 \log(C_2 r/\delta))^k$ , где  $C_1, C_2 > 0$  – некоторые константы, то ограничение на  $\delta$  в теореме 6 может быть ослаблено до  $\delta \gg \log \log \log \log p / \log \log p$  и, более того, прямая оценка для  $T_{2^k}$  дала бы  $\delta \gg 1/\log \log p$ . С другой стороны, это усложнило бы доказательство и лишь немного улучшило бы конечную оценку на  $t_{\text{mix}}$ , поэтому оставляем провести данные вычисления заинтересованному читателю.

СЛЕДСТВИЕ 1. Пусть  $g$  – первообразный корень и  $I, J \subseteq \mathbb{F}_p^*$  суть две геометрические прогрессии с одинаковым знаменателем  $g$  такие, что

$$\exp\left(\frac{C \log p \cdot \log \log \log p}{\log \log p}\right) \ll |I| = |J| \leq \frac{p}{2}, \tag{3.11}$$

где  $C > 0$  – абсолютная константа. Тогда

$$|\{(a, b) \in I \times J : a := f_*(b)\}| \leq (1 - \kappa) |I|, \tag{3.12}$$

где  $\kappa > 0$  – это абсолютная константа.

ДОКАЗАТЕЛЬСТВО. Пусть  $I = a \cdot \{1, g, \dots, g^n\}$ ,  $J = b \cdot \{1, g, \dots, g^n\}$ , где  $n = |I| = |J|$ . Применим теорему 6 с  $A = I$ ,  $B = J$ ,  $Y_1 = \{a\}$ ,  $Y_2 = \{b\}$ ,  $X = \{1, g, \dots, g^n\}$ ,  $K_* = 1$  и  $Z = \{1, g, \dots, g^m\}$ , где мы определили величину  $\delta$  как  $m := p^\delta$ , и пусть

$$m \leq \frac{cn}{r}, \tag{3.13}$$

где  $c = 1/8$  и  $M \geq 2/\delta$ . Тогда  $K = |XZ^M|/|X| \leq 1 + 2c$ . По формуле (3.9) получаем

$$|\{(a, b) \in I \times J : a := f_*(b)\}| - \frac{(1 + 2c)^2 |I| |J|}{p} \ll |I| \cdot p^{-\delta^{C/\delta}},$$

где  $C > 0$  – это абсолютная константа. Имеем  $(1 + 2c)^2 |I| |J| / p \leq (25/32) |I|$ , поскольку  $n \leq p/2$ . Вспоминая, что  $M \sim 1/\delta$  и  $\log n / \log p \gg \log \log \log p / \log \log p$ , мы удовлетворим условию (3.13), выбирая  $\delta \sim \log \log \log p / \log \log p$  и получим оценку (3.12) благодаря нашему предположению (3.11). Следствие доказано.

Теперь можно доказать теорему 1, которую мы формулируем в немного более общем виде (опять можно ослабить условие (3.14) и верхнее ограничение на  $n$ ). В наших рассуждениях мы используем некоторые части доказательства из [8].

ТЕОРЕМА 7. Пусть  $p$  – простое число и  $\gamma \in \mathbb{F}_p^*$  элемент порядке не менее

$$\exp\left(\Omega\left(\frac{\log p \cdot \log \log \log p}{\log \log p}\right)\right). \tag{3.14}$$

Также пусть  $\varepsilon_j$  – случайная величина, равномерно распределенная на  $\{\gamma^{-1}, \gamma\}$ . Рассмотрим ленивую марковскую цепь  $0 \neq X_0, X_1, \dots, X_n, \dots$ , определенную как

$$X_{j+1} = \begin{cases} f_*(X_j) \cdot \varepsilon_{j+1} & \text{с вероятностью } \frac{1}{2}, \\ X_j & \text{с вероятностью } \frac{1}{2}. \end{cases}$$

Тогда для произвольной  $c > 0$  и для любого  $n = c \exp(\log p \cdot \log \log \log p / \log \log p)$  выполняется

$$\|P_n - U\| := \max_{A \subseteq \mathbb{F}_p^*} \left| \mathbb{P}(X_n \in A) - \frac{|A|}{p-1} \right| \leq K e^{-Kc},$$

где  $K > 0$  – абсолютная константа. То же выполняется для цепи  $X_{j+1} = f_*(X_j) \cdot \varepsilon_{j+1}$ , где  $\varepsilon_j$  обозначает случайную величину, распределенную равномерно на  $\{1, \gamma^{-1}, \gamma\}$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $P$  – эргодическая цепь Маркова на  $k$ -регулярном ориентированном графе  $G = G(V, E)$ . Пусть  $h(G)$  – константа Чигера

$$h(G) = \min_{|S| \leq |V|/2} \frac{e(S, S^c)}{k|S|}, \tag{3.15}$$

где  $e(S, S^c)$  – число ребер между  $S$  и дополнением  $S$ . Нам нужен результат из [5] (более компактная версия – [8; теорема 4.1]).

ТЕОРЕМА 8. Пусть  $P$  – эргодическая цепь Маркова на графе  $G = G(V, E)$ . Рассмотрим ленивую цепь  $X_0, X_1, \dots, X_n, \dots$  с матрицей переходов  $(I+P)/2$ , начиная с некоторого определенного  $X_0$ . Тогда для любого  $c > 0$  и любого  $n = ch(G)^{-2} \log |V|$  имеем

$$\max_{A \subseteq V} \left| P(X_n \in A) - \frac{|A|}{|V|} \right| \leq e^{-Kc},$$

где  $K > 0$  – абсолютная константа.

В нашем случае  $G = G(V, E)$  с  $V = \mathbb{F}_p^*$  и  $x \rightarrow y$  тогда и только тогда, когда  $y = f_*(x)\gamma^{\pm 1}$ . Таким образом, наша задача состоит в оценке константы Чигера  $G$ . Берем любое  $S$ ,  $|S| \leq p/2$ , и запишем  $S$  как дизъюнктное объединение  $S = \bigsqcup_{j \in J} G_j$ , где  $G_j$  – геометрические прогрессии с шагом  $\gamma^2$ . Здесь и далее мы используем факт, что группа  $\mathbb{F}_p^*$  циклическая, изоморфна  $\mathbb{Z}/(p-1)\mathbb{Z}$  и порождена фиксированным первообразным корнем  $g$ . Рассмотрим  $z, z\gamma, z\gamma^2$ , где  $z \in S$  – правая конечная точка (если она существует) некоторого  $G_j$ . Тогда  $z\gamma^2 \in S^c$  и  $z, z\gamma^2$  смежны с  $f_*^{-1}(z\gamma)$ . Вершина  $f_*^{-1}(z\gamma)$  принадлежит  $S$  или  $S^c$ , но в любом из этих случаев мы имеем ребро между  $S$  и  $S^c$ . Пусть  $J = J_0 \sqcup J_1$ , где для  $j \in J_0$  множество  $G_j$  не имеет правого конца и  $J_1 = J \setminus J_0$ . Ясно, что  $|J_0| \leq 2|S|/\text{ord}(\gamma)$ . По приведенным выше рассуждениям

$$\frac{|J_1|}{|S|} \geq \frac{|J|}{|S|} - \frac{2}{\text{ord}(\gamma)}. \tag{3.16}$$

Мы хотим получить другую нижнюю оценку для  $h(G)$ , которая работает лучше в случае, когда  $J$  мало. Положим  $L = |S|/|J|$ , и пусть  $\omega \in (0, 1)$  – некоторый малый параметр, который мы выберем позже. Имеем  $\sum_{j \in J} |G_j| = |S|$  и, таким образом,  $\sum_{j: |G_j| \geq \omega L} |G_j| \geq (1 - \omega)|S|$ . Разбивая  $G_j$  на интервалы длины  $L_\omega := \omega L/2$ , мы видим, что оставшаяся часть не более  $2\omega|S|$ . Таким образом, мы получили некоторые геометрические прогрессии  $G'_i$ ,  $i \in I$ , имеющие длины  $L_\omega$  и шаг  $\gamma^2$  такие, что  $\sum_{i \in I} |G'_i| \geq (1 - 2\omega)|S|$ . Положим  $S' = \bigsqcup_{i \in I} G'_i$ , и пусть  $\Omega = S \setminus S'$ ,  $|\Omega| \leq 2\omega|S|$ . Другими словами, мы имеем  $S' = XY$ ,  $|S'| = |X||Y| \geq (1 - 2\omega)|S|$ , где  $X = [1, \gamma^2, \dots, \gamma^{2(L_\omega - 1)}]$  и  $Y$  – некоторое множество мультипликативных сдвигов. Ясно, что

$$\frac{e(S, S^c)}{|S|} \geq 1 - \frac{e(S, S)}{|S|} \geq 1 - 8\omega - \frac{e(S', S')}{|S|}. \tag{3.17}$$

Положим  $Z = [1, \gamma^2, \dots, \gamma^{2(L'_\omega - 1)}]$ , где величина  $\delta$  определена как  $L'_\omega = \lceil p^\delta \rceil$ , и пусть

$$m \leq \frac{cL_\omega}{M}, \tag{3.18}$$

где  $c = 1/8$  и  $M \geq 2/\delta$ . Тогда  $|XZ^M|/|X| \leq 1 + 2c$ . Также по предположению элемент  $\gamma$  имеет порядок не менее  $\exp(\Omega(\log p \cdot \log \log \log p / \log \log p))$ . Используя теорему 6 с  $K = 1 + 2c$ ,  $M \sim 1/\delta$  и принимая  $\delta \geq C \log \log \log p / \log \log p$  для достаточно большой константы  $C > 0$ , получим

$$\frac{e(S', S')}{|S|} - \frac{25|S'|}{16p} \ll p^{-\delta^{O(1/\delta)}} \leq \frac{1}{32}.$$

Вспоминая, что  $|S'| \leq |S| \leq p/2$ , находим

$$\frac{e(S', S')}{|S|} \leq \frac{25|S'|}{16p} + \frac{1}{32} \leq \frac{25}{32} + \frac{1}{32} = \frac{13}{16}.$$

Подставляя последнюю формулу в (3.17), выбирая достаточно большое  $p$  и полагая, скажем,  $\omega = 2^{-8}$ , имеем  $h(G) \geq 1/32$ . Необходимо проверить условие (3.18). Если условие не выполняется, то

$$\frac{|S|}{|J|} = L\delta^{-1} \ll L_\omega\delta^{-1} \ll |Z| \leq p^\delta \sim \exp\left(O\left(\frac{\log p \cdot \log \log \log p}{\log \log p}\right)\right),$$

и в этом случае  $|J| \gg |S| \exp(-O(\log p \cdot \log \log \log p / \log \log p))$ . Но тогда по (3.16) и нашему предположению  $\text{ord}(\gamma) = \exp(\Omega(\log p \cdot \log \log \log p / \log \log p))$ , и мы видим, что в любом случае  $h(G) \gg \exp(-O(\log p \cdot \log \log \log p / \log \log p))$ . Сопоставляя последнюю оценку для константы Чигера и теорему 8, получаем

$$n \leq \exp\left(O\left(\frac{\log p \cdot \log \log \log p}{\log \log p}\right)\right).$$

Последняя часть теоремы 7 получается таким же методом, если добавить к нему рассуждения из [4] и [8; п. 4.3]. Нужно убедиться, что биекция  $f_*(f_*^{-1}(\cdot)\gamma): \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$  имеет тот же вид, что и в (1.4) (конечно, учитывая, что, как обычно,  $f_*(-\beta/\alpha) = 1/\alpha$ ). Это можно проверить непосредственными вычислениями или использовать то, что  $f_*$  соответствует стандартному действию нижнетреугольной матрицы из  $\text{GL}_2(\mathbb{F}_p)$ . Теорема 7 доказана.

**ЗАМЕЧАНИЕ 2.** Рассмотрим ленивую марковскую цепь (1.2) с  $f(x) = x^2$  и  $p \equiv 3 \pmod{4}$ ,  $\varepsilon_i$  – независимые случайные величины, равномерно распределенные на  $\pm\gamma$ ,  $\gamma \in \mathbb{F}_p^*$  и  $p$  – достаточно большое простое число. Используя те же рассуждения, что и в доказательстве теоремы 7, мы приходим к уравнениям  $y + a = f(x + b) = x^2 + 2bx + b^2$ , где  $a, b$  принадлежат некоторой арифметической прогрессии  $P$  и  $x, y$  из дизъюнктного объединения  $J$  арифметических прогрессий (детали доказательства могут быть найдены в [8]). Строго говоря, теперь стационарное распределение  $\pi$  не равномерно и задается формулой

$$\pi(\alpha) = (2p)^{-1} |\{\beta \in \mathbb{F}_p : \beta^2 \pm \gamma = \alpha\}|,$$

сходимость и, значит,  $t_{\text{mix}}$  определяются относительно  $\pi(\cdot)$  и, более того, соответствующий граф уже будет нерегулярным, что приведет к изменению определения (3.15) (см. подробное обсуждение данных обстоятельств в [8; п. 2.1]). Тем не менее легко показать, что

$$t_{\text{mix}} = O(p \log p). \quad (3.19)$$

*Набросок доказательства (3.19).* Как и в доказательстве теоремы 7, выберем  $S$ ,  $|S| \leq p/2$ , определим граф  $G = G(V, E)$ ,  $x \rightarrow y$  тогда и только тогда, когда  $y = x^2 \pm \gamma$ , и далее определим множества и числа  $G_j, J, L, S' = P + Y$ ,  $|P| \gg L$ , как ранее. Как было рассмотрено выше, мы получаем уравнение  $y + a = x^2 + 2bx + b^2$ ,  $a, b \in P$ ,  $x, y \in S'$ , и это уравнение может быть интерпретировано как вопрос об инцидентях множества прямых  $\mathcal{L}$  вида  $Y = 2bX + (b^2 - a)$

и множества точек  $\mathcal{P} = (y - x^2, x)$ . Имеем  $|\mathcal{L}| = |P|^2$  и  $|\mathcal{P}| = |S'|^2$ . Используя основной результат из [33] (также, см. [26]), получаем

$$\left| \mathcal{I}(\mathcal{P}, \mathcal{L}) - \frac{|\mathcal{P}| |\mathcal{L}|}{p} \right| \leq \sqrt{|\mathcal{P}| |\mathcal{L}| p}. \tag{3.20}$$

По формуле (3.20) и вычислениям, как выше (см. подробности в [8; п. 4.2]), наш граф образует экспандер, если  $|S|/J \sim |P| \gg \sqrt{p}$ . Действительно, в этом случае

$$\frac{e(S', S')}{|S|} \leq \frac{|S'|^2}{p|S|} + |P|^{-2} |S|^{-1} \sqrt{|\mathcal{P}| |\mathcal{L}| p} \leq \frac{1}{2} + \sqrt{p|P|^{-2}} \leq 1 - c$$

для некоторого  $c > 0$ . Наконец, если, наоборот,  $J \gg |S|/\sqrt{p}$ , тогда по формуле, аналогичной (3.16), получим  $h(G) \gg 1/\sqrt{p}$ . Таким образом, в силу теоремы 8 мы видим, что время перемешивания  $O(p \log p)$ , как и требовалось.

Метод доказательства теоремы 7 (см. также замечание 2) позволяет легко получить ленивые цепи Маркова на  $\mathbb{F}_p^*$  с временем перемешивания  $O(p \log p)$ , например,

$$X_{j+1} = \begin{cases} \text{ind}(X_j) \cdot \varepsilon_{j+1} & \text{с вероятностью } \frac{1}{2}, \\ X_j & \text{с вероятностью } \frac{1}{2} \end{cases} \tag{3.21}$$

( $X_0 \neq 0$ ) или, как в (1.2) с  $f(x) = \exp(x)$ , а именно,

$$X_{j+1} = \begin{cases} \exp(X_j) + \varepsilon_{j+1} & \text{с вероятностью } \frac{1}{2}, \\ X_j & \text{с вероятностью } \frac{1}{2}. \end{cases} \tag{3.22}$$

(как всегда  $\varepsilon_i$  обозначают независимые случайные величины, распределенные равномерно на  $\pm\gamma$ ,  $\gamma \in \mathbb{F}_p^*$ ). Действительно, в первой цепи мы приходим к уравнению  $ya = \text{ind}(x) + \text{ind}(b)$ , а во второй к  $y + b = \exp(x) \cdot \exp(a)$ . Оба уравнения соответствуют инциденциям точек и прямых. Заметим еще раз, что наша функция  $\text{ind}(x)$  определена на  $\mathbb{F}_p^*$ , но не на  $\mathbb{F}_p$  (опять, для аддитивной цепи Маркова можно доопределить функцию  $\exp(x)$  как  $\exp(0) = 0$  и получить биекцию), но в действительности два значения  $\exp(0)$ ,  $\text{ind}(0)$  привносят пренебрежимую величину ошибки в инциденции. В любом случае имеется намного более лучшая оценка для времени перемешивания двух цепей Маркова, приведенных выше.

**ТЕОРЕМА 9.** Пусть  $p$  – достаточно большое простое число,  $\gamma \in \mathbb{F}_p^*$ . Тогда время перемешивания цепи Маркова (3.22) есть  $\exp(O(\log p \cdot \log \log \log p / \log \log p))$ . Если дополнительно порядок  $\gamma$  равен  $\exp(\Omega(\log p \cdot \log \log \log p / \log \log p))$ , то время перемешивания цепи Маркова (3.21) есть  $\exp(O(\log p \cdot \log \log \log p / \log \log p))$ .

**ДОКАЗАТЕЛЬСТВО.** Наши рассуждения следуют той же схеме, что и доказательства теоремы 6 и теоремы 7. В обоих случаях нужно оценить энергию  $T_{2^k}$  множества аффинных преобразований  $L$  вида  $x \rightarrow gx + s$ , где коэффициенты

$g \in \Gamma = a \cdot \{1, \gamma, \dots, \gamma^n\}$  и  $s \in P$  принадлежат геометрической и арифметической прогрессиям размера  $n = \sqrt{|L|}$  соответственно. В силу предложения 1 можно оценить требуемое число инцидентов уравнения  $y = gx + s$ ,  $g \in \Gamma$ ,  $s \in P$ . Ниже мы можем предположить, что  $P, \Gamma$  достаточно малы (но больше чем  $\exp(\Omega(\log p \cdot \log \log \log p / \log \log p))$ , конечно). Дальнейшее применение леммы 3 бесполезно, так как  $\Gamma_{2^k}^+(P)$  максимально. Тем не менее мы делаем дополнительный шаг, рассматривая множество  $L^{-1}L$ , и замечаем, что любой элемент  $L^{-1}L$  имеет вид  $x \rightarrow g_2/g_1x + (s_2 - s_1)/g_1$ , где  $g_1, g_2 \in \Gamma$ ,  $s_1, s_2 \in P$ . Теперь в силу рассуждений из леммы 3 наша задача – получить оценку  $|\Gamma|^{2^{k+1}-1} \Gamma_{2^k}^+(f_{(P-P)/\Gamma})$ . Запишем  $W = Q/\Gamma$ , где  $Q = P - P$ , и пусть  $\bar{Q} = Q + Q$ . Получим грубую нижнюю оценку  $|W|$ , а именно,  $|W| \gg n^{3/2}$ . Действительно, можно использовать неравенство

$$E^\times(P, \Gamma) \leq n^{-2} \left| \left\{ (g_1, g_2, q_1, q_2, \bar{q}_1, \bar{q}_2) \in \Gamma^2 \times Q^2 \times \bar{Q}^2 : (\bar{q}_1 - q_1)g_1 = (\bar{q}_2 - q_2)g_2 \right\} \right|$$

и, таким образом, для малых  $P, \Gamma$  выполняется  $E^\times(P, \Gamma) \ll n^{5/2}$  в силу теоремы Руднева (см. [21]). Действительно, последняя оценка влечет  $|W| \gg n^{3/2}$  в силу неравенства Коши–Шварца. Положим  $X = \{1, \gamma, \dots, \gamma^m\}^{-1} \subset \Gamma^{-1}$  и  $m = p^\delta$ . Пусть

$$\frac{4}{\delta} m \leq cn^{1/2} \quad (3.23)$$

для достаточно малого  $c > 0$ , и если это так, то мы видим, что для любого целого  $M \leq 4/\delta$  выполняется

$$|WX^M| = \left| \frac{Q}{\Gamma \cdot X^M} \right| \leq |W| + Mnm = \frac{5|W|}{4}.$$

Применяя теорему 4 с  $k \leq 4/\delta$ , получим

$$\Gamma_{2^k}^+(f_{(P-P)/\Gamma}) \lesssim \log p \cdot (|P|^2|\Gamma|)^{2^{k+1}} p^{-\delta'(2^k-2)}.$$

Опять, выбираем  $k$  такое, что  $\delta'(2^k - 2) \gg 1$ . Тогда, рассуждая, как в лемме 3, получим

$$\Gamma_{2^{k+1}}(f_L) \lesssim |\Gamma|^{2^{k+1}-1} 2^{2r} \log p \cdot (|P|^2|\Gamma|)^{2^{k+1}} p^{-\delta'(2^k-2)} \ll |L|^{2^{k+2}} p^{-\delta'(2^k-2)}.$$

После этого мы применяем те же рассуждения, что и в доказательстве теоремы 7. Наконец, чтобы выполнить (3.23), выбираем  $\delta \sim \log \log \log p / \log \log p$  и вспоминаем наше условие  $\exp(\Omega(\log p \cdot \log \log \log p / \log \log p))$ . Теорема доказана.

#### § 4. Комбинаторные применения

Применим разработанную технику к множествам Сидона, следуя схеме из [28]. Нам понадобятся лемма 3, лемма 7 и теорема 4.

**ЛЕММА 4.** Пусть  $A \subseteq \mathbf{G}$  – произвольное множество. Тогда для любого  $k \geq 2$  имеем

$$\text{Sid}_{3k-3}(A) \gg \left( \frac{|A|^{2k}}{\bar{E}_k(A)} \right)^{1/(2k-1)}, \quad \text{Sid}_{2k-2}(A) \gg \left( \frac{|A|^{2k}}{\bar{E}_k(A)} \right)^{1/(2k-1)}. \quad (4.1)$$



ЛЕММА 5. Пусть  $A \subseteq \mathbf{G}$  – произвольное множество,  $A = B + C$  и  $k \geq 1$  – целое число. Тогда

$$\text{Sid}_k(A) \leq \min \left\{ |C| \sqrt{k|B|} + |B|, |B| \sqrt{k|C|} + |C| \right\}.$$

ТЕОРЕМА 10. Пусть  $A \subseteq \mathbf{G}$  – произвольное множество,  $\delta, \varepsilon \in (0, 1]$  – параметры,  $\varepsilon \leq \delta$ .

1) Тогда существует  $k = k(\delta, \varepsilon) = \exp(O(\varepsilon^{-1} \log(1/\delta)))$  такое, что либо  $E_k(A) \leq |A|^{k+\delta}$ , либо же найдутся  $H \subseteq \mathbf{G}$ ,  $|H| \gtrsim |A|^{\delta(1-\varepsilon)}$ ,  $|H + H| \ll |A|^\varepsilon |H|$ , и множество  $Z \subseteq \mathbf{G}$ ,  $|Z| |H| \ll |A|^{1+\varepsilon}$

$$|(H + Z) \cap A| \gg |A|^{1-\varepsilon}.$$

2) Аналогично, либо найдутся множества  $A' \subseteq A$ ,  $|A'| \gg |A|^{1-\varepsilon}$ , и  $P \subseteq \mathbf{G}$ ,  $|P| \gtrsim |A|^\delta$ , такие, что для всех  $x \in A'$  имеем  $r_{A-P}(x) \gg |P| |A|^{-\varepsilon}$ , либо же  $E_k(A) \leq |A|^{k+\delta}$  для  $k \ll 1/\varepsilon$ .

Для работы в вещественном случае нам потребуется известная теорема Семереди–Троттера (см. [31]).

ТЕОРЕМА 11. Пусть  $\mathcal{P}, \mathcal{L}$  – произвольные конечные множества точек и прямых в  $\mathbb{R}^2$ . Тогда

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) \ll (|\mathcal{P}| |\mathcal{L}|)^{2/3} + |\mathcal{P}| + |\mathcal{L}|.$$

Теперь мы готовы доказать теорему 2. Возьмем любое  $\delta < 1/2$ , например,  $\delta = 1/4$ , и пусть  $\varepsilon \leq \delta/4$  – некоторый параметр, который мы выберем позже. В силу леммы 4 мы видим, что неравенство  $E_k^\times(A) \leq |A|^{k+\delta}$  влечет

$$\text{Sid}_{3k-3}^\times(A) \gg |A|^{1/2+(1-2\delta)/(2(2k-1))} = |A|^{1/2+1/(4(2k-1))}, \quad (4.2)$$

и мы получаем требуемое. Здесь  $k = k(\varepsilon)$ . Иначе существует  $H \subseteq \mathbb{F}$ ,  $|H| \gtrsim |A|^{\delta(1-\varepsilon)} \geq |A|^{\delta/2}$ ,  $|HH| \ll |A|^\varepsilon |H|$ , и существует  $Z \subseteq \mathbb{F}$ ,  $|Z| |H| \ll |A|^{1+\varepsilon}$ , с  $|(HZ) \cap A| \gg |A|^{1-\varepsilon}$ . Здесь произведение  $H$  и  $Z$  прямое, т.е.  $h_1 z_1 = h_2 z_2$  для  $h_1, h_2 \in H$ ,  $z_1, z_2 \in Z$  влечет  $h_1 = h_2$  и  $z_1 = z_2$ . Положим  $A_* = (HZ) \cap A$ ,  $|A_*| \gg |A|^{1-\varepsilon}$ , и мы хотим оценить  $E_{l+1}^\times(A_* + 1)$  или же  $\widehat{E}_{l+1}^\times(A_* + 1)$  для большого  $l$ . После этого, имея хорошую верхнюю оценку для  $E_{l+1}^\times(A_* + 1)$  или  $\widehat{E}_{l+1}^\times(A_* + 1)$ , применим лемму 4 еще раз для нахождения большого мультипликативного подмножества Сидона в  $A_*$ .

Во-первых, заметим, что в силу (2.1) мы имеем

$$|HA_*^{-1}| \leq |HH^{-1}| |Z| \ll |A|^{2\varepsilon} |H| |Z| \ll |A|^{1+3\varepsilon}.$$

Другими словами, множество  $A_*^{-1}$  почти не растет после умножения на  $H$ . Пусть  $Q = HA_*^{-1}$ ,  $|Q| \ll |A|^{1+3\varepsilon}$ , и также пусть  $M = |A|^\varepsilon$ . Во-вторых, фиксируем произвольное  $\lambda \neq 0, 1$ . Количество решений уравнения  $a_1/a_2 = \lambda$ , где  $a_1, a_2 \in A_* + 1$ , не превосходит

$$\sigma_\lambda := |H|^{-2r} \left| \left\{ h_1, h_2 \in H, q_1, q_2 \in Q: \frac{h_1/q_1 + 1}{h_2/q_2 + 1} = \lambda \right\} \right|.$$

Последнее уравнение имеет вид (3.10), а именно

$$\frac{h_1}{q_1} - \frac{\lambda h_2}{q_2} = \lambda - 1,$$

и оно может быть интерпретировано как вопрос о числе инцидентий точек и прямых. Для каждого  $\lambda \neq 0, 1$  величина  $\sigma_\lambda$  может быть оценена как

$$\sigma_\lambda \ll |H|^{-2} \cdot |Q| |H|^{2-\kappa} \ll |A|^{1+3\varepsilon} |H|^{-\kappa} \quad (4.3)$$

так же, как и в доказательстве теоремы 6 выше (в случае  $\mathbb{F} = \mathbb{R}$  то же самое верно в силу теоремы 11). Здесь  $\kappa = \kappa(\delta) > 0$ . Действительно, по нашему предположению  $|A| < \sqrt{p}$ , а также по теореме 5, предположению 1 и лемме 3 мы находим

$$\sigma_\lambda - \frac{|Q|^2}{p} \lesssim |Q| |H|^{-1/2} (|Q| \mathbb{T}_{2r}^+(H))^{1/2r+2} \lesssim |Q| \sqrt{M} (M^3 |A| |H|^{-(r+1)/2})^{1/2r+2}, \quad (4.4)$$

поскольку еще  $|H| \gtrsim_r M^{2r+1}$  и  $|H|^{r+1} \ll p$ . Здесь  $r$  – некоторый параметр и мы выбираем  $r \sim 1/\delta$  для выполнения второго условия. Для выполнения первого условия просто возьмем  $\varepsilon 2^{r+1} \ll \delta$  (другими словами,  $\varepsilon \leq \exp(-\Omega(1/\delta))$ ) и получим требуемое, ибо  $|H| \gg |A|^{\delta/2}$ .

Далее, используя  $|H| \gg |A|^{\delta/2}$ ,  $|A_*| \gg |A|^{1-\varepsilon}$ , оценку (4.3) и выбирая любое  $\varepsilon \leq \delta\kappa/100$ , получаем после вычислений, что  $\sigma_\lambda \ll |A_*|^{1-\delta\kappa/4}$ . Теперь, взяв достаточно большое  $l \gg (\delta\kappa)^{-1}$ , получаем

$$\begin{aligned} \widehat{\mathbb{E}}_{l+1}^\times(A_*) &= \sum_\lambda r_{A_* A_*}^{l+1}(\lambda) \ll |A_*|^{l+1} + (|A_*|^{1-\delta\kappa/2})^l |A_*|^2 \\ &\ll |A_*|^{l+1} + |A|^{l+2-\delta\kappa l/2} \ll |A_*|^{l+1}. \end{aligned}$$

Применяя лемму 4 и выбирая  $\varepsilon \ll l^{-1}$ , мы видим, что

$$\begin{aligned} \text{Sid}_{2l}^\times(A) &\geq \text{Sid}_{2l}^\times(A_*) \gg |A_*|^{(l+1)/(2l+1)} \gg |A|^{((1-\varepsilon)(l+1))/(2l+1)} \\ &= |A|^{1/2+(1-2\varepsilon(l+1))/(2(2l+1))} \gg |A|^{1/2+c}, \end{aligned}$$

где  $c = c(\delta) > 0$  – абсолютная константа. Мы получили неравенство (1.8) теоремы 2.

Для получения оценки (1.10) мы используем те же рассуждения, что и выше, но теперь наш аналог величины  $\sigma_\lambda$  – это  $\exp(q_1) \exp(h_1) - \exp(q_2) \exp(h_2) = \lambda$ , где  $q_1, q_2 \in Q = A_* + H$ ,  $h_1, h_2 \in H$ . Последнее уравнение может быть рассмотрено как вопрос об инцидентиях множества прямых  $x \exp(h_1) - y \exp(h_2) = \lambda$ ,  $|\mathcal{L}| = |H|^2$  и соответствующего множества точек  $\mathcal{P}$  размера  $|Q|^2$ . Тогда аналогии оценок (4.3), (4.4) верны и результат получен.

Осталось доказать оценку (1.11) теоремы. Для любых множества  $X_1, X_2, X_3$  рассмотрим множество  $R[X_1, X_2, X_3]$

$$R[X_1, X_2, X_3] = \left\{ \frac{x_1 - x_3}{x_2 - x_3} : x_1, x_2, x_3 \in X, x_2 \neq x_3 \right\}.$$

Если  $X_1 = X_2 = X_3 = X$ , то мы полагаем  $R[X_1, X_2, X_3] = R[X]$ . Можно проверить, что  $1 - R[X_1, X_2, X_3] = R[X_1, X_3, X_2]$ . Для  $\mathbb{F} = \mathbb{R}$  или  $\mathbb{F} = \mathbb{F}_p$

возьмем  $X = P$ ,  $A = R[X]$ , где  $P = \{1, \dots, n\}$ ,  $\bar{P} = \{-n, \dots, n\}$ , и пусть  $n < \sqrt{p}$  в случае  $\mathbb{F}_p$ . Тогда  $A$  содержится в  $\bar{P}/\bar{P} := B \cdot C$  и в силу леммы 5 любое мультипликативное  $k$ -сидоновское подмножество  $A$  имеет размер не более  $O(\sqrt{k}|A|^{3/4})$ , потому что, как можно проверить,  $|A| \gg |P|^2$ . Далее,  $1 - A = A$  и, таким образом, те же рассуждения применимы к множеству  $1 - A$ . Осталось заметить, что  $\text{Sid}^\times(X) = \text{Sid}^\times(-X)$  для любого множества  $X$ . Наконец, заметим, что существует альтернативный (но, возможно, немного более сложный) способ получить оценку (1.11). Действительно, рассмотрим  $R[\Gamma]$ , где  $\Gamma \subseteq \mathbb{F}_p^*$ ,  $|\Gamma| < \sqrt{p}$  – мультипликативная подгруппа (мы рассматриваем случай  $\mathbb{F} = \mathbb{F}_p$ ). Можно заметить, что  $R[\Gamma] = (\Gamma - 1)/(\Gamma - 1)$  и повторить те же рассуждения, что и выше.

Посвящается академику А. Н. Паршину.

### Список литературы

- [1] C. Ascì, “Generating uniform random vectors”, *J. Theoret. Probab.*, **14**:2 (2001), 333–356.
- [2] J. Bourgain, “Multilinear exponential sums in prime fields under optimal entropy condition on the sources”, *Geom. Funct. Anal.*, **18**:5 (2009), 1477–1502.
- [3] J. Bourgain, A. Gamburd, “Uniform expansion bounds for Cayley graphs of  $\text{SL}_2(\mathbb{F}_p)$ ”, *Ann. of Math. (2)*, **167**:2 (2008), 625–642.
- [4] S. Chatterjee, P. Diaconis, “Speeding up Markov chains with deterministic jumps”, *Probab. Theory Related Fields*, **178**:3-4 (2020), 1193–1214.
- [5] Fan Chung, “Laplacians and the Cheeger inequality for directed graphs”, *Ann. Comb.*, **9**:1 (2005), 1–19.
- [6] F. R. K. Chung, P. Diaconis, R. L. Graham, “Random walks arising in random number generation”, *Ann. Probab.*, **15**:3 (1987), 1148–1165.
- [7] S. Eberhard, P. P. Varjú, “Mixing time of the Chung–Diaconis–Graham random process”, *Probab. Theory Related Fields*, **179**:1-2 (2021), 317–344.
- [8] J. He, “Markov chains on finite fields with deterministic jumps”, *Electron. J. Probab.*, **27** (2022), 28, 17 pp.
- [9] J. He, Huy Tuan Pham, Max Wenqiang Xu, “Mixing time of fractional random walk on finite fields”, *Electron. J. Probab.*, **27** (2022), 133, 15 pp.
- [10] M. Hildebrand, “A lower bound for the Chung–Diaconis–Graham random process”, *Proc. Amer. Math. Soc.*, **137**:4 (2009), 1479–1487.
- [11] M. Hildebrand, “Random processes of the form  $X_{n+1} = a_n X_n + b_n \pmod{p}$  where  $b_n$  takes on a single value”, *Random discrete structures* (Minneapolis, MN, 1993), IMA Vol. Math. Appl., **76**, Springer, New York, 153–174.
- [12] M. Hildebrand, “Random processes of the form  $X_{n+1} = a_n X_n + b_n \pmod{p}$ ”, *Ann. Probab.*, **21**:2 (1993), 710–720.
- [13] C. Pohoata, *Sidon sets and sum-product phenomena*, <https://pohoatza.wordpress.com/2021/01/23/sidon-sets-and-sum-product-phenomena/>.
- [14] J. Komlós, M. Sulyok, E. Szemerédi, “Linear problems in combinatorial number theory”, *Acta Math. Acad. Sci. Hungar.*, **26**:1-2 (1975), 113–121.
- [15] И. А. Круглов, “Случайные последовательности вида  $X_{t+1} = a_t X_t + b_t \pmod{n}$  с зависимыми коэффициентами  $a_t, b_t$ ”, *Дискрет. матем.*, **17**:2 (2005), 49–55; англ. пер.: I. A. Kruglov, “Random sequences of the form  $X_{t+1} = a_t X_t + b_t \pmod{n}$  with dependent coefficients  $a_t, b_t$ ”, *Discrete Math. Appl.*, **15**:2 (2005), 145–151.
- [16] D. A. Levin, Y. Peres, *Markov chains and mixing times*, 2nd ed., Amer. Math. Soc., Providence, RI, 2017, xvi+447 pp.

- [17] B. Murphy, “Upper and lower bounds for rich lines in grids”, *Amer. J. Math.*, **143**:2 (2021), 577–611.
- [18] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, I. D. Shkredov, “New results on sum–product type growth over fields”, *Mathematika*, **65**:3 (2019), 588–642.
- [19] K. O’Bryant, “A complete annotated bibliography of work related to Sidon sequences”, *Electron. J. Combin.*, 2004, Dynamic Surveys, DS11, 39 pp.
- [20] O. Roche-Newton, A. Warren, “Additive and multiplicative Sidon sets”, *Acta Math. Hungar.*, **165**:2 (2021), 326–336.
- [21] M. Rudnev, “On the number of incidences between points and planes in three dimensions”, *Combinatorica*, **38**:1 (2018), 219–254.
- [22] M. Rudnev, I. D. Shkredov, “On the growth rate in  $SL_2(\mathbb{F}_p)$ , the affine group and sum–product type implications”, *Mathematika*, **68**:3 (2022), 738–783.
- [23] T. Schoen, I. D. Shkredov, “Higher moments of convolutions”, *J. Number Theory*, **133**:5 (2013), 1693–1737.
- [24] А. С. Семченков, “Максимальные подмножества без арифметических прогрессий в произвольных множествах”, *Матем. заметки*, **102**:3 (2017), 436–444; англ. пер.: A. S. Semchenkov, “Maximal subsets free of arithmetic progressions in arbitrary sets”, *Math. Notes*, **102**:3 (2017), 396–402.
- [25] I. D. Shkredov, “Some remarks on the asymmetric sum–product phenomenon”, *Mosc. J. Comb. Number Theory*, **8**:1 (2019), 15–41.
- [26] И. Д. Шкредов, “Об асимптотических формулах в некоторых вопросах теории сумм произведений”, Тр. ММО, **79**, № 2, МЦНМО, М., 2018, 271–334; англ. пер.: I. D. Shkredov, “On asymptotic formulae in some sum–product questions”, *Trans. Moscow Math. Soc.*, **2018** (2018), 231–281.
- [27] I. D. Shkredov, “Modular hyperbolas and bilinear forms of Kloosterman sums”, *J. Number Theory*, **220** (2021), 182–211.
- [28] I. D. Shkredov, “On an application of higher energies to Sidon sets”, *Combinatorica*, 2023, Publ. online.
- [29] S. Sidon, “Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen”, *Math. Ann.*, **106**:1 (1932), 536–539.
- [30] S. Stevens, F. de Zeeuw, “An improved point-line incidence bound over arbitrary fields”, *Bull. Lond. Math. Soc.*, **49**:5 (2017), 842–858.
- [31] E. Szemerédi, W. T. Trotter, Jr., “Extremal problems in discrete geometry”, *Combinatorica*, **3**:3-4 (1983), 381–392.
- [32] T. Tao, Van H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006, xviii+512 pp.
- [33] L. A. Vinh, “The Szemerédi–Trotter type theorem and the sum–product estimate in finite fields”, *European J. Combin.*, **32**:8 (2011), 1177–1181.
- [34] A. Warren, *Additive and multiplicative Sidon sets*, Report at CANT–2021, <http://www.theoryofnumbers.com/cant/CANT2021-abstracts.pdf>.

Илья Дмитриевич Шкредов  
(Илья D. Shkredov)

Математический институт им. В. А. Стеклова  
Российской академии наук, г. Москва  
E-mail: [ilya.shkredov@gmail.com](mailto:ilya.shkredov@gmail.com)

Поступила в редакцию  
13.07.2022 и 09.11.2022