Неархимедова динамика, компьютеры и криптография

В. С. Анашин

Московский государственный университет
им. М. В. Ломоносова

10-адические числа

- 9

10-адические числа

- 9
- 99

10-адические числа

- 9
- 99
- 999

10-адические числа

- 9
- 99
- 999
- . . . . . .

10-адические числа

- 9
- 99
- 999
- . . . . . .
- . . . 9999

10-адические числа

- 9
- 99
- 999
- .....
- ...9999

10-адические числа — это всевозможные бесконечные последовательности цифр 0,1,2,...,9

10-адическая арифметика

10-адические числа можно складывать и умножать "в столбик"

10-адическая арифметика

10-адические числа можно складывать и умножать "в столбик"

$$
\begin{array}{rcccc}
 & \ldots 1 & 2 & 7 & 1 \\
+ & & & & \\
 & \ldots 8 & 4 & 0 & 9 \\
\hline
 & \ldots 9 & 6 & 8 & 0
\end{array}
$$

10-адическая арифметика

$$
\begin{array}{rcccc}
 & \ldots 9 & 9 & 9 & 9 \\
+ & & & & \\
 & \ldots 0 & 0 & 0 & 1 \\
\hline
 & \ldots 0 & 0 & 0 & 0
\end{array}
$$

Значит, $\ldots 9999 = -1$.

10-адическая арифметика

$$
\begin{array}{rcccc}
 & \ldots 3 & 3 & 3 & 3 \\
\times & & & & \\
 & \ldots 0 & 0 & 0 & 3 \\
\hline
 & \ldots 9 & 9 & 9 & 9
\end{array}
$$

Значит, $\ldots 3333 = -\frac{1}{3}$.

10-адическая арифметика

Получается, что

- 9, 99, 999,…"сходится"к -1
- 3, 33, 333,…"сходится"к $-\frac{1}{3}$

10-адическая арифметика

Получается, что

- 9, 99, 999,…"сходится"к -1
- 3, 33, 333,…"сходится"к $-\frac{1}{3}$

В каком смысле "сходится"?

10-адическая арифметика

Получается, что

- 9, 99, 999,…"сходится"к -1
- 3, 33, 333,…"сходится"к $-\frac{1}{3}$

В каком смысле "сходится"?

Последовательность чисел a_n, $n = 0, 1, 2, \ldots$, сходится к a, если для любого $\varepsilon > 0$ найдется N такое, что

$$|a_n - a| < \varepsilon$$

как только $n > N$. *Наша "сходимость"явно НЕ такая!!!*

Целые p-адические числа

Фиксируем простое число p и рассмотрим множество $\mathbb{Z}_p$ всех бесконечных строчек $\ldots \alpha_2 \alpha_1 \alpha_0$, где $\alpha_i \in \{0, 1, \ldots, p-1\}$, и зададим на $\mathbb{Z}_p$ операции сложения и умножения с помощью алгоритмов сложения и умножения "в столбик"для чисел, представленных в системе счисления с основанием p.

Целые p-адические числа

Фиксируем простое число p и рассмотрим множество $\mathbb{Z}_p$ всех бесконечных строчек $\ldots \alpha_2\alpha_1\alpha_0$, где $\alpha_i \in \{0, 1, \ldots, p-1\}$, и зададим на $\mathbb{Z}_p$ операции сложения и умножения с помощью алгоритмов сложения и умножения "в столбик"для чисел, представленных в системе счисления с основанием p. Множество $\mathbb{Z}_p$ с так определенными операциями сложения и умножения называется *кольцом целых p-адических чисел.*

Целые p-адические числа

Фиксируем простое число p и рассмотрим множество $\mathbb{Z}_p$ всех бесконечных строчек $\ldots\alpha_2\alpha_1\alpha_0$, где $\alpha_i \in \{0, 1, \ldots, p-1\}$, и зададим на $\mathbb{Z}_p$ операции сложения и умножения с помощью алгоритмов сложения и умножения "в столбик"для чисел, представленных в системе счисления с основанием p.
Множество $\mathbb{Z}_p$ с так определенными операциями сложения и умножения называется *кольцом целых p-адических чисел.*
В частности, $\mathbb{Z}_2$, кольцо целых 2-адических чисел — это множество всех бесконечных бинарных строк с обычными операциями сложения и умножения чисел в двоичной системе.

Кольцо $\mathbb{Z}_2$

Этот пример показывает, что $\ldots 11111 = -1$ в $\mathbb{Z}_2$.

$$
\begin{array}{cccccc}
 & \ldots 1 & 1 & 1 & 1 \\
+ & & & & \\
 & \ldots 0 & 0 & 0 & 1 \\
\hline
 & \ldots 0 & 0 & 0 & 0
\end{array}
$$

Кольцо $\mathbb{Z}_2$

$$
\begin{array}{cccccc}
\ldots 0 & 1 & 0 & 1 & 0 & 1 \\
\times & & & & & \\
\ldots 0 & 0 & 0 & 0 & 1 & 1 \\
\hline
\ldots 0 & 1 & 0 & 1 & 0 & 1 \\
+ & & & & & \\
\ldots 1 & 0 & 1 & 0 & 1 & \\
\hline
\ldots 1 & 1 & 1 & 1 & 1 & 1
\end{array}
$$

Кольцо $\mathbb{Z}_2$

Значит,

$$\ldots 01010101 = -\frac{1}{3} \text{ в } \mathbb{Z}_2$$

Кольцо $\mathbb{Z}_2$

И эту арифметику прекрасно понимает даже калькулятор!

Кольцо $\mathbb{Z}_2$

Строчкам, в которых лишь конечное число единиц, соответствуют неотрицательные рациональные числа

$$\ldots 00011 = 3$$

$$3 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + \ldots$$

Кольцо $\mathbb{Z}_2$

Строчкам, в которых лишь конечное число нулей, соответствуют отрицательные рациональные числа

$$\ldots 111100 = -4$$

$$-4 = 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \ldots$$

Обратите внимание: $-4 = (-1) \cdot 2^2$

$$-1 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \ldots$$

Кольцо $\mathbb{Z}_2$

Периодическим (с какого-то места) строчкам соответствуют рациональные числа, которые могут быть представлены в виде несократимых дробей с *нечетными* знаменателями

$$\ldots 1010101 = -\frac{1}{3}$$

$$-\frac{1}{3} = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + \ldots$$

Кольцо $\mathbb{Z}_2$

Всем остальным строчкам (т.е. тем, которые НЕпериодичны НИ с какого места) НЕ соответствуют ни рациональные, ни действительные, ни комплексные числа

$$\ldots 100001000100101$$

Метрика на $\mathbb{Z}_2$

Определение 1. Пусть $M \neq \emptyset$, и пусть $d\colon M \times M \to \mathbb{R}_{\geq 0}$ — функция от двух переменных, определенная на M и принимающая значения во множеств неотрицательных действительных чисел. Функция d наз. *метрикой* (а M — *метрическим пространством*) если d удовлетворяет всем след. условиям:

1. Для любых $a, b \in M$: $d(a,b) = 0 \Longleftrightarrow a = b$.
2. Для любых $a, b \in M$: $d(a,b) = d(b,a)$.
3. Для любых $a, b, c \in M$: $d(a,b) \leq d(a,c) + d(c,b)$.

Например, множество $\mathbb{R}$ всех действительных чисел есть метрическое пространство с метрикой $d(a,b) = |a-b|$, где $|\cdot|$ — абсолютная величина.

Метрика на $\mathbb{Z}_2$

Будем считать, что расстояние $d_2(u,v)$ между строчка $u,v \in \mathbb{Z}_2$ равно $2^{-\ell}$, где ℓ есть длина наибольшего общего начального сегмента у u и v. Абсолютная величина (=*норма*) 2-адического целого числа есть расстояние от него до 0: $\|u\|_2 = d_2(u,0)$. Т.о., $d_2(u,v) = \|u-v\|_2$. Например,

$$\left.\begin{array}{l} \ldots 1010\mathbf{1}0\mathbf{1}0\mathbf{1} = -\dfrac{1}{3} \\ \ldots 0000\mathbf{0}0\mathbf{1}0\mathbf{1} = 5 \end{array}\right\} \Longrightarrow d_2\left(-\frac{1}{3}, 5\right) = \frac{1}{2^4} = \frac{1}{16}$$

Иными словами, $-\frac{1}{3} \equiv 5 \pmod{16}$; $-\frac{1}{3} \not\equiv 5 \pmod{32}$.

Метрика на $\mathbb{Z}_2$

Будем считать, что расстояние $d_2(u,v)$ между строчка $u,v \in \mathbb{Z}_2$ равно $2^{-\ell}$, где ℓ есть длина наибольшего общего начального сегмента у u и v. Абсолютная величина (=*норма*) 2-адического целого числа есть расстояние от него до 0: $\|u\|_2 = d_2(u,0)$. Т.о., $d_2(u,v) = \|u-v\|_2$. Нетрудно видеть, что метрика d_2 удовлетворяет более сильному условию, чем (3) из Определения 1:

$(3')$ Для всех $a,b,c \in \mathbb{Z}:\ d_2(a,b) \leq \max\{d_2(a,c), d_2(c,b)\}$.

Это условие наз. *сильным неравенством треугольника*, а удовлетворяющая ему метрика наз. *неархимедовой* метрикой, или *ультраметрикой*.

Метрика на $\mathbb{Z}_2$

Будем считать, что расстояние $d_2(u,v)$ между строчка $u, v \in \mathbb{Z}_2$ равно $2^{-\ell}$, где ℓ есть длина наибольшего общего начального сегмента у u и v. Абсолютная величина (=*норма*) 2-адического целого числа есть расстояние от него до 0: $\|u\|_2 = d_2(u,0)$. Т.о., $d_2(u,v) = \|u-v\|_2$. Нетрудно видеть, что метрика d_2 удовлетворяет более сильному условию, чем (3) из Определения 1:

$(3')$ Для всех $a, b, c \in \mathbb{Z}:\ d_2(a,b) \leq \max\{d_2(a,c), d_2(c,b)\}$.

Удивительно, но факт: При сложении отрезка с самим собой он может стать короче, чем был!

Метрика на $\mathbb{Z}_2$

Будем считать, что расстояние $d_2(u,v)$ между строчка $u,v \in \mathbb{Z}_2$ равно $2^{-\ell}$, где ℓ есть длина наибольшего общего начального сегмента у u и v. Абсолютная величина (=*норма*) 2-адического целого числа есть расстояние от него до 0: $\|u\|_2 = d_2(u,0)$. Т.о., $d_2(u,v) = \|u-v\|_2$. Нетрудно видеть, что метрика d_2 удовлетворяет более сильному условию, чем (3) из Определения 1:

$(3')$ Для всех $a,b,c \in \mathbb{Z}:\ d_2(a,b) \leq \max\{d_2(a,c), d_2(c,b)\}$.

Удивительно, но факт: Все треугольники равнобедренные! Каждая точка внутри окружности является ее центром!

Сходимость в $\mathbb{Z}_2$

Поскольку метрика на $\mathbb{Z}_2$ задана, можно говорить о сходящихся последовательностях, пределах, непрерывных функциях, производных и т.п.

Определение 2 (Предел). *2-адическое целое z является пределом последовательности $\{z_i\}_{i=0}^{\infty}$, если для любого $\varepsilon > 0$ найдется N такое, что $\|z_i - z\|_2 < \varepsilon$ как только $i > N$.*

Однако, согласно определению 2-адической метрики, величина $\|z_i - z\|_2$ может принимать только значения вида$2^{-\ell}$ для подходящих $\ell = 0, 1, 2, \ldots$; поэтому можно считать, что $\varepsilon = 2^{-r}$, где $r = 0, 1, 2, \ldots$.
А тогда можно переписать определение в эквивалентном виде:

Сходимость в $\mathbb{Z}_2$

Поскольку метрика на $\mathbb{Z}_2$ задана, можно говорить о сходящихся последовательностях, пределах, непрерывных функциях, производных и т.п.

Определение 3 (Предел, экв. форм.). *2-адическое целое z есть предел посл-ти $\{z_i\}_{i=0}^{\infty}$ если для любого (достаточно большого) положительного рационального целого K найдется N такое, что $z_i \equiv z \pmod{2^K}$ при всех $i > N$.*

Замечание: По определению 2-адической метрики

$$\|z_i - z\|_2 \leq 2^{-K} \Longleftrightarrow z_i \equiv z \pmod{2^K}$$

Сходимость в $\mathbb{Z}_2$

Поскольку метрика на $\mathbb{Z}_2$ задана, можно говорить о сходящихся последовательностях, пределах, непрерывных функциях, производных и т.п.

Пример: $1, 3, 7, 15, 31, \ldots, 2^i - 1 \ldots \xrightarrow{2} -1$

$$
\begin{array}{lccccc}
\ldots & 0 & 0 & 0 & 0 & 1 \\
\ldots & 0 & 0 & 0 & 1 & 1 \\
\ldots & 0 & 0 & 1 & 1 & 1 \\
\ldots & 0 & 1 & 1 & 1 & 1 \\
\ldots & . & . & . & . & . \\
\ldots & 1 & 1 & 1 & 1 & 1
\end{array}
\begin{array}{l}
= 1 \\
= 3 \\
= 7 \\
= 15 \\
. \\
= -1
\end{array}
$$

Непрерывность на $\mathbb{Z}_2$

Определение 4 (Непрерывная функция) *Функция* $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ *наз. непрерывной в точке* $z \in \mathbb{Z}_2$, *если для любого (достаточно большого) положительного рационального целого* M *найдется положительное рациональное целое* L *такое, что* $f(x) \equiv f(z) \pmod{2^M}$ *как только* $x \equiv z \pmod{2^L}$

Замечание: Функция f наз. *равномерно* непрерывной на $\mathbb{Z}_2$, если f непрерывна в каждой точке $z \in \mathbb{Z}_2$, и L зависит только от M и не зависит от z.

Непрерывность на $\mathbb{Z}_2$

Определение 4 (Непрерывная функция) *Функция* $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ *наз. непрерывной в точке* $z \in \mathbb{Z}_2$, *если для любого (достаточно большого) положительного рационального целого* M *найдется положительное рациональное целое* L *такое, что* $f(x) \equiv f(z) \pmod{2^M}$ *как только* $x \equiv z \pmod{2^L}$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:

$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$

Эквивалентно: $\|f(a) - f(b)\|_2 \leq \|a - b\|_2$

Непрерывность на $\mathbb{Z}_2$

Определение 4 (Непрерывная функция) *Функция* $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ *наз. непрерывной в точке* $z \in \mathbb{Z}_2$, *если для любого (достаточно большого) положительного рационального целого* M *найдется положительное рациональное целое* L *такое, что* $f(x) \equiv f(z) \pmod{2^M}$ *как только* $x \equiv z \pmod{2^L}$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:

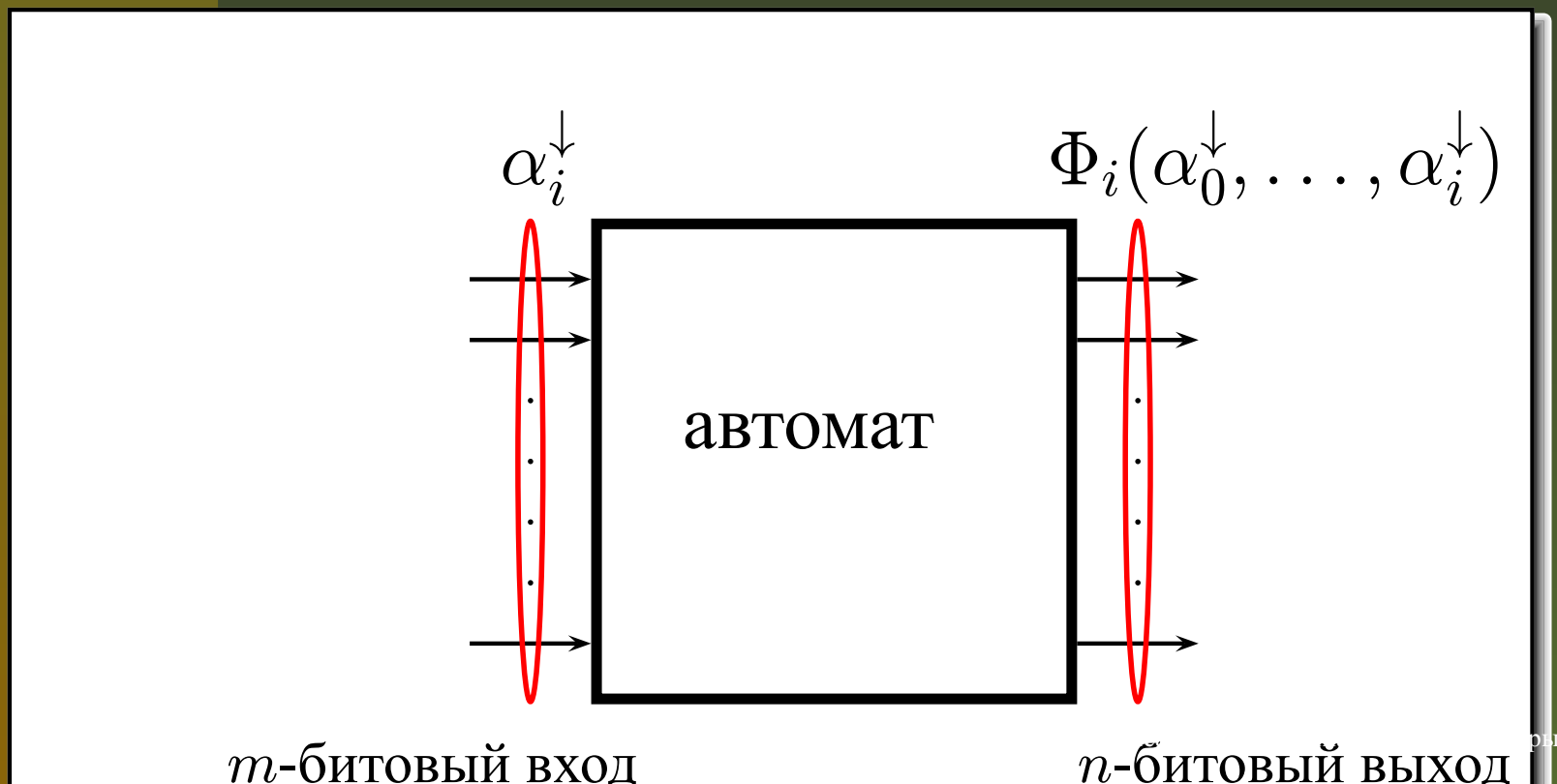
$$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$$

Эквивалентно: $(\ldots, \chi_2, \chi_1, \chi_0) \overset{f}{\mapsto}$
$(\ldots, \psi_2(\chi_0, \chi_1, \chi_2), \psi_1(\chi_0, \chi_1), \psi_0(\chi_0))$

Непрерывность на $\mathbb{Z}_2$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:

$$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$$



Непрерывность на $\mathbb{Z}_2$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:
$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$
Примеры T-функций:

- Арифметические операции (сложение, умножение, ...);
- Поразрядные логические операции (OR, XOR, AND, NOT, ...);
- Всевозможные композиции арифметических и поразрядных логических операций.

Непрерывность на $\mathbb{Z}_2$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:
$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$
Некоторые другие «естественные» функции тоже являются T-функциями:

- *экспоненцирование*, $\uparrow$: $(u, v) \mapsto u \uparrow v = (1 + 2 \cdot u)^v$;
- *возведение в отрицательную степень*, $u \uparrow (-r) = (1 + 2 \cdot u)^{-r}, r \in \mathbb{N}$;
- *деление* $/$: $u/v = u \cdot (v \uparrow (-1)) = \frac{u}{1+2 \cdot v}$.

Непрерывность на $\mathbb{Z}_2$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:
$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$
Это тоже T-функция одного 2-адического переменного x:

$$(1+x)\,\mathsf{XOR}\,4\cdot\left(1-2\cdot\frac{x\ \mathsf{AND}\ x^2+x^3\ \mathsf{OR}\ x^4}{3-4\cdot(5+6x^5)^{x^6\mathsf{XOR}x^7}}\right)^{7-\frac{8x^8}{9+10x^9}}$$

Непрерывность на $\mathbb{Z}_2$

Важный пример: *Функции треугольного вида*=T-функции=функции, удовлетворяющие условию Липшица с константой 1=совместимые функции=детерминированные функции:
$x \equiv z \pmod{2^M} \Longrightarrow f(x) \equiv f(z) \pmod{2^M}$

Вывод: Компьютер осуществляет *приближенные* (относительно 2-адической метрики) вычисления значений непрерывных функций на $\mathbb{Z}_2$.

Редукцию по модулю 2^n, где n — разрядность процессора, компьютер делает автоматически.

Дифференцируемость на $\mathbb{Z}_2$

Определение 5. Функция $F = (f_1, \ldots, f_m) \colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ наз. дифференцируемой (дифференцируемой по модулю 2^M) в т. $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_2^n$, если для любого достаточно большого $M \in \mathbb{N}$ существует $N \in \mathbb{N}$ и $(n \times m)$-матрица $F'_k(\mathbf{u})$ над $\mathbb{Z}_2$ (*матрица Якоби* функции F в т. $\mathbf{u}$), такая что для любого $K \geq N$ и любого $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}_2^n$ вып. сравнение

$$F(\mathbf{u} + \mathbf{h}) \equiv F(\mathbf{u}) + \mathbf{h} \cdot F'_M(\mathbf{u}) \pmod{2^{M+K}}$$

как только $\mathbf{h} \equiv 0 \pmod{2^K}$. Равномерная дифференцируемость (по модулю 2^M): для данного M, наименьшее N обозн. $N_M(F)$.

Дифференцируемость на $\mathbb{Z}_2$

Др. словами, обычная дифференцируемость функции f одной переменной означает, что для любого M

$$\left\| \frac{f(x+h)-f(x)}{h} - f'_M(x) \right\|_2 \leq \frac{1}{2^M}$$

если h достаточно мало, т.е. $\|h\|_2 \leq 2^{-N_M(f)}$, в то время как дифференцируемость по модулю 2^M означает, что нер-во вып. для M фиксированного.

В p-адическом анализе жаргонизм «производная с точностью до M знаков после запятой» имеет точный смысл!

Дифференцируемость на $\mathbb{Z}_2$

Функция $f(x) = x$ AND C *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$

Дифференцируемость на $\mathbb{Z}_2$

Функция $f(x) = x$ AND C *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$

Если $n \geq \ell(|C|)$, где $\ell(|C|)$ — число разрядов, необходимых для двоичной записи $|C|$, то $f(x + 2^n s) = f(x)$ при $C \geq 0$, и $f(x + 2^n s) = f(x) + 2^n s$ при $C < 0$.

Помним, что 2-адическое представление отрицательного числа $-R$ начинается с двоичного представления числа $2^{\ell(R)} - R$ в младших разрядах, за которыми следуют $\ldots 11$: $-1 = \ldots 111$, $-3 = \ldots 11101$, и т.п..

Дифференцируемость на $\mathbb{Z}_2$

Функция $f(x) = x$ AND C *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$

$f'(x) = 0$, если $C \geq 0$, и $f'(x) = 1$ если $C < 0$

Дифференцируемость на $\mathbb{Z}_2$

Функция $f(x) = x \text{ AND } C$ *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$
$f'(x) = 0$, если $C \geq 0$, и $f'(x) = 1$ если $C < 0$

Функция $f(x) = x \text{ XOR } C$ *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$; $f'(x) = 1$, если $C \geq 0$, и $f'(x) = -1$, если $C < 0$.

Это сразу следует из первого утверждения в силу тождества $u \text{ XOR } v = u + v - 2(x \text{ AND } v)$
Т.о., $(x \text{ XOR } C)' = x' + C' - 2(x \text{ AND } C)' =$
$1 + 2 \cdot (0$ если $C \geq 0; -1$ если $C < 0)$.

Дифференцируемость на $\mathbb{Z}_2$

Функция $f(x) = x \,\mathsf{AND}\, C$ *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$
$f'(x) = 0$, если $C \geq 0$, и $f'(x) = 1$ если $C < 0$

Функция $f(x) = x \,\mathsf{XOR}\, C$ *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$; $f'(x) = 1$, если $C \geq 0$, и $f'(x) = -1$, если $C < 0$.

Функции $x \bmod 2^n$, $\mathsf{NOT}(x)$ *и* $x \,\mathsf{OR}\, C$, *где* $C \in \mathbb{Z}$, *равномерно дифференцируемы на* $\mathbb{Z}_2$, *и* $(x \bmod 2^n)' = 0$, $(\mathsf{NOT}\, x)' = -1$, $(x \,\mathsf{OR}\, c)' = 1$, *если* $C \geq 0$, $(x \,\mathsf{OR}\, C)' = 0$ *если* $C < 0$.

Дифференцируемость на $\mathbb{Z}_2$

Функция $f(x) = x$ AND C *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$
$f'(x) = 0$, если $C \geq 0$, и $f'(x) = 1$ если $C < 0$

Функция $f(x) = x$ XOR C *равномерно дифференцируема на* $\mathbb{Z}_2$ *при любом* $C \in \mathbb{Z}$; $f'(x) = 1$, если $C \geq 0$, и $f'(x) = -1$, если $C < 0$.

Функция $f(x, y) = x$ XOR y *не везде дифференцируема на* $\mathbb{Z}_2^2$ *как функция двух переменных. Однако она равномерно дифференцируема по модулю* 2 *на* $\mathbb{Z}_2^2$; ее частные производные по модулю 2 равны 1 всюду на $\mathbb{Z}_2^2$.

Динамика: некоторые понятия

Динамическая система — это просто пара $\langle \mathbb{S}, f \rangle$, где $\mathbb{S}$ – непустое множество, а $f : \mathbb{S} \to \mathbb{S}$ – отображение.

Последовательность

$$x_0,\ x_1 = f(x_0), \ldots, x_{i+1} = f(x_i) = f^{i+1}(x_0), \ldots$$

наз. *траекторией* (или *орбитой*) точки x_0, а последовательность

$$y_0 = F(x_0),\ y_1 = F(x_1), \ldots, y_i = F(x_i), \ldots.$$

наз. наблюдаемой, где $F : \mathbb{S} \to \mathbb{T}$.

Обычно f и F — *измеримые* и непрерывные отображения.

Динамика: некоторые понятия

Говорят, что отображение $F : \mathbb{S} \to \mathbb{T}$ вероятностных пр-в с мерой μ *сохраняет меру* μ, если $\mu(F^{-1}(S)) = \mu(S)$ для любого измеримого подмножества $S \subset \mathbb{T}$.

Динамика: некоторые понятия

Говорят, что отображение $F : \mathbb{S} \to \mathbb{T}$ вероятностных пр-в с мерой μ *сохраняет меру* μ, если $\mu(F^{-1}(S)) = \mu(S)$ для любого измеримого подмножества $S \subset \mathbb{T}$. Отображение $f : \mathbb{S} \to \mathbb{S}$ наз. *эргодическим*, если мера любого f-инвариантного μ-измеримого подмн-ва $S \in \mathbb{S}$ есть либо 0, либо 1: $f^{-1}(S) = S \Longrightarrow \mu(S) \in \{0, 1\}$.

Динамика: некоторые понятия

Говорят, что отображение $F : \mathbb{S} \to \mathbb{T}$ вероятностных пр-в с мерой μ *сохраняет меру* μ, если $\mu(F^{-1}(S)) = \mu(S)$ для любого измеримого подмножества $S \subset \mathbb{T}$. Отображение $f : \mathbb{S} \to \mathbb{S}$ наз. *эргодическим*, если мера любого f-инвариантного μ-измеримого подмн-ва $S \in \mathbb{S}$ есть либо 0, либо 1: $f^{-1}(S) = S \Longrightarrow \mu(S) \in \{0, 1\}$.
Для конечных мн-в: если $\#\mathbb{M} = M$ и $A \subset \mathbb{M}$, то $\mu(A) = \frac{\#A}{M}$.

F сохраняет $\mu \Longleftrightarrow F$ сбалансировано; т.е. у каждой точки одно и то же число F-прообразов.

Динамика: некоторые понятия

Говорят, что отображение $F : \mathbb{S} \to \mathbb{T}$ вероятностных пр-в с мерой μ *сохраняет меру* μ, если $\mu(F^{-1}(S)) = \mu(S)$ для любого измеримого подмножества $S \subset \mathbb{T}$. Отображение $f : \mathbb{S} \to \mathbb{S}$ наз. *эргодическим*, если мера любого f-инвариантного μ-измеримого подмн-ва $S \in \mathbb{S}$ есть либо 0, либо 1: $f^{-1}(S) = S \Longrightarrow \mu(S) \in \{0, 1\}$.
Для конечных мн-в: если $\#\mathbb{M} = M$ и $A \subset \mathbb{M}$, то $\mu(A) = \frac{\#A}{M}$.

Сбалансированность отображения f означает, что f биективно.

Динамика: некоторые понятия

Говорят, что отображение $F : \mathbb{S} \to \mathbb{T}$ вероятностных пр-в с мерой μ *сохраняет меру* μ, если $\mu(F^{-1}(S)) = \mu(S)$ для любого измеримого подмножества $S \subset \mathbb{T}$. Отображение $f : \mathbb{S} \to \mathbb{S}$ наз. *эргодическим*, если мера любого f-инвариантного μ-измеримого подмн-ва $S \in \mathbb{S}$ есть либо 0, либо 1: $f^{-1}(S) = S \Longrightarrow \mu(S) \in \{0, 1\}$.
Для конечных мн-в: если $\#\mathbb{M} = M$ и $A \subset \mathbb{M}$, то $\mu(A) = \frac{\#A}{M}$.

f эргодично $\Longleftrightarrow$ f транзитивно, т.е. орбита каждой точки имеет максимально длинный период; именно, длины M: $f^k(x) = x \Longrightarrow M \mid k$.

Эргодическая теория T-функций

На пространстве $\mathbb{Z}_2$ существует естественная вероятностная мера: *нормализованная мера Хаара* μ_2.

Эргодическая теория T-функций

На пространстве $\mathbb{Z}_2$ существует естественная вероятностная мера: *нормализованная мера Хаара* μ_2.

Именно, множество $a + 2^k\mathbb{Z}_2$ (мн-во всех 2-адических целых чисел, сравнимых с a по модулю 2^k) есть *шар* радиуса 2^{-k}; его *объем* есть $\mu_2(a + 2^k\mathbb{Z}_2) = 2^{-k}$. Это вероятность того, что первые k разрядов у случайно выбранного 2-адического числа такие же, как у a.

$\cdots * * * * * 0101 = 5 + 16 \cdot \mathbb{Z}_2 = -\frac{1}{3} + 16 \cdot \mathbb{Z}_2$

— это 2-адический шар радиуса (и объема) $\frac{1}{16}$ с центром в точке 5 (или, что то же самое, в точке $-\frac{1}{3}$); все 2-адические целые, сравнимые с 5 по модулю 16, образуют этот шар.

Эргодическая теория T-функций

T-функция $F\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ наз. сбалансированной по модулю 2^k, если индуцированное отображение $F \bmod 2^k$ сбалансировано, т.е. $F \bmod 2^k$ отображает $(\mathbb{Z}/2^k\mathbb{Z})^m$ НА $(\mathbb{Z}/2^k\mathbb{Z})^n$, и каждый элемент из $(\mathbb{Z}/2^k\mathbb{Z})^n$ имеет одно и то же число F-прообразов в $(\mathbb{Z}/2^k\mathbb{Z})^m$.

T-функция $F\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ наз. биективной (соотв., транзитивной) по модулю 2^k если индуцированное отображение $F \bmod 2^k\colon x \mapsto F(x) \pmod{2^k}$ кольца вычетов $\mathbb{Z}/2^k\mathbb{Z}$ в себя биективно (соотв., транзитивно).

Эргодическая теория T-функций

Теорема 1. *T-функция* $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ *сохраняет меру* μ_2 *тогда и только тогда, когда каждое индуцированное отображение*

$$F \bmod 2^k : (\mathbb{Z}/2^k\mathbb{Z})^n \to (\mathbb{Z}/2^k\mathbb{Z})^m$$

сбалансировано, $k = 1, 2, 3, \ldots$.

При $m = n = 1$, *T-функция* F *эргодична (по отношению к мере* μ_2*) тогда и только тогда, когда каждое индуцированное отображение*

$$F \bmod 2^k : \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2^k\mathbb{Z}$$

транзитивно, $k = 1, 2, 3, \ldots$.

Эргодическая теория T-функций

Другими словами, T-функция сохраняет меру (эргодична) как функция, определенная на множестве $\mathbb{Z}_2$ всех бесконечных бинарных слов, тогда и только тогда, когда она сохраняет меру (эргодична) как функция, определенная на множестве $\mathbb{Z}/2^k\mathbb{Z}$ всех бинарных слов длины k, для всех $k = 1, 2, \ldots$.

Эргодическая теория T-функций

Теорема 2. *Пусть T-функция* $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ *равномерно дифференцируема по модулю 2. F сохраняет меру, если она сбалансирована по модулю* 2^k *для некоторого* $k \geq N_1(F)$*, и ранг ее матрицы Якоби* $F_1'(\mathbf{u})$ *по модулю 2 равен* m *во всех точках* $\mathbf{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}/2^k\mathbb{Z})^n$*. При* $m = n$*, эти условия и необходимы, т.е. F сохраняет меру тогда и только тогда, когда она биективна по модулю* 2^k *для некоторого* $k \geq N_1(F)$*, и* $\det(F_1'(\mathbf{u})) \not\equiv 0 \pmod 2$ *во всех точках* $\mathbf{u} = (u_1, \ldots, u_n) \in (\mathbb{Z}/2^k\mathbb{Z})^n$*. Более того, в этом случае F сохраняет меру тогда и только тогда, когда она сбалансирована по модулю* $2^{N_1(F)+1}$.

Эргодическая теория T-функций

Следующая T-функция f сохраняет меру (т.е. биективна по модулю 2^r для всех $r = 1, 2, \ldots$):
$f(x) = (x + 3x^3)$ XOR x^3
Док-во: $f(x) \equiv x \pmod 2$, т.е. биективна по модулю 2. Т. к. XOR равномерно дифференцируема по модулю 2, то и ф-я f р. д. по модулю 2, и $N_1(f) = 1$. Именно, при $\ell \geq 1$

$$f(x + 2^\ell s) \equiv$$

$$\equiv (x+2^\ell s+9x^3+27x^2\cdot 2^\ell s)\text{XOR}(x^3+3x^2\cdot 2^\ell s) \pmod{2^{\ell+1}}$$

$$\equiv f(x)+2^\ell s(1+27x^2+3x^2) \equiv f(x)+2^\ell s \pmod{2^{\ell+1}}$$

Теперь применяем Теорему 2.

Эргодическая теория T-функций

Следующая T-функция F сохраняет меру (т.е. биективна по модулю 2^r для всех $r = 1, 2, \ldots$):
$F(x, y) = (x \text{ XOR } (2(x \text{ AND } y)), (y + 3x^3) \text{ XOR } x)$

В с. д., F биективна по модулю 2, F равномерно дифференцируема по модулю 2, и $N_1(F) = 1$; именно

$$F(x + 2^n t, y + 2^m s) \equiv$$

$$F(x, y) + (2^n t, 2^m s) \cdot \begin{pmatrix} 1 & x+1 \\ 0 & 1 \end{pmatrix} \pmod{2^{k+1}}$$

для всех $m, n \geq 1$ (здесь $k = \min\{m, n\}$); $\det F_1'(x, y) \equiv 1 \pmod 2$. Теперь применяем Теорему 2. $\square$

Эргодическая теория T-функций

Теорема 3. *Пусть T-функция* $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ *равномерно дифференцируема по модулю 4 на* $\mathbb{Z}_2$. *Функция* f *эргодична тогда и только тогда, когда она транзитивна по модулю* $2^{N_2(f)+2}$.

Например, из этой теоремы следует, что полином с рациональными целыми коэффициентами транзитивен по каждому модулю 2^n тогда и только тогда, когда он транзитивен по модулю 8.
(М. В. Ларин)
Из Теоремы 2 следует, что полином с рациональными целыми коэффициентами биективен по каждому модулю 2^n тогда и только тогда, когда он биективен по модулю 4.

Эргодическая теория T-функций

Пример. (Klimov–Shamir, 2002) *Функция* $x + (x^2 \,\mathsf{OR}\, 5)$ *эргодична.*

Эргодическая теория T-функций

Пример. (Klimov–Shamir, 2002) *Функция* $x + (x^2 \text{ OR } 5)$ *эргодична.*

В статье Klimov–Shamir упоминали мою публикацию 1993 года с Теоремой 3, однако утверждали, что

> "...neither the invertibility nor the cycle structure of $x + (x^2 \text{ OR } 5)$ could be determined by his techniques."

На самом деле, их результат мгновенно следует из Theorem 3.

Эргодическая теория T-функций

Пример. (Klimov–Shamir, 2002) *Функция* $x + (x^2 \text{ OR } 5)$ *эргодична.*

Док-во: Функция $f(x) = x + (x^2 \text{ OR } 5)$ равномерно дифференцируема на $\mathbb{Z}_2$:
$f'(x) = 1 + 2x \cdot (x \text{ OR } 5)' = 1 + 2x$, и $N_2(f) = 3$, т.к. $(x + h) \text{ OR } 5 = (x \text{ OR } 5) + h$ если $h \equiv 0 \pmod 8$ — это очевидно ввиду того, что 5 =...000101. Для завершения док-ва в силу Теоремы 3 достаточно убедится, что f транзитивна по модулю 32, что и делается с помощью прямых вычислений значений of $f(0), f(f(0)), \ldots$ в $\mathbb{Z}/32\mathbb{Z}$. □

Эргодическая теория T-функций

Пример. (Klimov–Shamir, 2002) *Функция* $x + (x^2 \text{ OR } 5)$ *эргодична.*

Теорема 4. *T-функция* $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ *эргодична тогда и только тогда, когда* $f(x) = 1 + x + 2 \cdot (g(x+1) - g(x))$, *где* g — *любая T-функция.*

Эргодическая теория T-функций

Пример. (Klimov–Shamir, 2002) *Функция* $x + (x^2 \,\mathsf{OR}\, 5)$ *эргодична.*

Теорема 4. *T-функция* $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ *эргодична тогда и только тогда, когда* $f(x) = 1 + x + 2 \cdot (g(x+1) - g(x))$, *где* g — *любая T-функция.*

$$f(x) = 2 + \frac{x}{3} + \frac{1}{3^x} + 2\left(\frac{(x^2+2x)\,\mathsf{XOR}\,(1/3)}{2x+3}\right)^{\frac{(x+1)\mathsf{AND}(1/5)}{1-2x}} +$$

$$+ 2 \cdot \mathsf{NOT}\left(\left(\frac{(x^2-1)\,\mathsf{XOR}\,(1/3)}{2x+1}\right)^{\frac{x\mathsf{AND}(1/5)}{5-2x}}\right).$$

Поточное шифрование

- К открытому тексту α_0 α_1 α_2 $\ldots$

Поточное шифрование

- К открытому тексту $\alpha_0 \quad \alpha_1 \quad \alpha_2 \quad \ldots$
- прибавляем $\mathrm{mod}2 \quad \oplus$

Поточное шифрование

- К открытому тексту $\alpha_0 \quad \alpha_1 \quad \alpha_2 \quad \ldots$
- прибавляем $\mathrm{mod}2 \quad \oplus$
- гамму (=keystream) $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \ldots$

Поточное шифрование

- К открытому тексту $\alpha_0 \quad \alpha_1 \quad \alpha_2 \quad \ldots$
- прибавляем $\mathrm{mod}2$ $\oplus$
- гамму (=keystream) $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \ldots$
- и получаем $\underline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$

Поточное шифрование

- К открытому тексту $\alpha_0 \quad \alpha_1 \quad \alpha_2 \quad \ldots$
- прибавляем $\mathrm{mod}2 \quad \oplus$
- гамму (=keystream) $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \ldots$
- и получаем
- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \ldots$

Поточное шифрование

Чтобы расшифровать сообщение, берем

- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \ldots$

Поточное шифрование

Чтобы расшифровать сообщение, берем

- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \ldots$
- прибавляем $\mathrm{mod}2$ $\oplus$

Поточное шифрование

Чтобы расшифровать сообщение, берем

- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \ldots$
- прибавляем $\mathrm{mod}2$ $\oplus$
- ту же самую гамму $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \ldots$

Поточное шифрование

Чтобы расшифровать сообщение, берем

- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \dots$
- прибавляем $\mod 2$ $\oplus$
- ту же самую гамму $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \dots$
- и получаем $\_\_\_\_\_$

Поточное шифрование

Чтобы расшифровать сообщение, берем

- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \dots$
- прибавляем $\mathrm{mod}2$ $\oplus$
- ту же самую гамму $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \dots$
- и получаем
- сообщение : $\alpha_0 \quad \alpha_1 \quad \alpha_2 \quad \dots$

Поточное шифрование

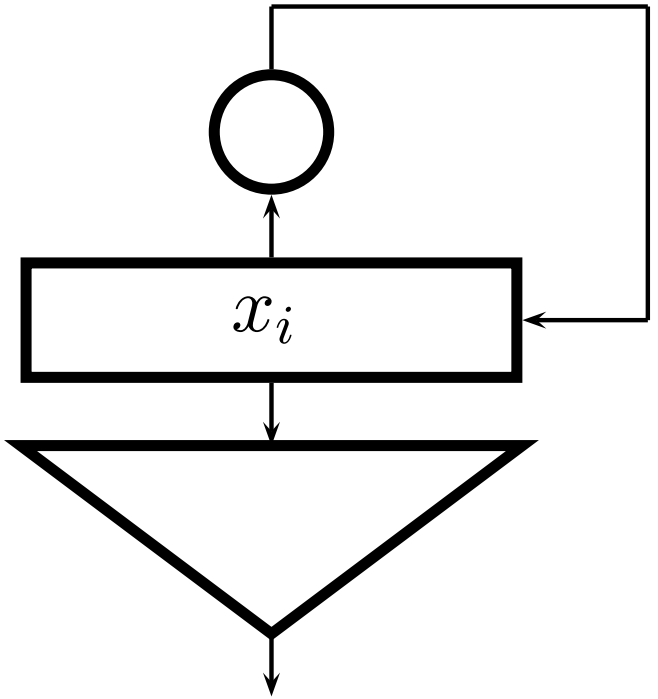
Чтобы расшифровать сообщение, берем

- шифрованный текст $\zeta_0 \quad \zeta_1 \quad \zeta_2 \quad \dots$
- прибавляем $\mathrm{mod}2$ $\oplus$
- ту же самую гамму $\gamma_0 \quad \gamma_1 \quad \gamma_2 \quad \dots$
- и получаем
- сообщение : $\alpha_0 \quad \alpha_1 \quad \alpha_2 \quad \dots$

Такое шифрование стойкое, если гамма случайна и равновероятна (К. Шеннон).

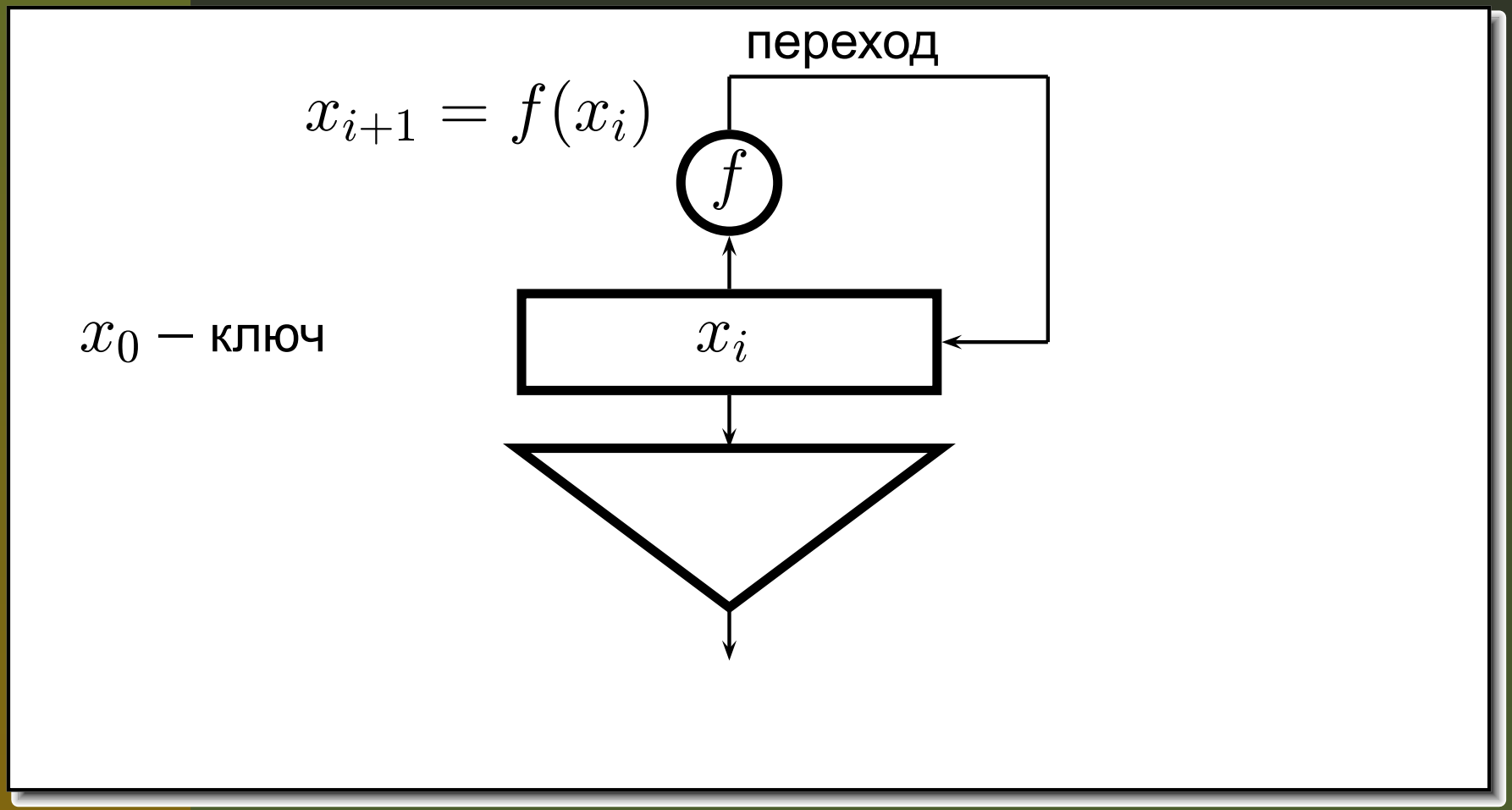
Псевдослучайный генератор

x_0 — ключ



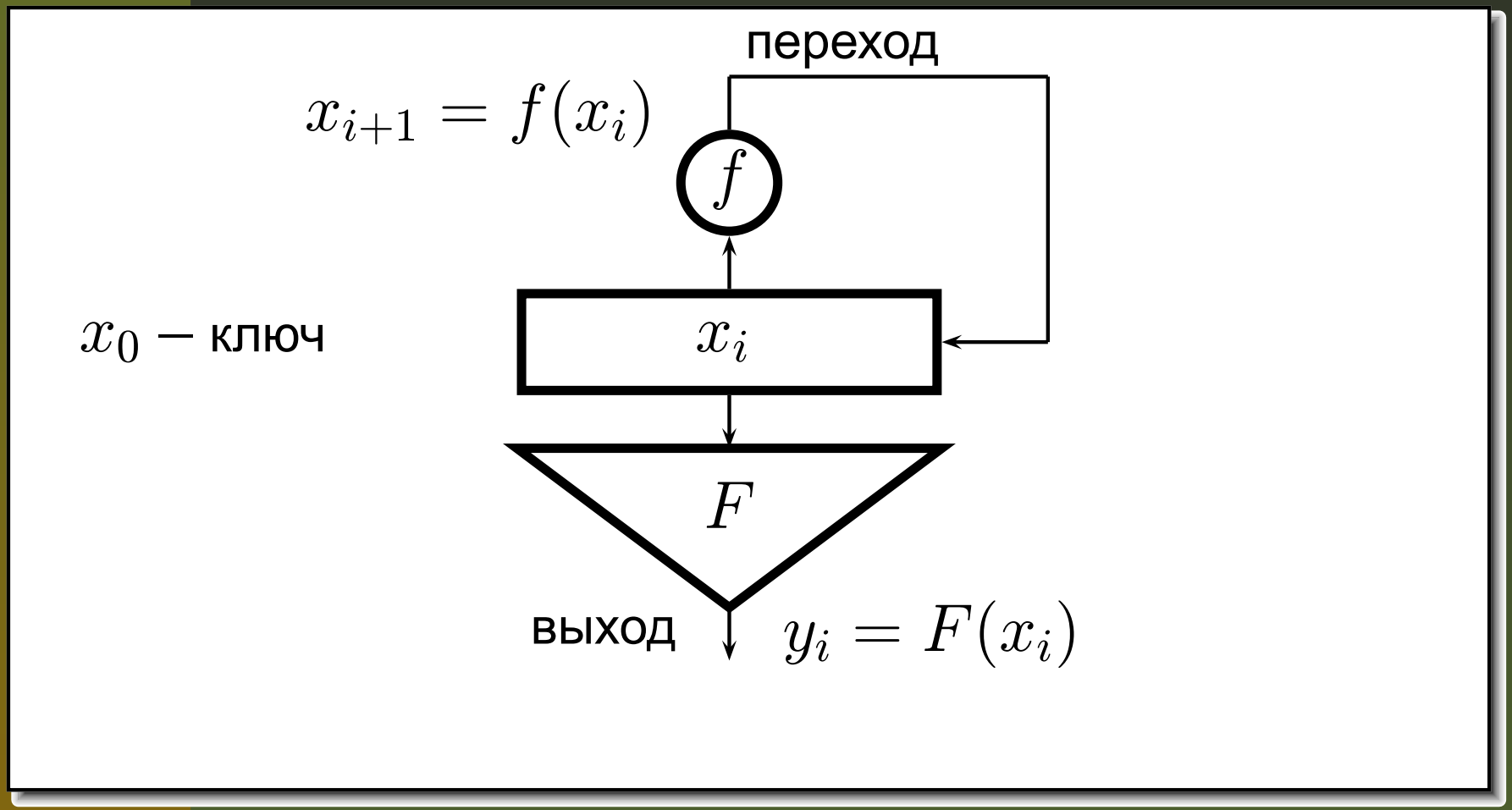
$(x_i \in \mathbb{B}^n, y_i \in \mathbb{B}^m, \mathbb{B} = \{0, 1\})$

Псевдослучайный генератор



$(x_i \in \mathbb{B}^n, y_i \in \mathbb{B}^m, \mathbb{B} = \{0,1\})$ $f : \mathbb{B}^n \to \mathbb{B}^n$ — функция *перехода*,

Псевдослучайный генератор



$(x_i \in \mathbb{B}^n, y_i \in \mathbb{B}^m, \mathbb{B} = \{0,1\})$ $f\colon \mathbb{B}^n \to \mathbb{B}^n$ — функция *перехода*, $F\colon \mathbb{B}^n \to \mathbb{B}^m$ — функция *выхода*. Можно отождествить $\mathbb{B}^k = \mathbb{Z}/2^k\mathbb{Z}$, или $\mathbb{B}^k = (\mathbb{Z}/2^\ell\mathbb{Z})^s$, если $k = \ell s$.

ПСГ как динамическая система

Посл-ть *внутренних состояний* ПСГ — это траектория ключа

$$x_0,\ x_1 = f(x_0), \ldots, x_{i+1} = f(x_i) = f^{i+1}(x_0), \ldots.$$

ПСГ как динамическая система

Посл-ть *внутренних состояний* ПСГ — это траектория ключа

$$x_0,\ x_1 = f(x_0), \ldots, x_{i+1} = f(x_i) = f^{i+1}(x_0), \ldots.$$

Выходная посл-ть ПСГ — это наблюдаемая

$$y_0 = F(x_0),\ y_1 = F(x_1), \ldots, y_i = F(x_i), \ldots.$$

Требования к ПСГ

Хороший ПСГ должен удовлетворять след. условиям:

- *Функция перехода f должна обеспечивать псевдослучайность*; в частности, равномерное распределение и длинный период посл-ти состояний

Требования к ПСГ

Хороший ПСГ должен удовлетворять след. условиям:

- *Функция перехода f должна обеспечивать псевдослучайность*
- *Функция выхода F не должна портить псевдослучайность* (в частности, выходная посл-ть должна остаться равномерно распределенной и иметь длинный период); сверх того, в поточных шифраторах именно *F обеспечивает стойкость шифрования* (в частности, для данного y_i, нахождение x_i из уравнения $y_i = F(x_i)$) должно быть вычислительно трудоемкой задачей.

Требования к ПСГ

Хороший ПСГ должен удовлетворять след. условиям:

- *Функция перехода f должна обеспечивать псевдослучайность*
- *Функция выхода F не должна портить псевдослучайность* ; сверх того, в поточных шифраторах именно *F обеспечивает стойкость шифрования*
- Чтобы ПСГ допускал простую программную реализацию, обе функции *f и F должны быть несложными композициями элементарных команд процессора*: арифметических операций (сложения, умножения,...) и поразрядных логических операций (XOR, OR, AND, NOT)

Как этого добиться?

Чтобы выполнить условие 1 (из 3) можно взять *эргодическую* T-функцию f на $\mathbb{Z}_2$ (приведение по модулю 2^n, где n — длина регистра, компьютер выполнит автоматически)

Посл-ть состояний

$$x_0,\ x_1 = f(x_0), \ldots, x_{i+1} = f(x_i) = f^{i+1}(x_0), \ldots$$

тогда будет посл-тью n-разрядных слов максимально длинного периода (длины 2^n) и иметь *строго равномерное распределение*: каждое n-разрядное слово встретится на периоде ровно 1 раз.

Как этого добиться?

Чтобы выполнить первую часть условия 2, можно взять *сбалансированное* отображение $F\colon \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^m\mathbb{Z}$. Если $n = kr$, $m = ks$, $s \leqslant r$, то в качестве F можно взять сохраняющую меру T-функцию $F\colon \mathbb{Z}_2^r \to \mathbb{Z}_2^s$.

Если $s \ll r$, то таким образом можно добиться выполнения второй части условия 2, т.к. в этом случае уравнение $y_i = F(x_i)$ имеет очень много решений, $2^{k(r-s)}$.

Как этого добиться?

Чтобы обеспечить выполнение условия 3, нужно уметь строить эргодические (соотв., сохраняющие меру) T-функции в виде композиций элементарных команд процессора.

Все это мы уже умеем делать. Например, эргодические T-функции можно строить с помощью Теоремы 4, а сохраняющие меру — с помощью Теоремы 2.

Латинские квадраты

Определение 6. *Латинский квадрат порядка P* — $P \times P$ матрица содержащая P различных символов (к-рые будем обозначать $0, 1, \ldots, P-1$), такая, что в каждой строке и в каждом столбце каждый символ встречается ровно 1 раз.

Латинские квадраты

Определение 6. *Латинский квадрат порядка P* — $P \times P$ матрица содержащая P различных символов (к-рые будем обозначать $0, 1, \ldots, P-1$), такая, что в каждой строке и в каждом столбце каждый символ встречается ровно 1 раз.

В алгебре латинские квадраты наз. бинарными квазигруппами: это алгебраические системы на множестве $\mathcal{A} = \{0, 1, \ldots, P-1\}$ с единственной бинарной операцией $*$, которая задается с помощью таблицы Кэли, являющейся латинским квадратом. Операция $*$ обратима по каждой переменной: для любых $a, b \in \mathcal{A}$, каждое из ур-ий $a * y = b$ и $x * a = b$ имеет единственное решение. Операция $*$ не обязательно ассоциативна.

Латинские квадраты

Определение 6. *Латинский квадрат порядка P* — $P \times P$ матрица содержащая P различных символов (к-рые будем обозначать $0, 1, \ldots, P-1$), такая, что в каждой строке и в каждом столбце каждый символ встречается ровно 1 раз.
Другими словами, латинский квадрат — это функция от двух переменных

$$F : \mathcal{A}^2 \to \mathcal{A},$$

(где $\mathcal{A} = \{0, 1, \ldots, P-1\}$), которая обратима (т.е. биективна) по каждой из переменных.

Латинские квадраты

Определение 6. *Латинский квадрат порядка P* — $P \times P$ матрица содержащая P различных символов (к-рые будем обозначать $0, 1, \ldots, P-1$), такая, что в каждой строке и в каждом столбце каждый символ встречается ровно 1 раз.
Пример латинского квадрата:

$$\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 0 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 0 & 1 & 2 & 3 & 4 \end{array}$$

Латинские квадраты

Определение 6. *Латинский квадрат порядка P* — $P \times P$ матрица содержащая P различных символов (к-рые будем обозначать $0, 1, \ldots, P-1$), такая, что в каждой строке и в каждом столбце каждый символ встречается ровно 1 раз.
Проблема в том, как написать программу, генерирующую много больших латинских квадратов.

Латинские квадраты

Определение 6. *Латинский квадрат порядка P* — $P \times P$ матрица содержащая P различных символов (к-рые будем обозначать $0, 1, \ldots, P-1$), такая, что в каждой строке и в каждом столбце каждый символ встречается ровно 1 раз.
Проблема в том, как написать программу, генерирующую много больших латинских квадратов.

Более того, в о многих случаях (напр., в смарт-картах) нвозможно хранить всю матрицу целиком, поэтому программа должна для любых двух данных чисел $a, b \in \{0, 1, \ldots, P-1\}$ строить элемент с номером (a, b).

Как строить латинские квадраты

Основной инструмент — Следствие из Теоремы 2,которая справедлива для любого простого p:

Следствие 1. *Равномерно дифференцируемая по модулю p совместимая функция $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ является латинским квадратом по модулю p^k для всех $k = 1, 2, \ldots$, если $f \bmod p^{N_1(f)}$ — это латинский квадрат, и $\frac{\partial_1 f(\mathbf{u})}{\partial_1 x_i} \not\equiv 0 \pmod{p}$ для всех $\mathbf{u} \in (\mathbb{Z}/p^{N_1(f)}\mathbb{Z})^2$, $i = 1, 2$.*

Как строить латинские квадраты

Следствие 1. *Равномерно дифференцируемая по модулю p совместимая функция $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ является латинским квадратом по модулю p^k для всех $k = 1, 2, \ldots$, если $f \bmod p^{N_1(f)}$ — это латинский квадрат, и $\frac{\partial_1 f(\mathbf{u})}{\partial_1 x_i} \not\equiv 0 \pmod{p}$ для всех $\mathbf{u} \in (\mathbb{Z}/p^{N_1(f)}\mathbb{Z})^2$, $i = 1, 2$.*

Пример: латинский квадрат порядка 2^k.

Положим $f(x, y) = x + y + \gamma + 2 \cdot v(x, y)$, где $v(x, y)$ — *любая* T-функция, $\gamma \in \{0, 1\}$.

Тогда $f(x, y) \bmod 2$ — латинский квадрат, и $\frac{\partial_1 f(x,y)}{\partial_1 x} \equiv \frac{\partial_1 f(x,y)}{\partial_1 x} \equiv 1 \pmod{2}$. □

Как строить латинские квадраты

Следствие 1. *Равномерно дифференцируемая по модулю p совместимая функция $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ является латинским квадратом по модулю p^k для всех $k = 1, 2, \ldots$, если $f \bmod p^{N_1(f)}$ — это латинский квадрат, и $\frac{\partial_1 f(\mathbf{u})}{\partial_1 x_i} \not\equiv 0 \pmod{p}$ для всех $\mathbf{u} \in (\mathbb{Z}/p^{N_1(f)}\mathbb{Z})^2$, $i = 1, 2$.*

Пример: латинский квадрат порядка $2^k \cdot 3^\ell \cdots p^r$. Положим $f(x, y) = x + y + 2 \cdot 3 \cdots p \cdot v(x, y)$, где $v(x, y)$ — *любой* полином с рациональными целыми коэффициентами. Тогда $f(x, y)$ — латинский квадрат по модулям $2, 3, \ldots, p$, и $\frac{\partial f(x,y)}{\partial x} \equiv \frac{\partial f(x,y)}{\partial x} \equiv 1 \pmod{q}$ для всех $q = 2, 3, \ldots, p$. □

Как строить латинские квадраты

Следствие 1. *Равномерно дифференцируемая по модулю p совместимая функция $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ является латинским квадратом по модулю p^k для всех $k = 1, 2, \ldots$, если $f \bmod p^{N_1(f)}$ — это латинский квадрат, и $\frac{\partial_1 f(\mathbf{u})}{\partial_1 x_i} \not\equiv 0 \pmod{p}$ для всех $\mathbf{u} \in (\mathbb{Z}/p^{N_1(f)}\mathbb{Z})^2$, $i = 1, 2$.*

Если $g(x, y)$ — совместимый латинский квадрат порядка $P = 2 \cdot 3 \cdots p$ (нек-рые сомн-тели могут отсутствовать), то $f(x, y) = g(x, y) + h(x, y) + 2 \cdot 3 \cdots p \cdot v(x, y)$ — латинский квадрат порядка $2^k \cdot 3^\ell \cdots p^r$ при любом $v(x, y) \in \mathbb{Z}[x, y]$, и $f(x, y) \equiv g(x, y) \pmod{P}$.

Ортогональные лат. квадраты

Два лат. квадрата порядка P наз. ортогональными $\Longleftrightarrow$ при наложении их друг на друга каждая из P^2 упоряд. пар символов встречается ровно 1 раз.

Ортогональные лат. квадраты

Два лат. квадрата порядка P наз. ортогональными $\Longleftrightarrow$ при наложении их друг на друга каждая из P^2 упоряд. пар символов встречается ровно 1 раз.

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

$$\begin{array}{ccc} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{array}$$

Ортогональные лат. квадраты

Два лат. квадрата порядка P наз. ортогональными $\Longleftrightarrow$ при наложении их друг на друга каждая из P^2 упоряд. пар символов встречается ровно 1 раз.

Следствие 2 [Теоремы 2]. *Лат. квадраты* $g, f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ *ортогональны* $\mod p^k$ $k = 1, 2, \ldots$ $\Longleftrightarrow$ *совместимая р. дифф.* $\mod p$ *ф-я* $F(x, y) = (f(x, y), g(x, y)) : \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ *сохраняет меру. Это выполняется* $\Longleftrightarrow$

$$\det \begin{pmatrix} \frac{\partial_1 f(x,y)}{\partial_1 x} & \frac{\partial_1 g(x,y)}{\partial_1 x} \\ \frac{\partial_1 f(x,y)}{\partial_1 y} & \frac{\partial_1 g(x,y)}{\partial_1 y} \end{pmatrix} \not\equiv 0 \pmod{p}$$

для всех $(x, y) \in (\mathbb{Z}/p^{N_1(F)}\mathbb{Z})^2$

Ортогональные лат. квадраты

Два лат. квадрата порядка P наз. ортогональными $\Longleftrightarrow$ при наложении их друг на друга каждая из P^2 упоряд. пар символов встречается ровно 1 раз.

$$f(x,y) \bmod 3 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad g(x,y) \bmod 3 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

$f(x,y) = x+y+3\cdot v(x,y);\ g(x,y) = 2x+y+3\cdot w(x,y)$
$v(x,y), w(x,y) \in \mathbb{Z}_3[x,y]$ — любые

$$\det \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \equiv 2 \pmod 3$$

Ортогональные лат. квадраты

Два лат. квадрата порядка P наз. ортогональными $\Longleftrightarrow$ при наложении их друг на друга каждая из P^2 упоряд. пар символов встречается ровно 1 раз.

Пусть $\mathcal{P}$ — мн-во *нечетных* простых чисел, $v(x,y), w(x,y) \in \mathbb{Z}[x,y]$. Тогда след. лат. квадраты ортогональны $\mod P$ для любого числа P, все простые делители к-рого лежат в $\mathcal{P}$:

$$f(x,y) = x+y+\Pi\cdot v(x,y);\ g(x,y) = -x+y+\Pi\cdot w(x,y);$$

здесь

$$\Pi = \prod_{p\in\mathcal{P}} p$$

Ортогональные лат. квадраты

Два лат. квадрата порядка P наз. ортогональными $\Longleftrightarrow$ при наложении их друг на друга каждая из P^2 упоряд. пар символов встречается ровно 1 раз.

Если $\{f_i(x,y)\}_{i=1}^N$ совместимые попарно ортогональные лат. квадраты порядка $P = 3 \cdot 5 \cdots p$ (нек-рые сомн-тели могут отсутствовать), и $v_i(x,y) \in \mathbb{Z}[x,y]$, то $\{f_i(x,y) + h_i(x,y) + P \cdot v_i(x,y)\}_{i=1}^N$ — попарно ортогональные лат. квадраты порядка $3^k \cdot 5^\ell \cdots p^r$.

Это реклама!!!

Обо всех этих (и многих других) приложениях неархимедовой динамики можно прочитать в книжке

Applied Algebraic Dynamics,

by Vladimir Anashin and Andrei Khrennikov

Publisher: W. de Gruyter, Berlin—N.Y.
2009 (должна выйти в мае).