Сложность конечных последовательностей нулей и единиц и геометрия конечных функциональных пространств

В. И. Арнольд *

Последовательность 001 001 001 001 проще, чем последовательность 01 001 0111 001. Ниже описана формальная математическая теория, придающая этому интуитивно понятному утверждению точный смысл.

Пусть x – последовательность из n нулей и единиц, $x = (x_1, \dots, x_n), x_j \in \mathbb{Z}_2$. Множество M всех 2^n таких последовательностей есть множество вершин n-мерного куба. Оно является также n-мерным векторным пространством над полем $\mathbb{Z}_2$ из двух элементов: $M = \mathbb{Z}_2^n$.

Для анализа сложности функции $x \in M$ мы последуем идее Ньютона и рассмотрим ее первые разности, определив линейный оператор

$$A : M \to M\,, \quad y = Ax$$

формулой $y_j = x_{j+1} - x_j$. Чтобы разностей получилось n, мы определим x_{n+1} как x_1, т.е. будем считать нашу последовательность x циклической (так, что функция x со значениями x_j в точках $_j$ будет периодической, с периодом n). Изложенная ниже геометрическая теория доставляет информацию о жордановой нормальной форме этого оператора A над полем $\mathbb{Z}_2$.

Отображение A конечного множества M в себя задается графом с 2^n вершинами x. Из каждой вершины x в этом графе выходит ровно одно ребро, оно ведет в Ax.

Пример. При $n = 3$ граф имеет 8 вершин и 8 ребер, $A(0,0,0) = (0,0,0)$, $A(1,1,1) = (0,0,0)$, $A(1,0,0) = (1,0,1)$, $A(0,1,0) = (1,1,0)$, $A(0,0,1) = (0,1,1)$, $A(1,1,0) = (0,1,1)$, $A(1,0,1) = (1,1,0)$, $A(0,1,1,) = (1,0,1)$.

Обозначая последовательность $x = (x_1, \dots, x_n)$ числом в двоичной записи

$$X = x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n \cdot 1\,,$$

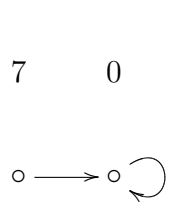
мы записываем предыдущий граф в виде графа с вершинами

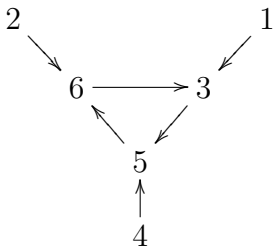
$X(x)$	0	1	2	3	4	5	6	7
$X(Ax)$	0	3	6	5	5	6	3	0

,

*Частично поддержано РФФИ, грант 05-01-00104. Доложено Московскому математическому Обществу 22 ноября 2005 г., видеозапись этого доклада находится на сайте Общества в интернете.

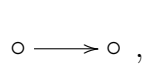
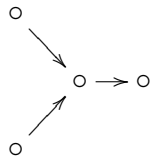
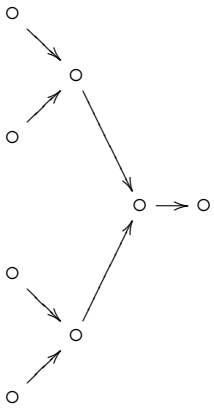
являющимися вычетами по модулю $2^n = 8$. При $n = 3$ этот граф состоит из двух компонент связности,

$(O_1 * T_2) =$ 

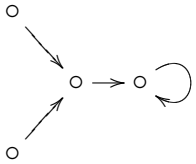
, $(O_3 * T_2) =$ 

.

Мы будем обозначать символом O_m цикл из m циклически соединенных вершин. Знаком T_{2^n} будет обозначаться бинарное дерево из 2^n вершин:

$T_2 =$  , $T_4 =$  , $T_8 =$  .

Знаком $(O_m * T)$ будем обозначать цикл из m вершин, оснащенный лесом из m корневых деревьев T, корнями которых являются вершины цикла O_m (эти корневые деревья предполагаются состоящими из ориентированных направлениями к корням ребер):

$(O_1 * T_4) =$  , $(O_2 * T_2) =$  .

Граф $(O_m * T_{2^n})$ имеет, таким образом, $m2^n$ вершин.

Граф оператора взятия разностей $A : M \to M$ разбивается на компоненты связности. Например, для $n = 3$ он состоит из двух компонент, $(O_1 * T_2)$ и $(O_3 * T_2)$, изображенных выше.

Теорема 1. *Каждая компонента связности графа любого отображения конечного множества в себя имеет цикл, и притом только один.*

Доказательство. Конечность множества образов $x, A(x), A^2(x), A^3(x), \ldots$ влечет существование повторения $A^p(x) = A^q(x)$, а потому существование цикла периода $p - q$.

Если бы в одной связной компоненте было бы два цикла, то на соединяющей их цепочке ребер $(x, \ldots, w)$ из какой-либо промежуточной вершины выходило бы два ориентированных ребра – одно к одному, а другое – к другому циклу. Теорема 1 доказана.

Прямые вычисления графов операторов взятия разностей $A : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ при $n \le 12$ приводит к следующим ответам: (в наиболее сложном случае $n = 12$ приходится соединять всего 4096 вершин, и рисунок умещается на одной странице).

n	число компонент	компоненты графа	соотношение
2	1	$(O_1 * T_4)$	$A^2 = 0$
3	2	$(O_3 * T_2) + (O_1 * T_2)$	$A^4 = A$
4	1	$(O_1 * T_{16})$	$A^4 = 0$
5	2	$(O_{15} * T_2) + (O_1 * T_2)$	$A^{16} = A$
6	4	$2(O_6 * T_4) + (O_3 * T_4) + (O_1 * T_4)$	$A^8 = A^2$
7	10	$9(O_7 * T_2) + (O_1 * T_2)$	$A^8 = A$
8	1	$(O_1 * T_{256})$	$A^8 = 0$
9	6	$4(O_{63} * T_2) + (O_3 * T_2) + (O_1 * T_2)$	$A^{64} = A$
10	10	$8(O_{30} * T_4) + (O_{15} * T_4) + (O_1 * T_4)$	$A^{32} = A^2$
11	4	$3(O_{341} * T_2) + (O_1 * T_2)$	$A^{342} = A$
12	24	$20(O_{12} * T_{16}) + 2(O_6 * T_{16}) + (O_3 * T_{16}) + (O_1 * T_{16})$	$A^{16} = A^4$

Пример. Общее число вершин компонент графа с $n = 11$ есть $(3 \cdot 341 + 1)2 = 2^{11}$.

В графе "соотношение" выписано алгебраическое тождество, получаемые следующим путем. Обозначим через $\delta : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ оператор циклического сдвига последовательности: если $\delta x = y$, то $y_j = x_{j-1}$ (где x_{-1} означает x_n, поскольку последовательности предполагаются циклически замкнутыми).

Очевидно, линейный оператор δ удовлетворяет тождеству $\delta^n = 1$. Оператор взятия разностей A связан с ним соотношением $A = \delta + 1$ (для вычетов по модулю 2 разность совпадает с суммой).

Из этих соотношений легко вытекают "соотношения" таблицы. Например, для $n = 3$ мы находим последовательно:

$$A = 1 + \delta, \quad A^2 = 1 + 2\delta + \delta^2 = 1 + \delta^2, \quad A^3 = 1 + \delta + \delta^2 + \delta^3 = 1 + \delta + \delta^2 + 1 = \delta + \delta^2,$$

$$A^4 = \delta + \delta^2 + \delta^2 + \delta^3 = \delta + 2\delta^2 + 1 = 1 + \delta = A.$$

Рассматривая приведенную выше таблицу ответов легко обнаружить много эмпирических закономерностей, которые приводят к доказанным ниже общим теоремам и для произвольных значений n (а также к еще большему числу недоказанных гипотез).

В качестве меры сложности последовательности или функции ($x \in \mathbb{Z}_2^n$) мы будем использовать геометрические свойства графа операции взятия разностей A и положение вершины x в этом графе.

А именно, мы будем считать объект x более сложным, если длина цикла содержащей его компоненты графа больше. В пределах компонент с циклами данной длины вершины будут считаться тем более сложными, чем дальше они удалены от цикла.

Следующие примеры объясняют этот выбор понятия сложности рецептом Ньютона исследования эмпирических последовательностей значений функций. Самые простые функции – это константы $x = 0$ и $x = 1$. В этом случае период равен 1, а расстояние до цикла равно 0 в первом и 1 во втором случае (так что константа 0 проще константы 1).

Если функция x – многочлен степени меньше d, то для нее $A^d x = 0$, так что вершина x принадлежит области притяжения аттрактора 0 периода 1.

Обратно, если вершина x притягивается к нулю, т.е. $A^d x = 0$, то функция x – "многочлен" степени меньше d (как доказал Ньютон).

Под "многочленами" здесь понимаются приведенные по модулю 2 функции с целыми значениями

$$x(t) = a_1 t^r + \ldots + a_{r+1},$$

коэффициенты которых – рациональные числа, а значения, приведенные по модулю 2, образуют последовательность $x(1) \equiv x_1, x(2) \equiv x_2, \ldots$ периода n.

Пример. Числа сочетаний $C_t^2, t \geq 2$ образуют, после приведения по модулю 2, последовательность $(1, 1, 0, 0, 1, 1, 0, 0, \ldots)$ периода 4. Коэффициенты этого "многочлена"

$$C_t^2 = \frac{t(t-1)}{2}$$

– не целые, а рациональные числа, но все значения в целых точках целые.

Из теории Ньютона следует, что кольцо всех таких "многочленов" представляет собой компоненту связности (корневое дерево) цикла $x = 0$ периода 1 в $\mathbb{Z}_2^n$.

Эти деревья "многочленов" периода n приведены для $n \leq 12$ в виде последнего слагаемого суммы компонент: $(O_1 * T_4)$ при $n = 2$, $(O_1 * T_2)$ при $n = 3$, ..., $(O_1 * T_{16})$ при $n = 12$.

Теорема 2. *Граф "многочленов" периода $n = 2^k(2a+1)$ является корневым бинарным деревом с 2^k этажами, так что содержащая $x = 0$ компонента графа оператора взятия разностей есть $(O_1 * T_{2^{2^k}})$.*

Пример. При первых значениях n числа $V = 2^{2^k}$ вершин деревьев оказываются такими:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k	1	0	2	0	1	0	3	0	1	0	2	0	1	0	4
2^k	2	1	4	1	2	1	8	1	2	1	4	1	2	1	16
V	4	2	16	2	4	2	256	2	4	2	16	2	4	2	65536

Последняя строка указывает число "многочленов" периода n (приведенных по модулю два многочленов с рациональными коэффициентами и целыми значениями).

Среди $2^{12} = 4096$ функций периода $n = 12$ кольцу "многочленов" принадлежат всего 16 функций, а при периоде $n = 16$ все $2^{16} = 65536$ 16-периодических функций являются "многочленами" (степеней $0, \ldots, 15$).

Замечание. Теорему 2 можно сформулировать как описание ядер итераций оператора A,

$$\mathrm{Ker}A \subseteq \mathrm{Ker}(A^2) \subseteq \mathrm{Ker}(A^3) \subseteq \ldots \quad .$$

Эта растущая последовательность векторных подпространств $\mathbb{Z}_2^n$ стабилизируется в виде подпространства $\mathrm{Ker}(A^N) = \mathrm{Ker}(A^{N+1}) = \ldots$ с достаточно большим N. Это "стабильное ядро" мы будем обозначать $\mathrm{Ker}(A^\infty)$.

Мы докажем сейчас, что это векторное пространство над полем $\mathbb{Z}_2$ имеет размерность 2^k:

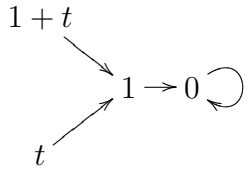
$$\mathrm{Ker}(A^\infty) \approx \mathbb{Z}_2^{2^k}, \text{ если } n = 2^k(2a+1),$$

так что число точек стабильного ядра есть

$$|\mathrm{Ker}(A^\infty)| = 2^{2^k}.$$

Эти точки, как мы сейчас докажем, образуют вершины бинарного корневого дерева $(O_1 * T_{2^{2^k}})$, о котором идет речь в теореме.

Пример. При $n = 2$ мы получаем $k = 1$ и дерево $(O_1 * T_{2^2})$, состоящее из $2^2 = 4$ вершин – "многочленов"



степени меньше 2 от переменной t. Других "многочленов" периода $n = 2$ не существует.

При $n = 12$ мы находим $k = 2$. Стабильное ядро четырёхмерно и представляет собой корневое дерево из шестнадцати "многочленов" $(O_1 * T_{2^{2^k}}) = (O_1 * T_{16})$.

Из $2^{12} = 4096$ функций x периода 12 со значениями в $\mathbb{Z}_2$ "многочленами" оказываются только эти 16 функций, притягиваемых аттрактором $x = 0$. Для этих "многочленов" $A^4x = 0$, так что их степени не превосходят 3:

$$x(t) = a_1t^3 + a_2t^2 + a_3t + a_4.$$

В качестве базиса четырёхмерного векторного пространства "многочленов" периода 12 над $\mathbb{Z}_2$ можно взять "многочлены" $C_t^0 = 1, C_t^1 = t, C_t^2 = \frac{t(t-1)}{2}, C_t^3 = \frac{t(t-1)(t-2)}{6}$, доставляющие числа сочетаний из t элементов.

Доказательство теоремы 2. Решение разностного уравнения $Ax = w$ относительно неизвестной функции x доставляется операцией "интегрирования",

$$x_{j+1} = x_j + w_j \quad (j = 1, 2, \ldots), \text{ если } x_1 \text{ задано.}$$

Выбрав начальное условие $x_1 = 0$ (либо $x_1 = 1$), мы последовательно вычисляем все значения x_i неизвестной функции.

Единственная трудность состоит в том, что результирующая функция должна иметь период n, т.е. должно выполняться соотношение $x_{n+1} = x_1$. Поскольку $x_{n+1} - x_1 = \sum_{j=1}^n w_j$, мы заключаем, что "интегрирование" доставляет искомое решение если и только если число единиц среди значений w_j четно.

Например, единственные 2 решения уравнения $Ax = 0$ доставляются постоянными функциями $x = 0$ и $x = 1$, так как $w = 0$ не принимает значения 1 и число единиц в $w = 0$ четно.

Итак, ядро $\mathrm{Ker}A = \mathbb{Z}_2$ состоит из двух постоянных функций 0 и 1.

Для вычисления $\mathrm{Ker}(A^2)$ приходится решать уравнение $Ax = 1$ $(\in \mathrm{Ker}A)$. Если число n нечетно, то решений нет, т.е. $\mathrm{Ker}(A^2) = \mathrm{Ker}A$, так как число единиц в последовательности в правой части равно n и нечетно. Если же число n четно, то "интегрирование" доставляет последовательность $x = (0, 1, 0, 1, 0, 1, \ldots)$ при начальном условии $x_1 = 0$ и последовательность $x = (1, 0, 1, 0, \ldots)$ при начальном условии $x_1 = 1$.

Продолжая в этом случае “интегрирование” повторно, мы последовательно вычисляем всё бóльшие ядра до тех пор, пока в правой части не появится функция w с нечетным числом значений 1 (у которой нет n-периодического “интеграла”).

Основное утверждение теоремы 2 состоит в том, что это препятствие встретится нам *одновременно* на всех ветвях бинарного корневого дерева последовательных “интегралов”. Из-за этого стабильное ядро окажется множеством всех вершин бинарного корневого дерева, а не какой-то его части. Мы увидим также, что в момент остановки число этажей получаемого стабильного дерева окажется степенью двойки.

Предположим, что дерево прообразов нуля при r итерациях оператора A содержит цепочку независимых элементов

$$w_r \to w_{r-1} \to \ldots \to w_2 \to w_1 \to 0\,,$$

причем пространство $\mathrm{Ker}(A^{r-1})$ состоит из 2^{r-1} функций

$$z = \varepsilon_1 w_1 + \ldots + \varepsilon_{r-1} w_{r-1}\,, \quad \varepsilon_j \in \mathbb{Z}_2\,.$$

Тогда для векторов r-мерного пространства комбинаций

$$x = \lambda_1 w_1 + \ldots + \lambda_r w_r$$

мы находим

$$Ax = \sum_{j=1}^{r} \lambda_j w_{j-1} \in \mathrm{Ker}(A^{r-1}),$$

так что $\dim \mathrm{Ker}(A^r) = r$. Итак, зная один элемент w_r r-го этажа бинарного дерева “интегралов”, мы получаем их полный набор, проектирующийся оператором A в полный набор элементов предыдущего этажа. В каждый элемент $r-1$-го этажа проектируются два элемента x r-го этажа. Действительно, выбор $\lambda_1 = 0$ и 1 в x приводит в Ax к одному элементу, поскольку $Aw_1 = 0$.

Остается сосчитать, на каком этаже впервые встретится функция w_r с нечетным числом значений 1.

С этой целью мы явно проведем итерированное “интегрирование” функции $x \equiv 1$ периода n.

Эти интегралы доставляются треугольником Паскаля

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & & \ldots & & \ldots & & \ldots & & \ldots & & \\
C_i^0 & & & C_i^1 & & C_i^2 & & \ldots & & C_i^i\,. &
\end{array}$$

Тождество $C_{i+1}^j = C_i^j + C_i^{j-1}$, определяющее треугольник Паскаля, показывает, что разности j-й косой строки C_{t+j}^j $(t = 1, 2, 3, \ldots)$ образуют предыдущую косую строку (номер $j-1$).

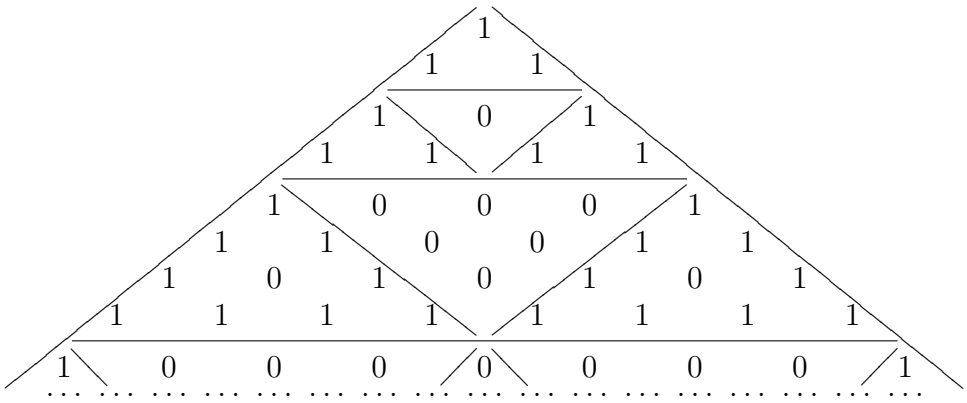
Соотношение верно и для вычетов по модулю 2, так что $A\{C_{t+j}^j\} = \{C_{t+j-1}^{j-1}\}$ (при фиксированном j).

Поэтому все итерированные "интегралы" (с начальным условием $C_{t+j}^j = 1$ при $t = 0$) – это приведенные по модулю 2 косые линии треугольника Паскаля, на которых $j = 0$ для исходной функции $w_1 = C_t^0 \equiv 1$, а затем, по мере повторного "интегрирования", ответы $w_2, w_3, \ldots$ доставляют косые линии с $j = 1, 2, \ldots$.

Следовательно, для выяснения того, сколько раз удастся "проинтегрировать" функцию w_1 в классе n-периодических функций остается выяснить, при каких значениях j функция $C_i^j \pmod 2$ аргумента i будет иметь период n.

Лемма. *Если $2^{k-1} \le j < 2^k$, то наименьший период функции $C_i^j \pmod 2$ по i равен 2^k.*

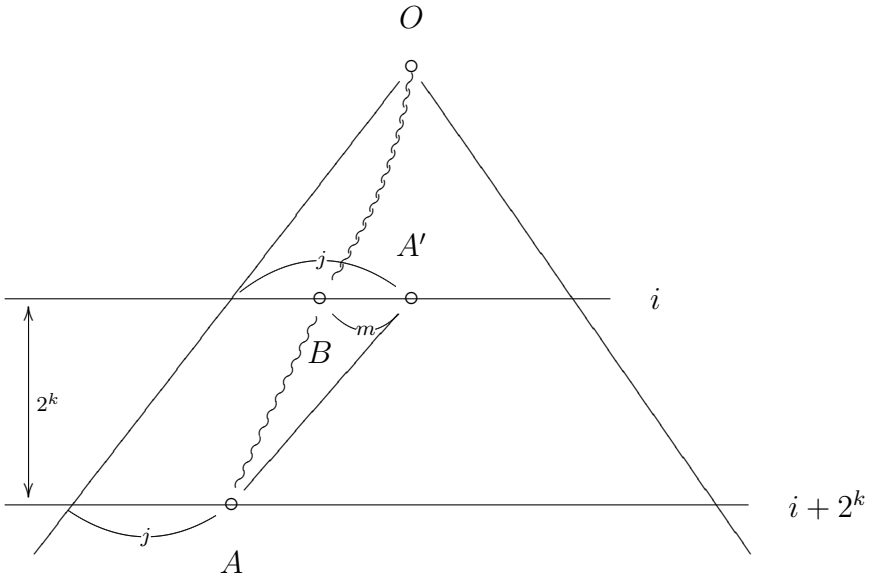
Пример. Приведенный по модулю 2 треугольник Паскаля



показывает при $j = (0), (1), (2, 3), (4, 5, 6, 7), 8$ периоды $(1), (2), (4, 4), (8, 8, 8, 8), 16$.

Доказательство леммы. Проверим сначала, что число 2^k является периодом при $j < 2^k$:

$$C_{i+2^k}^j \equiv C_i^j \pmod 2 \text{ при } j < 2^k, i \ge j\,.$$



Число $C^j_{i+2^k}$ есть число монотонно-решеточных путей из O в A. Каждый такой путь пересекает уровень горизонтали i в одной из точек B, для которой расстояние до точки A' равно m, где $0 \le m \le j < 2^k$. Числа путей AB и BO суть $C^m_{2^k}$ и C^{j-m}_i. Поэтому общее число монотонно-решеточных путей из O в A выражается суммой произведений

$$(*) \qquad C^j_{i+2^k} = \sum_{m=0}^{j} (C^m_{2^k}\, C^{j-m}_i).$$

Первый сомножитель $C^m_{2^k} = \frac{2^k}{m} C^{m-1}_{2^k-1}$ чётен при $0 < m < 2^k$, поэтому при $j < 2^k$ вся сумма сравнима по модулю два со слагаемым, для которого $m = 0$:

$$C^j_{i+2^k} \equiv C^0_{2^k}\, C^j_i = C^j_i \pmod 2.$$

Итак, число 2^k является одним из периодов функции $C^j_i \pmod 2$ аргумента i, если $j < 2^k$.

Покажем, что это – наименьший период, если вдобавок $2^{k-1} \le j$. Меньший период должен бы быть делителем числа 2^k, поэтому мы проверим, что число 2^{k-1} – не период.

Докажем, что при $2^{k-1} \le i < 2^k$ число сочетаний $K = C^i_{i+2^{k-1}}$ четно.

Введем обозначение $I = i - 2^{k-1}$, так что $0 \le I < 2^{k-1}$. В этих обозначениях

$$K = C^i_{I+2^k} = C^{I+2^{k-1}}_{I+2^k} = C^{2^{k-1}}_{I+2^k}.$$

По формуле $(*)$

$$(**) \qquad K = \sum_m (C^m_{2^k}\, C^{2^{k-1}-m}_I),$$

где $0 \le 2^{k-1} - m \le I$, то-есть $2^{k-1} + I \le m \le 2^{k-1}$. Из этих неравенств следует, что $0 < m < 2^k$. Поэтому биномиальный коэффициент $C^m_{2^k}$ четен, а значит доставляемая формулой $(**)$ сумма K четна.

С другой стороны, $C^i_i = 1$. Поэтому *число* 2^{k-1} *не является периодом функции* $C^j_i \pmod 2$ *по переменной* i, *когда* $2^{k-1} \le j < 2^k$: при этом условии $C^j_{j+2^{k-1}} \equiv 0(2)$, $C^j_j \equiv 1(2)$.

Из доказанного выделенного выше утверждения следует, что *число* 2^{k-1} *не является периодом ни при каком* $j \ge 2^{k-1}$ (ведь если бы число 2^{k-1} было периодом, то и число $2^{k'-1}$, где $k' > k$, было бы периодом, вопреки выделенному утверждению с нужным k' вместо k).

Теорема 2 вытекает из доказанных утверждений следующим образом. Если $n = 2^k(2a+1)$, то построение бинарного дерева $\mathrm{Ker}(A^r)$, описанного выше, будет успешным до тех пор, пока "j–кратные интегралы" $C^j_{i+j} \pmod 2$ от $w_1 \equiv 1$ будут оставаться n–периодическими функциями от аргумента i.

Из доказанных сравнений видно, что наименьший период указанной функции переменной i равен 2^r при $2^{r-1} \le j < 2^r$. Чтобы эта функция была n–периодической, нужно, чтобы число $n = 2^k(2a+1)$ делилось на наименьший период, т.е. чтобы $r \le k$. Стало быть, стабильное ядро есть $\mathrm{Ker}(A^\infty) = \mathrm{Ker}(A^k) \approx (\mathbb{Z}_2)^{2^k}$, что и доказывает теорему 2.

Теорема 3. *Дерево, притягиваемое каждой точкой каждого цикла графа оператора взятия разностей* $A : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$, *изоморфно дереву, притягиваемому точкой* $x = 0$ *(т.е. бинарному дереву* $T_{2^{2^k}}$ *компоненты* $\mathrm{Ker}(A^\infty) \approx (O_1 * T_{2^{2^k}})$ *теоремы 2).*

Замечание 1. В частности, *оснащение циклов всех компонент графа лесами аттракторов однородно: все оснащающие цикл корневые деревья одинаковы и всякая компонента графа имеет вид* $(O_m * T_{2^{2^k}})$, *когда* $n = 2^k(2a+1)$.

Замечание 2. *Число всех вершин всех циклов графа является степенью двойки: по теореме* 3,

$$\mathrm{Im}(A^\infty) \simeq \mathbb{Z}_2^{n-\dim \mathrm{Ker}(A^\infty)},$$

$$|\mathrm{Im}(A^\infty)| = 2^{n-2^k}.$$

Пример. При $n = 11$ мы получаем $k = 0$ и на четырех циклах $3 \cdot 341 + 1 = 1024 = 2^{11-1}$ вершин.

При $n = 12 = 2^2 \cdot 3$ имеем $k = 2, 2^k = 4, n - 2^k = 8$. Число вершин всех 24 циклов таблицы стр. 3 есть

$$20 \cdot 12 + 2 \cdot 6 + 1 \cdot 3 + 1 \cdot 1 = 256 = 2^8.$$

Доказательство теоремы 3. Объединение всех циклов есть векторное подпространство, к которому стабилизируется убывающая последовательность образов

$$\mathrm{Im}A \supseteq \mathrm{Im}(A^2) \supseteq \ldots \supseteq \mathrm{Im}(A^N) = \mathrm{Im}(A^{N' \geq N}) \subseteq \mathbb{Z}_2^n.$$

Обозначая этот "стабильный образ" через $\mathrm{Im}(\mathrm{A}^\infty)$, мы видим, что

$$\mathrm{Im}(A^\infty) \cong \mathbb{Z}_2^n / (\mathrm{Ker}(A^\infty)),$$

что и доказывает утверждение замечания 2.

Для доказательства теоремы 3 заметим, что для любого линейного оператора $L : V \longrightarrow W$ решения неоднородного уравнения являются аффинными подпространствами, параллельными ядру оператора:

$$L^{-1}(w) = v + \mathrm{Ker}\, L, \quad \text{если } Lw = v.$$

Для каждой точки x цикла $C \approx O_m$

$$C : \ldots \longrightarrow w_2 \longrightarrow w_1 \longrightarrow x \longrightarrow \ldots$$

графа оператора взятия разностей $A : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ мы находим прообразы, являющиеся аффинными подпространствами

$$A^{-1}x = w_1 + \mathrm{Ker}A,$$

$$A^{-s}x = w_s + \mathrm{Ker}(A^s),$$

откуда видно, что весь бассейн, притягиваемый циклом C, расслоен на аффинные подпространства

$$W_s = w_s + \mathrm{Ker}(A^\infty)(s = 1, \ldots, m) :$$

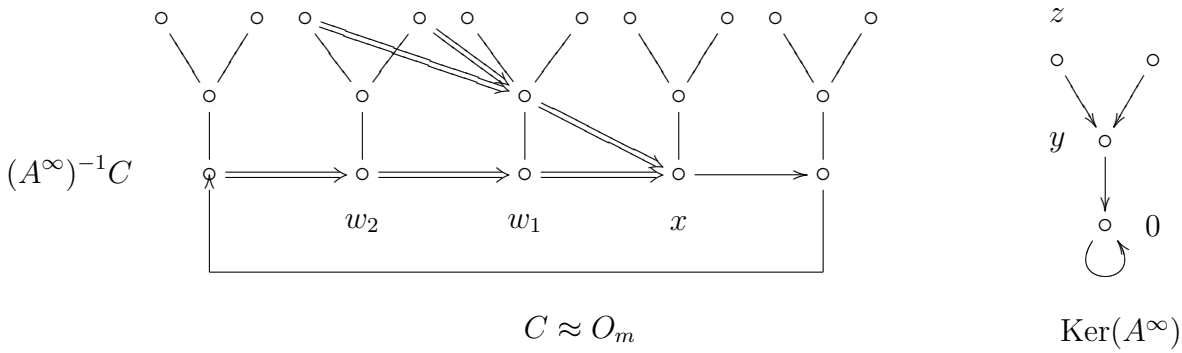
$$(A^\infty)^{-1}C = \bigcup_{s=1}^{m} W_s.$$

В этом смысле мы можем ввести на бассейне цикла $C \approx O_m$ координаты $s \in \mathbb{Z}_m$ и $y \in \mathrm{Ker}(A^\infty)$. Действие оператора A записывается в этих координатах так:

$$A(s, y) = ((s-1), Ay).$$

Иными словами, на прямом произведении $(O_m \times T_{2^{2^k}})$ оператор действует перекошенным образом, причем подграф графа оператора взятия разностей $A : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ на бассейне цикла C_m (т.е. компонента связности этого цикла в полном графе) изоморфен произведению $(O_m * T_{2^{2^k}})$, если $n = 2^k(2a+1)$.

Пример. Перекошенное действие изображено ниже (для $m = 5, k = 1$) двойными стрелками:



$C \approx O_m$ $\qquad\qquad$ $\mathrm{Ker}(A^\infty)$

В этом примере $A(w_2, z) = (w_1, y), A(w_1, y) = (x, 0), A^2(w_2, z) = x$.

Мы описали таким образом изоморфизм притягиваемого корнем $x \in C$ дерева стандартному бинарному дереву $\mathrm{Ker}(A^\infty)$, чем теорема 3 и доказана (вместе с замечанием 1 об однородности оснащения циклов лесами, составляющими их бассейны).

Замечание. Аналогичное утверждение об однородности было доказано ранее [1] для операции $x \to x^2$ в произвольной конечной группе. Я не знаю общего результата, содержащего теорему 3 вместе с этим фактом теории конечных групп.

Таблица стр. 3 подсказывает много других общих утверждений, кроме доказанных выше теорем 2 и 3. Например, *наибольшая из длин циклов компонент O_m графа оператора взятия разностей $A : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ делится* (в каждом из рассмотренных в таблице случаев) *на n.*

Пример. При $n = 11$ получается удивительный факт $341 = 11 \cdot 31$, опровергающий древне-китайскую гипотезу, согласно которой $2^u - 2$ делится на u только при простых u.

Делимость при простых u есть утверждение малой теоремы Ферма, число $u = 341$ является первым (наименьшим) контрпримером к попытке обращения этой теоремы Ферма.

Замечание. Делимость на n наибольшего периода $m > 1$ цикла O_m может объясняться симметрией δ порядка n, действующей на всем графе операции взятия разностей $A = 1 + \delta$ ввиду коммутирования $A\delta = \delta A$.

Однако я не нашел ни объяснения тому факту, что частное от деления наибольшего периода $m > 1$ на величину n оказывается уменьшенной на 1 степенью двойки, $m/n = 2^{q(n)} - 1$, ни разумной гипотезы о величине числа $q(n)$: по таблице стр. 3 при $n \le 12$ имеем

n	3	5	6	7	9	10	11	12
m	3	15	6	7	63	30	341	12
m/n	1	3	1	1	7	3	31	1
q	1	2	1	1	3	2	5	1

Упомянутая выше делимость числа $2^{341}-2$ на 341 вытекает из делимости периода $m=341$ на $n=11$ так:

$$2^5 \equiv -1(11), 2^5 \equiv 1(31).$$

Поэтому $2^{10} \equiv 1(11)$ и $2^{10} \equiv 1(31)$, так что $2^{31} \equiv 2(11), 2^{31} \equiv 2(31), 2^{11} \equiv 2(11), 2^{11} \equiv 2(31)$. Значит по модулю 31 имеем $2^{341} \equiv (2^{11})^{31} \equiv 2^{31} \equiv 2$ и по модулю 11 имеем $2^{341} \equiv (2^{31})^{11} \equiv 2^{11} \equiv 2$.

Поэтому число $2^{341}-2$ делится и на 31, и на 11, а значит делится и на 341.

Замечание. Если наибольший (при данном n) период есть m, то периоды $m' > 1$ остальных циклов таблицы на стр. 3 с этим n являются делителями длины m длиннейшего цикла.

Частные m/m' в большинстве случаев (например, при $n=12$) являются степенями двойки, но для $n=9$ таблица стр. 3 дает $m/m' = 63/3 = 21$, поэтому я не решаюсь формулировать общих гипотез об этих частных (целочисленность которых уже не очевидна).

Все эти вопросы касаются, естественно, жордановых нормальных форм линейных операторов A в конечных векторных пространствах.

Пример. Определим при $n = p-1$, где p простое, специальную арифметически-логарифмическую функцию $l \in \mathbb{Z}_2^n$ со значениями (при $k = 1, 2, \ldots, n$)

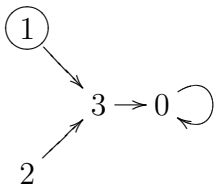
$$\begin{cases} l_k = 0, & \text{если } k \text{ квадратичный вычет по модулю } p, \\ l_k = 1, & \text{если } k \text{ квадратичный невычет по модулю } p. \end{cases}$$

Наши таблицы показывают, что сложность этой функции достигает наибольшего или почти наибольшего значения (среди всех функций со значениями 0 и 1 периода n).

Для упрощения записи орбит мы будем считать последовательность $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$ бинарной записью числа $X = x_1 2^{n-1} + x_2 2^{n-2} + \ldots + x_n$.

Ниже для $p = 3, 5, 7, 11$ и 13 (т.е. $n = 2, 4, 6, 10, 12$) приведены компоненты связности арифметического логарифма l.

Случай $p = 3, n = 2$. Имеем $\log_2 1 = 0$, $\log_2 2 = 1$, поэтому $l = (0,1), L = 0 \cdot 2 + 1 = 1$. Единственная компонента $(O_1 * T_4)$ имеет (в обозначениях X) вид



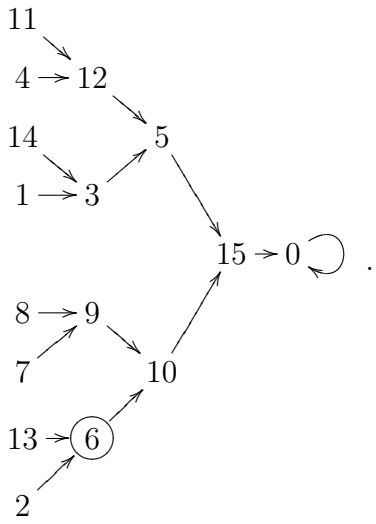
Арифметический логарифм $L = 1$ – самая сложная точка графа (наиболее удаленная от цикла).

Случай $p = 5, n = 4$. Имеем по модулю 5

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1.$$

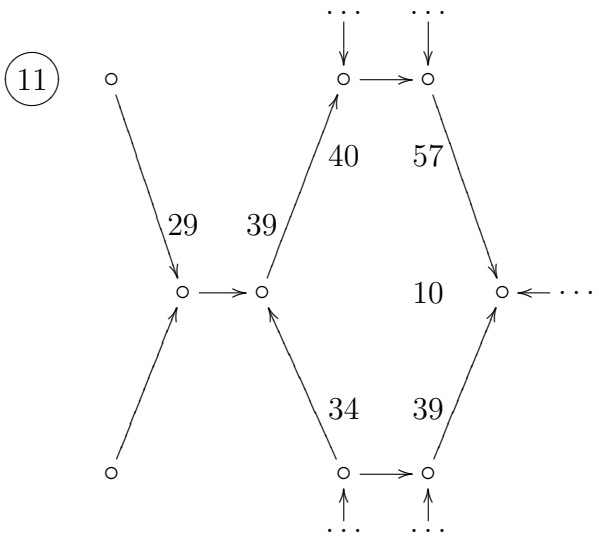
Поэтому $\log_2 1 = 4, \log_2 2 = 1, \log_2 3 = 3, \log_2 4 = 2$. Итак, арифметический логарифм есть последовательность $l = (0,1,1,0), L = 6$.

Единственная компонента $(O_1 * T_{16})$ графа оператора A для $n = 4$ есть бинарное корневое дерево (многочленов степени меньше 4), которое в X – обозначениях имеет вид



Обведенная кружком вершина L является почти самой сложной точкой графа (расстояние до цикла почти максимально).

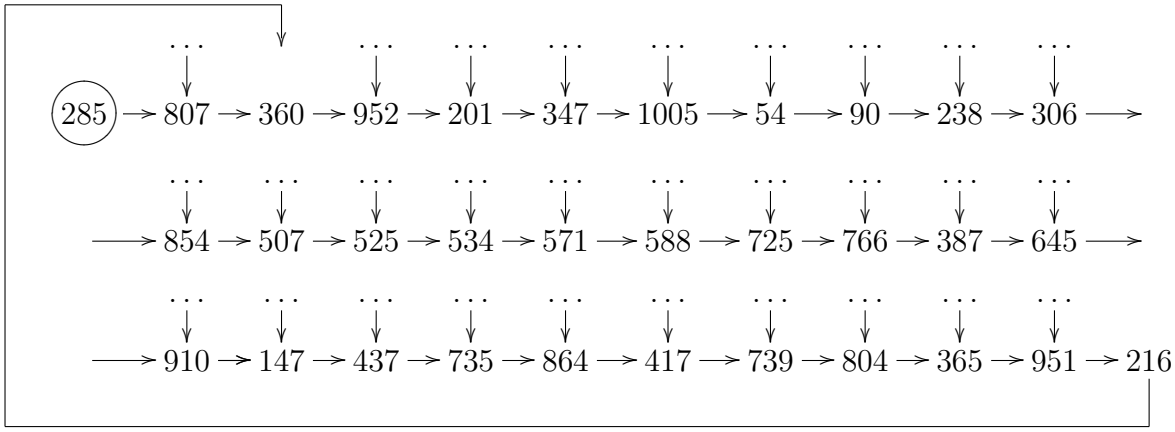
Случай $p = 7, n = 6$. Вычисления, аналогичные приведенным выше(для логарифмов по основанию первообразного вычета, например для $\log_3$) проводят к арифметическому логарифму $L = 11$. Его компонента графа, $O_6 * T_4$ – самая сложная (см. таблицу на стр. 3), и орбита точки L состоит, в X-обозначениях, из следующих вершин:



Таким образом, логарифмическая вершина $L = 11$ – самая сложная точка графа (она наиболее удалена от цикла и принадлежит наибольшей компоненте графа).

Случай $p = 11, n = 10$. Здесь вычет 2 первообразен и поэтому годятся двоичные логарифмы. Геометрическая прогрессия вычетов степеней двойки по модулю 11 доставляет последовательность $(2, 4, 8, 5, 10, 9, 7, 3, 6, 1)$. Следовательно, арифметический логарифм есть функция $l = (0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$, так что $L = 256 + 16 + 8 + 4 + 1 = 285$.

Его компонента графа, $O_{30} * T_4$ – самая сложная при $n = 10$. Орбита арифметического логарифма $L = 285$ состоит из следующих 32 точек (в X-обозначениях):



Логарифм L имеет максимальную сложность среди всех функций периода $n = 10$: вершина принадлежит наибольшей компоненте и наиболее удалена от цикла.

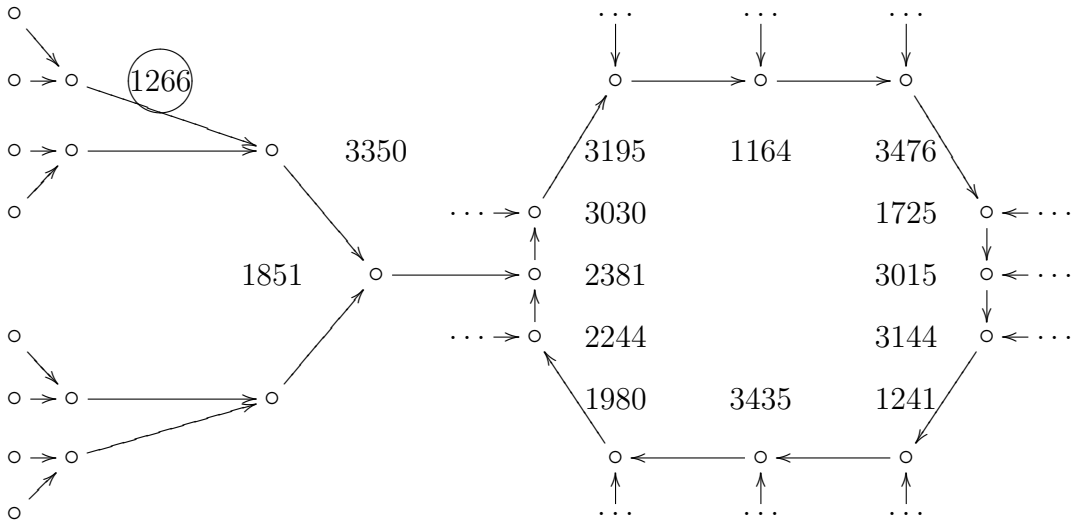
Случай $p = 13, n = 12$. Вычет $2 \pmod{13}$ первообразен, геометрическая прогрессия степеней двойки доставляет арифметические логарифмы вычетов $k = 1, 2, \ldots, 12$ равные

$$\log_2 k = (12, 1, 4, 2, 9, 5, 11, 3, 8, 10, 7, 6),$$

т.е.

$$l = (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0,),$$

откуда $L = 1266$. Эта вершина принадлежит наибольшей компоненте графа, имеющей вид $(O_{12} * T_{16})$. Орбита логарифмической функции L состоит из следующих 15 вершин:



Логарифмическая функция L оказывается почти наиболее сложной среди всех 4096 функций периода 12 со значениями 0 и 1: вершина L принадлежит наибольшей компоненте связности и расположена на одном из деревьев её леса на почти максимальном удалении от корня.

Список литературы

[1] В. И. Арнольд, *Топология и статистика арифметических и алгебраических формул*, Успехи математических наук **58**(2003), №4, 3–28 (особенно §6, с. 15–18).