

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 16 Выпуск 2 (2015)

УДК 512.532+519.142+517.43

БАЗИСЫ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ф. М. Малышев (г. Москва)

Аннотация

В работе приводится обзор результатов (с разной степенью подробности) по трём различным направлениям.

Основное центральное направление относится к рекуррентным последовательностям, прежде всего к их базисным (в различном понимании) множествам.

Другое направление связано с новыми комбинаторными объектами – (v, k_1, k_2) -конфигурациями, возникающими на пути ослабления условий, определяющих известные комбинаторные объекты – (v, k, λ) -конфигурации.

Третье направление имеет дело с инвариантными дифференциалами высших порядков от нескольких гладких функций одной вещественной переменной.

В каждой из этих тем рассматриваемые вопросы связаны с комбинаторными конфигурациями в виде конечных плоскостей, а приводимые результаты получены благодаря однотипным представлениям точек соответствующих конфигураций точками многомерных локально евклидовых пространств. В случае инвариантных дифференциалов эти представления возникают естественно, а в случае рекуррентных последовательностей и (v, k_1, k_2) -конфигураций вводятся по аналогии, но уже искусственным образом.

Ключевые слова: рекуррентные последовательности, решётки, торы, комбинаторные конфигурации, инвариантные дифференциальные операторы.

Библиография: 39 названий.

BASES OF RECURRENT SEQUENCES

F. M. Malyshev (Moscow)

Abstract

This paper provides an overview of the results (with varying degrees of detail) in three different directions.

The main Central direction refers to recurrent sequences, primarily to their base (in a different sense) sets.

Another direction is related to new combinatorial objects (v, k_1, k_2) -configurations encountered on the way of weakening the determinants of well-known combinatorial objects (v, k, λ) -configuration.

The third direction deals with invariant differentials of higher orders from several smooth functions of one real variable.

In each of these themes the issues associated with combinatorial configurations in the form of finite planes, and the results obtained through the same type of views, points of the corresponding configurations of points in multidimensional locally Euclidean spaces. In the case of invariant differentials of these representations arise naturally, and in the case of recurrent sequences and (v, k_1, k_2) -configurations are introduced by analogy, but in an artificial way.

Keywords: recurrent sequences, lattices, Torah, combinatorial configuration, invariant differential operators.

Bibliography: 39 titles.

1. Введение

Основное содержание предлагаемого обзора относится к рекуррентным последовательностям. Приводимые результаты относительно порождающих множеств в рекуррентных последовательностях получены благодаря дополнительно вводимой многомерной структуре на множестве индексов, нумерующих элементы последовательности. Во введении приводится краткий обзор других примеров использования многомерных структур на дискретных нумерующих множествах, изначально мыслимых одномерными, линейно упорядоченными.

В качестве эпиграфа к настоящему обзору можно отнести высказывание со стр. 15 учебника [1] о том, что базисные векторы линейных пространств "*совершенно не обязательно*" нумеровать от 1 до n . Там подчёркивалось, что при решении конкретных задач вместо линейного упорядочения "*может оказаться важной другая структура на множестве индексов базиса*", а собственно линейная упорядоченность, добавим, может оказаться даже вредной.

Аналогичная ситуация имеет место с определениями декартова произведения семейств множеств, где также не всегда полезна линейная упорядоченность на множестве, индексирующем семейство "сомножителей" [2]. Элементы декартова произведения конечного или счётного числа множеств совсем не обязательно представлять упорядоченной последовательностью. Каждая решаемая задача, как правило, требует своей присущей именно ей какой-либо структуры на множестве индексов.

Впервые на важность этих замечаний автор обратил внимание в связи с одной из задач доклада [3] по описанию инвариантных дифференциалов

$$d(f_1(x), \dots, f_k(x))$$

порядка $k + r$ от гладких вещественных функций $f_1(x), \dots, f_k(x)$:

$$d(f_1(x), \dots, f_k(x)) = \sum_{\substack{i_1 \geq 0, \dots, i_k \geq 0 \\ i_1 + \dots + i_k = r}} c_{i_1 \dots i_k} f_1^{(1+i_1)}(x) \dots f_k^{(1+i_k)}(x) (dx)^{k+r}, \quad (1)$$

где $c_{i_1 \dots i_k} \in \mathbb{R}$ – некоторые определяющие дифференциал коэффициенты. В случае гладких замен переменной $x = x(t)$ данный дифференциал $d(\varphi_1(t), \dots, \varphi_k(t))$ от функций $\varphi_j(t) = f_j(x(t))$, $j = 1, \dots, k$, следует вычислять по формуле (1), в которой вместо $f_j^{(1+i_j)}(x)$ должны быть производные $\varphi_j^{(1+i_j)}(t) = \left(\frac{d}{dt}\right)^{1+i_j}(\varphi_j(t))$, а вместо $(dx)^{k+r}$, соответственно, $(dt)^{k+r}$. Но можно непосредственно в правую часть выражения (1) вместо x подставить $x(t)$ (тогда $f_j^{(1+i_j)}(x)$ заменяется на $f_j^{(1+i_j)}(x(t))$), а вместо $(dx)^{k+r}$, соответственно, $(dx(t))^{k+r} = (\dot{x}(t)dt)^{k+r} = \dot{x}(t)^{k+r}(dt)^{k+r}$. Дифференциал (1), задаваемый коэффициентами $c_{i_1 \dots i_k}$, является инвариантным, если результаты вычислений по этим двум схемам дают одинаковые выражения для любых функций $f_1(x), \dots, f_k(x)$ и замен $x(t)$. Отдельное ненулевое слагаемое в (1) является инвариантным дифференциалом только при $r = 0$, поскольку дифференциал $f^{(1+i)}(x)(dx)^{1+i}$ является инвариантным только при $i = 0$. При $k = 1$, $r = 0$ дифференциал (1) инвариантен по известной теореме об инвариантности первого дифференциала. Непосредственно проверяется, что инвариантным является дифференциал

$$d(f_1(x), f_2(x)) = (f_1'(x)f_2''(x) - f_1''(x)f_2'(x))(dx)^3.$$

Необходимые и достаточные условия на коэффициенты $c_{i_1 \dots i_k}$ для инвариантности дифференциала (1) в работе [4] сформулированы на языке однородных уравнений в частных производных многочленов от k переменных. Эти условия сводятся (см. [5]) к системе из $b = \binom{k+r-1}{k}$ линейных уравнений с $v = \binom{k+r-1}{r}$ неизвестными $c_{i_1 \dots i_k}$, причём в каждом уравнении k неизвестных, а каждое неизвестное участвует в r уравнениях, $vr = bk$. Совокупность из v неизвестных образует конечную плоскость [6] с b "прямыми", состоящими из k точек. Каждая точка плоскости содержится ровно в r "прямых". Приписывание в работе [5] неизвестных $c_{i_1 \dots i_k}$ к точкам $(i_1, \dots, i_k) \in \mathbb{N}_0 \subset \mathbb{R}^k$ высветило особенности этой системы, указывающие на способ её решения. После введения новых переменных $\tilde{c}_{i_1 \dots i_k} = i_1! \dots i_k! c_{i_1 \dots i_k}$ система предстаёт в виде

$$\sum_{j=1}^k (i_j + \delta + 1) \tilde{c}_{i_1 \dots i_{j-1}, i_j + \delta, i_{j+1}, \dots, i_k} = 0,$$

$\delta = 1, \dots, r$, $i_1 \geq 0, \dots, i_k \geq 0$, $i_1 + \dots + i_k = r - \delta$. В работе [5] доказано, что верхними оценками для размерностей пространств решений этих систем при разных k и r выступают величины $a_{k,r}$, определяемые равенством $\sum_{i \geq 0} a_{k,i} = (1+t)(1+t+t^2) \dots (1+t+\dots+t^{k-1})$. Отсюда следует, что Вронскиан $\det \left\| f_j^{(i)} \right\|_{i,j=1,\dots,k} (dx)^{\frac{k(k+1)}{2}}$ является инвариантным дифференциалом для k функций самого высокого возможного порядка.

Полезная для нахождения инвариантных дифференциалов $(k-1)$ -мерная структура на номерах $(i_1, \dots, i_k)$ неизвестных $c_{i_1 \dots i_k}$ присутствует в явном виде, оставалось только её использовать.

Ситуация иная в случае рекуррентных последовательностей $x_i \in X$, $i \in \mathbb{Z}$, рассматриваемых в настоящей работе в общем виде:

$$x_{i+m} = f(x_i, x_{i+s_1}, \dots, x_{i+s_{k-2}}), \quad (2)$$

$k \geq 3$, $0 < s_1 < \dots < s_{k-2} < m$, $\text{НОД}(s_1, \dots, s_{k-2}, m) = 1$. Алфавит X и отображение $f : X^{k-1} \rightarrow X$, задающие рекуррентное соотношение (2), могут быть произвольными.

Через v обозначаем минимальный период последовательности $\{x_i, i \in \mathbb{Z}\}$: $x_{i+v} = x_i$, $i \in \mathbb{Z}$. При отсутствии конечного периода считаем $v = \infty$. Здесь "прямые" $\{i, i + s_1, \dots, i + s_{k-2}, i + m\}$, $i \in \mathbb{Z}_v$, образуют конечную плоскость с параметрами $b = v$, $r = k$ на множестве вычетов $\mathbb{Z}_v = \{0, 1, \dots, v-1\} = \mathbb{Z}/\langle v \rangle$. Считаем $\mathbb{Z} = \mathbb{Z}_\infty$.

Группы по сложению $\mathbb{Z}$ и $\mathbb{Z}/\langle v \rangle$ из-за их естественных вложений соответственно в $\mathbb{R}$ и $\{z \in \mathbb{C}, |z| = 1\}$, обычно представляются одномерными. Но конкретные приложения рекуррентных последовательностей и удачный пример с инвариантными дифференциалами инициировали искусственное введение $(k-1)$ -мерных структур на $\mathbb{Z}$ и $\mathbb{Z}_v$ путём их дискретных вложений в $(k-1)$ -мерные цилиндр и тор соответственно. Такие вложения обеспечиваются эпиморфизмами

$$\varphi : \mathbb{Z}^{k-1} \rightarrow \mathbb{Z}_v, \varphi(z_0, z_1, \dots, z_{k-2}) = (mz_0 + s_1z_1 + \dots + s_{k-2}z_{k-2}) \bmod v,$$

при которых $\mathbb{Z}_v \cong \mathbb{Z}^{k-1} / \ker \varphi \subset \mathbb{R}^{k-1} / \ker \varphi$. Данные вложения позволили (см. §§ 2 – 6) определить строение всех возможных минимальных подмножеств элементов последовательности $\{x_i, i \in \mathbb{Z}\}$, по которым каждый знак x_j , $j \geq 0$, может быть получен за конечное число применений рекуррентного соотношения (2). Такие подмножества названы базисными в [7].

Случаю $k = 3$ дополнительно посвящена работа [8]. Он рассматривается в § 7 особо. Возникающее семейство вложений $\mathbb{Z}$ в цилиндр для всех пар (s_1, m) , $0 < s_1 < m$, $(s_1, m) = 1$, устанавливает в работе [9] связь между известным разбиением на фундаментальные области верхней комплексной полуплоскости при действии модулярной группой и приёмом (в плоском случае) максимального пустого шара Делоне – Сандаковой [10].

Ещё одно приложение связано с приводимым ниже рис. 1, взятым из работы [11] по клеточным автоматам. Там на местах $(i, j) \in \mathbb{Z}^2$ располагаются значения $z_{i,j} \in GF(2)$ (0 – светлая клетка, 1 – тёмная) так, что $z_{i-1,j} + z_{i,j} + z_{i,j+1} = 0$. На самой нижней горизонтальной линии эти значения выбирались псевдо случайным образом.

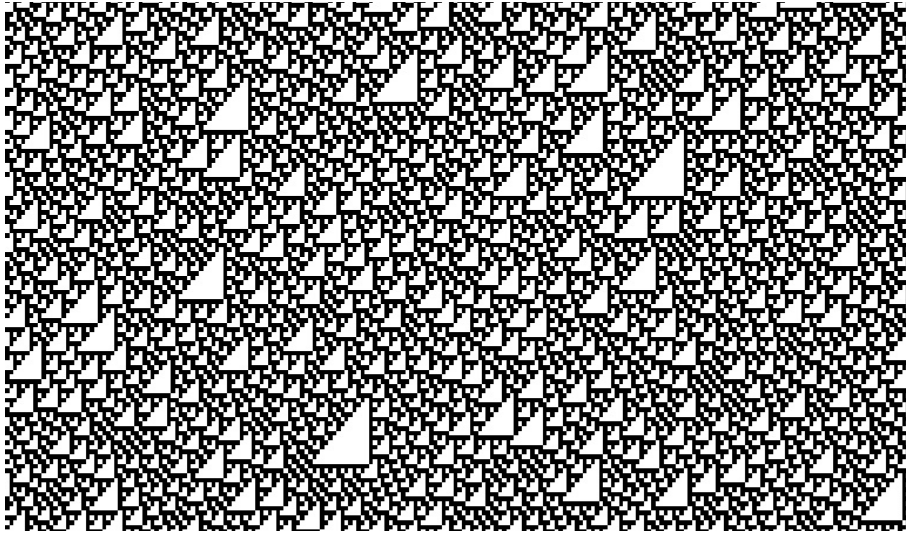


Рис. 1

Аналогичная картина будет иметь место и для рекуррентных последовательностей при $k = 3$, $X = GF(2)$, $f(x, y) = x + y$, если вложение $\mathbb{Z}$ в цилиндр таково, что номера $t, t + s_1, t + m$ знаков x_t, x_{t+s_1}, x_{t+m} оказываются соответственно на местах $(i - 1, j), (i, j), (i, j + 1)$ плоской развёртки цилиндра. Данное обстоятельство как раз и предопределило представление вычетов $\mathbb{Z}_v$ точками многомерных торов.

Наблюдаемая на рис. 1 закономерность позволила, в частности, получить теоремы о распределении в левой зоне числа единиц в булевых аналогах треугольников Паскаля [12].

В случае решёток $\Gamma \subset \mathbb{Z}^{k_1-1}$ максимального ранга вложения групп $\mathbb{Z}^{k_1-1}/\Gamma$ в торы $\mathbb{R}^{k_1-1}/\Gamma$ позволяют строить относительно новые комбинаторные объекты, так называемые (v, k_1, k_2) -конфигурации. Каждая такая конфигурация задаётся парой конечных плоскостей на одном и том же множестве из v точек с $b = v$ "прямыми", состоящими из k_1 точки в одной плоскости и из k_2 точек в другой плоскости. В первой плоскости через одну точку проходит $r_1 = k_1$ "прямых", а во второй, соответственно, $r_2 = k_2$ "прямых". Матрицы инцидентности этих плоскостей должны быть невырожденными над полем $GF(2)$ и взаимно обратными. При $k_1 = k_2 = k$ используется обозначение (v, k) -конфигурация. Если в качестве "прямых" выступают смежные классы подмножеств в группе G мощности соответственно k_1, k_2 , то (v, k_1, k_2) -конфигурацию называем (v, k_1, k_2) -группой, а при $k_1 = k_2 = k$ — (v, k) -группой.

Первоначальные примеры (v, k) -конфигураций были получены в работе [13]. При их построении привлекались известные по монографиям [14] – [18] (v, k, λ) -конфигурации, матрицы Адамара, конечные проективные плоскости, совершенные разностные множества, теоретико-числовые конструкции, графы с различными свойствами симметрии, однородные многогранники, триангуляции двумерных торов, связанные с расположением на них вычетов $\mathbb{Z}_v$, описываемыми выше в случае $k = 3$. Построением (v, k_1, k_2) -конфигураций в разное время занимались М. В. Брославский, А. М. Зубков, Е. Г. Красулина, Ф. М. Малышев, В. Н. Сачков, В. Е. Тараканов, А. Е. Тришин, А. А. Фролов.

К настоящему времени удалось показать, что каждая связная $(v, 3)$ -конфигурация реализуется на группе $\mathbb{Z}_v$ "прямыми" $\{i, i + 1, i + 1 + v/2\}$, $i \in \mathbb{Z}_v$, при чётном v , и триангуляцией листа Мёбиуса при $v = 5$. Доказательство этого утверждения в работе [19] продемонстрировало важность отсутствия структуры линейного упорядочения на множестве из v точек соответствующих конечных геометрий, упорядоченность скрывала бы инвариантные рассуждения при доказательстве. В практических приложениях (v, k_1, k_2) -конфигурации выступают в виде их матриц инцидентности, называемых (v, k_1, k_2) -матрицами и (v, k) -матрицами при $k_1 = k_2 = k$. Роль линейной упорядоченности на v точках чисто техническая, требуется только для задания этих матриц.

В работе [20] приводится исчерпывающая классификация циклических $(v, 5)$ -групп, а в [21] – остальных абелевых $(v, 5)$ -групп. В работе [22] дана классификация циклических $(v, 3, 7)$ -групп и всех конечных $(v, 3, 5)$ -групп.

Имеется способ получения $(v, 3, k)$ -конфигураций на двумерных торах, использующий паркетирование евклидовой плоскости правильными треугольниками. В качестве "прямых" рассматриваются вершины одинаково ориентированных треугольников, закрашенных для определённости, в тёмный цвет. Вокруг каждой вершины имеет место чередование светлых и тёмных треугольников. Если группа Γ движений плоскости (см. [23]) сохраняет такое паркетирование (с учётом раскраски), то оно

переносится и на поверхность $\mathbb{R}^2/\Gamma$. В случае тора решётки $\Gamma \subset \mathbb{Z}^2$ (см. [24]) разбиваются на два класса. Решётки одного класса предоставляют $(v, 3, k)$ -конфигурации, когда матрица инцидентности L соответствующей конечной геометрии с 3-х точечными "прямыми" на $v = |\mathbb{Z}^2/\Gamma|$ точках невырождена над полем $GF(2)$. Тогда L^{-1} будет матрицей инцидентности другой конечной геометрии на тех же v точках с некоторыми нечётными параметрами $k = r$. Для решёток другого класса, когда матрица L вырождена, вложение $\mathbb{Z}^2/\Gamma \subset \mathbb{R}^2/\Gamma$ будет отвечать описываемому в § 3 вложению, соответствующему трёхчленной рекуррентной последовательности или полилинейной рекуррентной последовательности [25], [26]. Напротив, для решёток Γ первого класса такая реализация вложения $\mathbb{Z}^2/\Gamma \subset \mathbb{R}^2/\Gamma$ невозможна. Интересно, что реальная практика криптографического синтеза давно предопределила такое разбиение: решётки первого класса предоставляют матрицы для блочных шифраторов (см., например, [27] – [30]), а решётки второго класса отвечают рекуррентным и полилинейным рекуррентным последовательностям, используемым в поточных шифраторах.

Изначально использование геометрических представлений в задачах рекуррентной природы, привлекающих для своих формулировок семейства подмножеств $i + B$, $i \in \mathbb{Z}$, с фиксированным $B = \{0, s_1, \dots, s_{k-2}, m\} \subset \mathbb{Z}$, предполагало предварительный поиск вложений $\mathbb{Z}_v \subset M$, $v \in \mathbb{N} \cup \{\infty\}$, в римановы пространства M как можно меньшей размерности, которые удовлетворяли бы следующим качественным неформальным требованиям: а) элементы $\mathbb{Z}_v$ равномерно, дискретно и достаточно плотно рассосредотачиваются по M ; б) имеется действие группы $\mathbb{Z}_v$ на M изометриями, при котором $z \cdot x = z + x$ для всех $z \in \mathbb{Z}_v$, $x \in \mathbb{Z}_v \subset M$; в) элементы подмножества $B_v = \{z(\bmod v), z \in B\}$ должны находиться в непосредственной близости друг от друга.

Такие вложения может обеспечивать следующая конструкция. Пусть имеется кристаллографическая группа G движений на одном из римановых односвязных пространств Λ постоянной кривизны [31], содержащая нормальную подгруппу Γ , свободно действующую на Λ , такую, что $G/\Gamma \cong \mathbb{Z}_v$. Требуемое вложение $G/\Gamma \subset \Lambda/\Gamma = M$ задаётся орбитой внутренней точки фундаментальной области при действии G/Γ на M . Условия а) и б) при этом выполняются. Для обеспечения свойства в) тройка $\Gamma \triangleleft G : \Lambda$ должна подбираться специальным образом. К настоящему времени использовался только случай, когда: Λ – евклидово пространство; $G \subset \Lambda$ – решётка максимального ранга [24]; $\Gamma \triangleleft G$ – подрешётка того же или на единицу меньшего ранга.

В заключении, обращаясь к началу введения, отметим, что в некоторых ситуациях бывает исключительно полезным даже отказ от искусственно вводимой линейной упорядоченности на конечных множествах. Примером этому может служить работа [32]. Там, действуя вопреки представлениям систем корней простых алгебр Ли из монографии [33], использующей линейную упорядоченность базиса, удалось описать регулярные подалгебры матричных алгебр Ли, содержащих все диагональные элементы, на языке предупорядоченностей [34] и конечных топологий [35]. В результате размерности когомологий этих подалгебр стали выражаться через числа Бетти обычных клеточных комплексов. Благодаря этому была получена большая серия ранее не известных (см. [36]) примеров так называемых жёстких разрешимых алгебр Ли. Алгебра является жёсткой, если при малом изменении её структурных констант получающаяся алгебра изоморфна исходной. К жёстким относятся прежде всего простые

и полупростые алгебры Ли.

2. Определения порождающих наборов элементов рекуррентных последовательностей

В настоящем и следующих параграфах рассматриваются последовательности $x_i \in X$, $i \in \mathbb{Z}$, заданные рекуррентными соотношениями вида

$$x_{i+m} = f(x_i, x_{i+s_1}, \dots, x_{i+s_{k-2}}), \quad i \in \mathbb{Z}, \quad (3)$$

где $k \geq 3$, $0 = s_0 < s_1 < \dots < s_{k-2} < s_{k-1} = m$, $\text{НОД}(s_1, \dots, s_{k-2}, m) = 1$. Случай, когда $\text{НОД}(s_1, \dots, s_{k-2}, m) = d > 1$, легко сводится к рассматриваемому, поскольку тогда рекуррентная последовательность разбивается на d подпоследовательностей, каждая из которых удовлетворяет соотношению вида (3).

Интересующие нас вопросы не зависят от конкретного алфавита X и отображения $f : X^{k-1} \rightarrow X$, а целиком определяются набором чисел $k, m, s_1, \dots, s_{k-2}$. Элементы рекуррентной последовательности x_i , $i \in \mathbb{Z}$, будут пониматься как переменные, принимающие значения из алфавита X .

Свойства рекуррентных последовательностей при заданном m зависят как от k , так и от конкретных значений $s_1, \dots, s_{k-2}$ [37].

Для подмножества $S \subset \mathbb{Z}$ будем обозначать через $[S] \subset \mathbb{Z}$ совокупность всех таких $i \in \mathbb{Z}$, что x_i представимо формулой (см. [38]), содержащей (кроме скобок и запятых) только символы f и x_t , $t \in S$. Построение формулы для x_i , $i \in [S]$, производится путём суперпозиции с помощью начального соотношения (3), начиная с равенства $x_i = f(x_{i-m}, x_{i-m+s_1}, \dots, x_{i-m+s_{k-2}})$. К некоторым переменным из правой части последнего равенства снова применяется соотношение (3), конечно, если номера этих переменных ещё не содержатся в S . Соотношения (3) привлекаются до тех пор, пока хотя бы один номер входящих в очередную формулу переменных не содержится в S . Полученную таким образом формулу будем записывать в виде $x_i = F_i(x_t, t \in S)$.

ОПРЕДЕЛЕНИЕ 1. Множество $S \subset \mathbb{Z}$ назовём минимальным порождающим набором, если выполняются следующие два условия:

- а) при некотором $T \in \mathbb{Z}$ имеем: $[S] \supset \{T, T+1, T+2, \dots\}$;
- б) условие а) не выполняется ни для какого собственного подмножества множества S .

Множество S рассматривается с точностью до сдвигов на целые числа, поскольку для любых $n \in \mathbb{Z}$ и минимального порождающего набора S множество $S+n = \{s+n \mid s \in S\}$ тоже будет минимальным порождающим набором.

Случай с минимально возможным значением $m = 2$ (когда $k = 3$ и $s_1 = 1$) не является типичным (хотя к нему относится одна из наиболее известных рекуррентных последовательностей – числа Фибоначчи). При $m = 2$, $k = 3$ и $s_1 = 1$, как нетрудно убедиться, минимальными порождающими наборами являются $\{i, i+1\}$, $i \in \mathbb{Z}$. Здесь всегда $|S| = m = 2$. Далее считаем $m \geq 3$.

Не является типичным и случай с максимально возможным значением $k = m+1$, когда $s_i = i$, $i = 1, \dots, m-1$. В этом случае минимальный порождающий набор тоже

только один с точностью до сдвигов, он состоит из m подряд идущих номеров. Далее считаем $3 \leq k \leq m$.

Подробные доказательства приводимых далее достаточно простых замечаний имеются в работе [7]. Это же относится и к формулируемым в этом параграфе теоремам.

Для минимального порождающего набора S представления элементов x_i , $i \in [S]$ в виде $x_i = F_i(x_t, t \in S)$, единственны. Но свойство однозначного представления x_i для всех $i \geq T$ при некотором достаточно большом T нельзя рассматривать в качестве эквивалентного определения для минимального порождающего набора. Минимальный порождающий набор существует, например, $S = \{-1, -2, \dots, -m\}$, его мощность всегда конечна — $|S| < \infty$, но при заданных параметрах $m, k, s_1, \dots, s_{k-2}$ мощность $|S|$ может быть сколь угодно большой.

Минимальный порождающий набор S минимально возможной мощности (с $|S| = m$) назовём базисным набором для рекуррентной последовательности.

Далее в § 3 теоремами 1, 2 и 3 характеризуются минимальные порождающие наборы в случае трёхчленных рекуррентных последовательностей (когда $k = 3$). При $k \geq 4$ в § 4 теоремами 4 и 5 описываются базисные наборы. В случае, когда функция f биективна по первой переменной при любой фиксации остальных переменных, имеется возможность однозначно продолжать рекурренту в обратную сторону. Тогда естественно рассматривать минимальные порождающие наборы, позволяющие получать x_{-i} для всех достаточно больших i , пользуясь при этом только соотношениями $x_i = \tilde{f}(x_{i+s_1}, \dots, x_{i+s_{k-2}}, x_{i+m})$, $i \in \mathbb{Z}$, где используемое отображение $\tilde{f} : X^{k-1} \rightarrow X$ получается из (3) благодаря биективности f по первой переменной. Базисный набор S , который остаётся базисным набором и в этом новом смысле, называем совершенным базисным набором. Теоремы 6 и 7 в § 5 устанавливают строение совершенных базисных наборов для любых $k \geq 3$. В § 6 формулируются другие постановки задач, относящихся к порождающим множествам.

3. Минимальные порождающие наборы для трёхчленных рекуррентных последовательностей

При $k = 3$ полагаем $s_1 = s \in \{1, \dots, m-1\}$. Воспользуемся специальным расположением множества целых чисел на бесконечном двумерном цилиндре, являющемся прямым произведением окружности $T^1 = \mathbb{R}/\mathbb{Z}$ и вещественной прямой $\mathbb{R}$. Приведём подробное описание конструкции такого расположения.

Пусть $\varphi : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ — гомоморфизм решётки $\mathbb{Z}^2 \subset \mathbb{R}^2$ евклидовой плоскости $\mathbb{R}^2$ на множество целых чисел $\mathbb{Z}$, заданный равенством

$$\varphi(x, y) = x(s - m) + ym. \quad (4)$$

В силу взаимной простоты чисел m и s гомоморфизм φ является эпиморфизмом. Обозначим через Γ ядро гомоморфизма φ : $\Gamma = \ker \varphi = \langle (m, m-s) \rangle$.

Векторы $e_1 = (1, 0)$ и $e_2 = (0, 1)$ считаем ортонормальными в $\mathbb{R}^2$, первый считаем горизонтальным и направленным вправо, а второй — вертикальным и направленным вверх.

По теореме о гомоморфизме эпиморфизм φ естественным образом задаёт изоморфизм $\mathbb{Z}^2/\Gamma \cong \mathbb{Z}$. Коль скоро $\mathbb{Z}^2 \subset \mathbb{R}^2$, то $\mathbb{Z}^2/\Gamma \subset \mathbb{R}^2/\Gamma$. Тем самым имеем требуемое

вложение множества целых чисел $\mathbb{Z} \cong \mathbb{Z}^2/\Gamma$ в цилиндр $\mathbb{R}^2/\Gamma$, обозначаемый далее через Z .

Плоскость $\mathbb{R}^2$ является накрывающей поверхностью для цилиндра $\mathbb{R}^2/\Gamma$, а часть плоскости $\mathbb{R}^2$ между параллельными прямыми, перпендикулярными вектору $(m, m - s)$ и проходящими, соответственно, через точки $(0, 0)$ и $(m, m - s)$, является развёрткой этого цилиндра. Окружность на цилиндре, накрываемую отрезком плоскости с концами $(0, 0)$ и $(m, m - s)$, обозначим через C .

Проводимые ниже построения на цилиндре удобней заменять соответствующими Γ -инвариантными построениями на его накрывающей плоскости.

Расположение целых чисел на цилиндре можно задать и непосредственно. Для этого на плоскости $\mathbb{R}^2$ рассмотрим три семейства параллельных прямых: e_2 -семейство состоит из прямых

$$\{(x, 0) + te_2, t \in \mathbb{R}\} = \{(x, t), t \in \mathbb{R}\}, x \in \mathbb{Z};$$

$(-e_1)$ -семейство состоит из прямых

$$\{(0, y) + t(-e_1), t \in \mathbb{R}\} = \{(-t, y), t \in \mathbb{R}\}, y \in \mathbb{Z};$$

$(e_1 + e_2)$ -семейство состоит из прямых

$$\{(0, z) + t(e_1 + e_2), t \in \mathbb{R}\} = \{(t, t + z), t \in \mathbb{R}\}, z \in \mathbb{Z}.$$

Данные три семейства прямых образуют 3-сеть на плоскости $\mathbb{R}^2$, которая инвариантна относительно сдвигов на элементы подгруппы Γ в $\mathbb{R}^2$ (групповой операцией в $\mathbb{R}^2$ является обычное сложение векторов). В силу Γ -инвариантности эта 3-сеть переносится на цилиндр.

Припишем какому-либо узлу 3-сети на цилиндре целое число 0. У этого узла ткани имеется шесть соседних узлов. Паре этих узлов на проходящей через нулевой узел прямой e_2 -семейства припишем целые числа m и $-m$ соответственно. При продвижении от узла 0 к узлу m должно происходить увеличение параметра t на соответствующей прямой. Двум другим парам узлов, соседних с узлом 0, аналогичным образом приписываем целые числа $m - s$ и $s - m$, s и $-s$. Числа s и $-s$ на прямой $(e_1 + e_2)$ -семейства, а числа $m - s$ и $s - m$ на прямой $(-e_1)$ -семейства. Увеличение параметра t на соответствующих прямых должно происходить при продвижении от узла 0 к узлам s и $m - s$ соответственно. По такому же принципу соседям узла i , $i \in \mathbb{Z}$, будем приписывать целые числа $i + m, i - m, i + m - s, i - m + s, i + s, i - s$. В результате каждому узлу на цилиндре (см. рис. 2) будет приписано единственное целое число, при этом каждое целое число будет отвечать какому-то одному узлу. Это свойство следует из использованной выше теоремы о гомоморфизме, применённой к эпиморфизму φ , заданному равенством (4).

Заметим, что всего на цилиндре имеется m прямых в e_2 -семействе, $m - s$ прямых в $(-e_1)$ -семействе и s прямых в $(e_1 + e_2)$ -семействе. Вершинам сети на одной прямой приписаны целые числа с одним значением вычета по модулю m , $m - s$ и s соответственно.

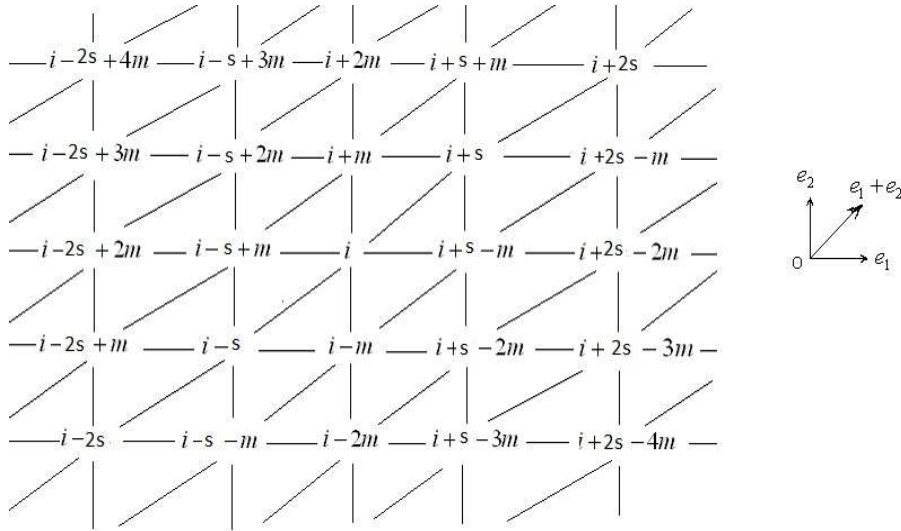


Рис. 2

Далее нам удобно картинку на рис. 2 представлять повёрнутой на 45° по часовой стрелке. Тогда отрезки $(e_1 + e_2)$ -прямых будут горизонтальными, на них параметр t увеличивается при движении направо (на развёртке цилиндра). У отрезков e_2 -прямых параметр t увеличивается при движении на “северо-восток”, а у отрезков $(-e_1)$ -прямых параметр t увеличивается при движении на “северо-запад”. Отрезки e_2 -прямых и $(-e_1)$ -прямых далее считаем наклонными.

На рис. 3 приведена развёртка цилиндра для значений параметров $m = 5$, $s = 2$. Пунктиром там указан отрезок, превращающийся в окружность C после склейки развёртки в цилиндр. (Рекомендуется представлять “шов” склейки за плоскостью рис. 3).

Прямые 3-сети на цилиндре Z (общим числом $2m$) являются винтовыми линиями. Прямые e_2 -семейства и $(e_1 + e_2)$ -семейства соответствуют правой резьбе, а прямые $(-e_1)$ -семейства закручены в противоположном направлении и соответствуют левой резьбе. Отрезки на этих прямых с концами в виде узлов сети будем называть e_2 -отрезками, $(-e_1)$ -отрезками и $(e_1 + e_2)$ -отрезками соответственно. Естественно, e_2 -отрезки и $(-e_1)$ -отрезки считать наклонными, а $(e_1 + e_2)$ -отрезки – горизонтальными. Целые числа будем отождествлять с узлами сети, называя их ещё целочисленными точками цилиндра.

За единицу длины $(e_1 + e_2)$ -отрезков (в отличие от e_2 -отрезков и $(-e_1)$ -отрезков) берётся длина вектора $e_1 + e_2$, т. е. (как и для e_2 -отрезков и $(-e_1)$ -отрезков) расстояние между двумя соседними узлами на отрезке.

Теперь мы располагаем всем необходимым для описания минимальных порождающих наборов.

Рассмотрим на цилиндре гомотопный окружности C цикл (замкнутый путь) L , состоящий из строго чередующихся горизонтальных и наклонных отрезков. Соседние отрезки образуют угол в 45° при вершине, обязательно являющейся узлом сети. Гомотопность означает непрерывную стягиваемость цикла L к окружности C . Другими словами, цикл L делает один оборот вокруг цилиндра.

На цикле L выбираем такую ориентацию, что на его горизонтальных $(e_1 + e_2)$ -отрезках она отвечает увеличению параметра t . Тогда на $(-e_1)$ -отрезках эта ориентация тоже будет отвечать увеличению t , но на e_2 -отрезках будет иметь место уменьшение параметра t .

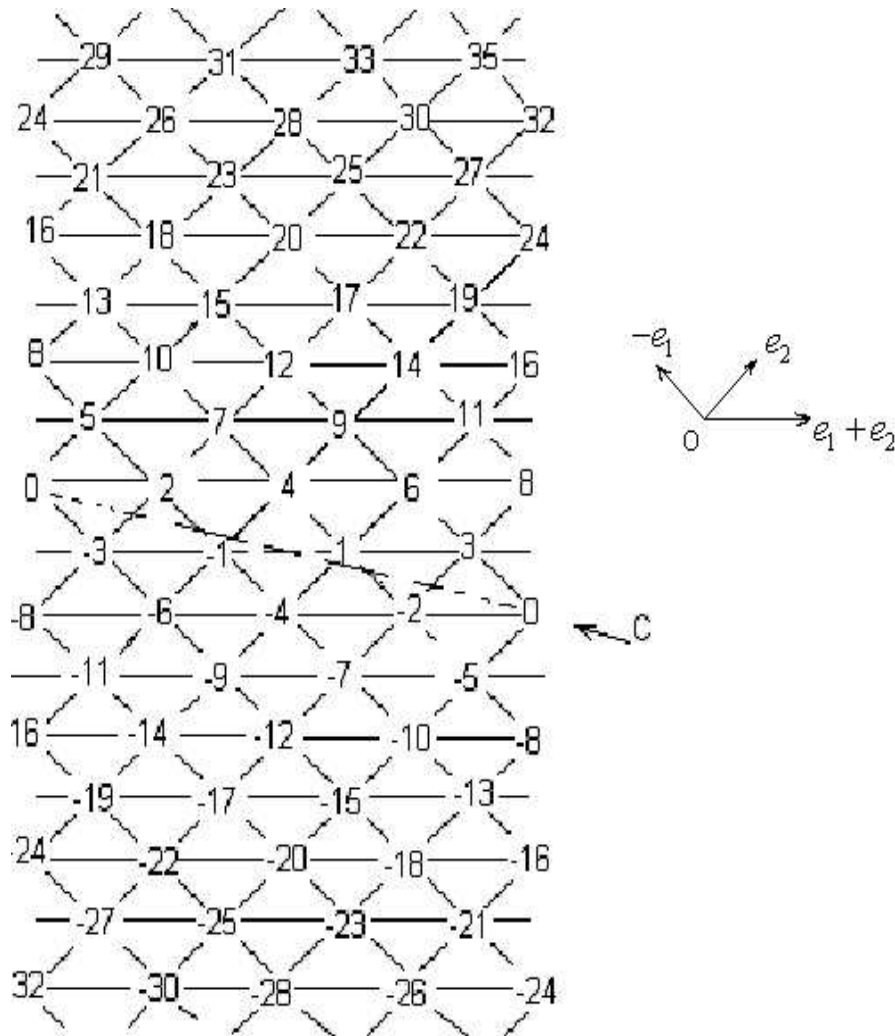


Рис. 3

Каждой точке $y \in Z \setminus L$ припишем белый или чёрный цвет. Для этого вначале в достаточно малых окрестностях $O(x)$, $x \in L \setminus \mathbb{Z}$, пересекающихся только с одним отрезком L , точки справа от L объявим белыми, а слева – чёрными. Если отрезок $[y, z]$ целиком содержится в $Z \setminus L$ и точке y приписан некоторый цвет, то точке z приписываем тот же цвет. В результате каждой точке $y \in Z \setminus L$ будет приписан белый или чёрный цвет, а некоторым точкам $Z \setminus L$ возможно будут приписаны оба цвета.

ОПРЕДЕЛЕНИЕ 2. Цикл L на цилиндре Z , гомотопный окружности C и являющийся ломаной из чередующихся горизонтальных и наклонных отрезков с углами в 45° в целочисленных вершинах, назовём правильным, если каждой точке $Z \setminus L$ приписан только один цвет – белый или чёрный и каждая белая точка содержится в горизонтальном отрезке из белых точек длиной более 1.99.

Пример правильного цикла приведён на рис. 4. Там представлена накрывающая плоскость цилиндра, вертикальные прямые накрывают “шов” продольного разреза цилиндра, полоса между двумя соседними из этих прямых является развёрткой цилиндра. Концы D ломаной на рис. 4 находятся на соседних вертикалях, потому как цикл L делает один оборот вокруг цилиндра.

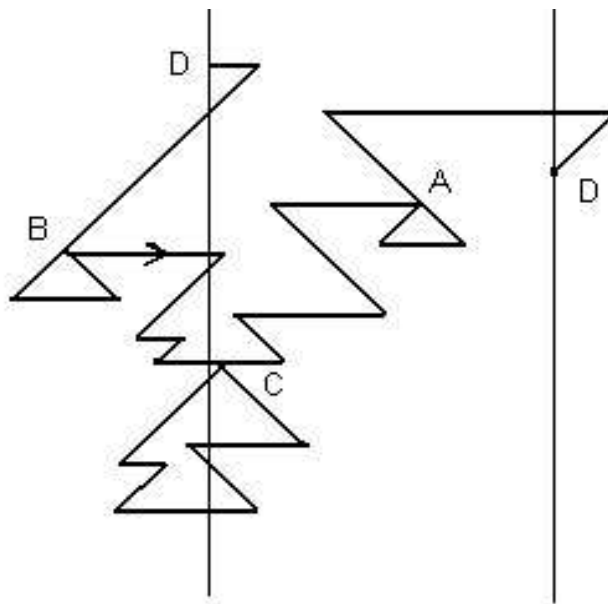


Рис. 4

Правильный цикл L не может иметь самопересечений, но может дважды проходить через некоторые целочисленные точки, которые называем точками касания.

На правильном цикле L точки касания могут быть только трёх следующих типов: а) внутренний узел $(-e_1)$ -отрезка, являющийся одновременно концевой точкой $(e_1 + e_2)$ -отрезка и начальной точкой следующего за ним e_2 -отрезка (точка A рис. 4); б) внутренний узел e_2 -отрезка, являющийся одновременно концевой точкой $(-e_1)$ -отрезка и начальной точкой следующего за ним $(e_1 + e_2)$ -отрезка (точка B рис. 4); в) узел при вершине угла в виде конечной точки $(e_1 + e_2)$ -отрезка и начальной точки e_2 -отрезка, являющийся одновременно вершиной угла в виде конечной точки $(-e_1)$ -отрезка и начальной точки $(e_1 + e_2)$ -отрезка (точка C рис. 4).

Множество белых точек, отвечающих правильному циклу L , связно неограниченно и располагается ниже L . Множество чёрных точек состоит из нескольких ограниченных односвязных областей и связной неограниченной области, располагающейся выше L .

Каждая из $2m$ прямых 3-сети на цилиндре разбивается на белые и чёрные отрезки и на два луча – один белый, другой чёрный.

Далее через M обозначим суммарную длину всех $(e_1 + e_2)$ -отрезков правильного цикла L , через K – суммарную длину всех e_2 -отрезков на L и через δ – суммарную длину всех $(-e_1)$ -отрезков на L . Тогда, очевидно, имеем: $M(1, 1) + K(0, -1) + \delta(-1, 0) = (m, m - s)$, или

$$M = m + \delta, \quad K = s + M - m = s + \delta. \quad (5)$$

ТЕОРЕМА 1. Пусть L – правильный цикл на цилиндре $Z = \mathbb{R}^2/\Gamma$. Тогда совокупность узлов $S = S(L)$, состоящая из внутренних узлов горизонтальных отрезков L и крайних нижних узлов наклонных отрезков, будет минимальным порождающим набором. Обратно, любой минимальный порождающий набор представляется в таком виде для некоторого правильного цикла L .

Для доказательства данной простой на первый взгляд теоремы в работе [7] потребовалось 4 страницы. По ходу доказательства устанавливается, что для правильного цикла L множество $|S(L)|$ состоит из всех целочисленных точек чёрного цвета и всех целочисленных точек, расположенных непосредственно на цикле L . Белые целочисленные точки в множество $|S(L)|$ не входят.

Поскольку на правильном цикле L имеет место строгое чередование наклонных и горизонтальных отрезков, мощность $|S(L)|$ соответствующего минимального порождающего набора $S(L)$ равна суммарной длине горизонтальных отрезков цикла L , обозначенной выше через M . Согласно условию (5) имеем: $|S| = M \geq m$.

При $m \geq 3$ мощностью минимального порождающего набора может быть любое целое, не меньшее m . В самом деле, $S_m = \{0, s, 2s, \dots, (m-1)s\}$ – не уменьшаемый порождающий набор мощности m , а для $i > m$ по индукции строится не уменьшаемый порождающий набор $S_i = (S_{i-1} \setminus \{\min S_{i-1}\}) \cup \{\min S_{i-1} - m, \min S_{i-1} - m + s\}$ мощности i .

Для базисных порождающих наборов, когда $|S| = m$, из равенств (5) получаем $\delta = 0$. Тогда на соответствующем правильном цикле нет $(-e_1)$ -отрезков, суммарная длина $(e_1 + e_2)$ -отрезков равна $M = m$, а суммарная длина e_2 -отрезков на этом цикле равна $K = s$.

Множество так устроенных правильных циклов L находится в естественной биекции с множеством ожерелий (см. [17]) из $m + s$ бусинок двух цветов – m бусинок одного цвета ($(e_1 + e_2)$ -отрезки длины один) и s бусинок другого цвета (e_2 -отрезки длины один). С учётом взаимной простоты m и s это замечание позволяет сформулировать следующую теорему.

ТЕОРЕМА 2. Число базисных наборов $N_{m,s}$ для трёхчленных рекуррентных последовательностей с параметрами $m, s, 0 < s < m, (s, m) = 1$, равно

$$N_{m,s} = \frac{1}{m+s} \binom{m+s}{s} = \frac{1}{m} \binom{m-1+s}{m-1}.$$

Как видно из этой теоремы, число базисных наборов увеличивается с увеличением s . При $s = 1$ базисный набор только один, он состоит из m подряд идущих номеров.

ТЕОРЕМА 3. Любой базисный набор для трёхчленной рекуррентной последовательности с параметрами $m, s, 0 < s < m, (s, m) = 1$, представляется объединением упорядоченной совокупности из $r \leq s$ конечных арифметических прогрессий с разностью s : $a_i, a_i + s, \dots, b_i - s, b_i, i = 0, 1, \dots, r - 1$, в которой $a_{(i+1) \bmod r} < b_i + s$, $b_i + s - a_{(i+1) \bmod r} \equiv 0 \pmod m$ для всех $i = 0, 1, \dots, r - 1$, и $\sum_{i=0}^{r-1} (b_i + s - a_{(i+1) \bmod r}) = sm$. Обратно, любой набор указанного вида является базисным.

Арифметическими прогрессиями в формулировке этой теоремы являются целочисленные точки отдельных горизонтальных отрезков соответствующего правильного цикла. Число горизонтальных отрезков обозначено через r . Крайние правые точки этих отрезков из указанных арифметических прогрессий исключаются.

4. Базисные наборы в случае $k \geq 4$

Здесь нам потребуется гомоморфизм $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_m, \pi(z) = z \pmod m, z \in \mathbb{Z}$. Если $S \subset \mathbb{Z}$ – базисный набор для рекуррентной последовательности (3), то $|S| = m$ и $|S \cap \pi^{-1}(y)| = 1$ для всех $y \in \mathbb{Z}_m$. В силу этого S является образом $\mathbb{Z}_m$ при некотором отображении $\sigma : \mathbb{Z}_m \rightarrow \mathbb{Z}$, удовлетворяющем условию $(\sigma \circ \pi)(y) = \pi(\sigma(y)) = y$ для всех $y \in \mathbb{Z}_m, S = \text{Im} \sigma$. Справедлива следующая теорема.

ТЕОРЕМА 4. Множество $S = \text{Im} \sigma$ для отображения $\sigma : \mathbb{Z}_m \rightarrow \mathbb{Z}$ с условием $(\sigma \circ \pi)(y) = \pi(\sigma(y)) = y, y \in \mathbb{Z}_m$, является базисным набором рекуррентной последовательности (3) тогда и только тогда, когда

$$\sigma(y + \pi(s_i)) \leq \sigma(y) + s_i \quad (6)$$

для всех $y \in \mathbb{Z}_m$ и $i = 1, 2, \dots, k - 2$. А в случае выполнения неравенств (6) имеем:

$$[S] = \bigcup_{y \in \mathbb{Z}_m} (\sigma(y) + m\mathbb{N}_0). \quad (7)$$

При конкретном формировании базисных наборов, как и в § 3, воспользуемся представлением множества целых чисел $\mathbb{Z}$ точками $(k - 1)$ -мерного цилиндра $C^{k-1} = T^{k-2} \times \mathbb{R}$, где T^{k-2} – $(k - 2)$ -мерный тор. По аналогии с гомоморфизмом (4), рассмотрим гомоморфизм $\varphi : \mathbb{Z}^{k-1} \rightarrow \mathbb{Z}, \varphi(z_0, z_1, \dots, z_{k-2}) = mz_0 + \sum_{i=1}^{k-2} s_i z_i$, являющийся эпиморфизмом, и потому $\mathbb{Z} \cong \mathbb{Z}^{k-1} / \Gamma, \Gamma = \ker \varphi$.

Используя вложение $\mathbb{Z}^{k-1} = \mathbb{Z} \times \mathbb{Z}^{k-2} \subset \mathbb{R} \times \mathbb{R}^{k-2} = \mathbb{R}^{k-1}$, получаем вложение множества всех целых чисел $\mathbb{Z} \cong \mathbb{Z}^{k-1} / \Gamma$ в $C^{k-1} = \mathbb{R}^{k-1} / \Gamma = T^{k-2} \times \mathbb{R}$. Здесь $T^{k-2} = \ker \Phi / \Gamma$, а $\Phi : \mathbb{R}^{k-1} \rightarrow \mathbb{R}, \Phi(x_0, x_1, \dots, x_{k-2}) = mx_0 + \sum_{i=1}^{k-2} s_i x_i$. Точке $(z_0, z_1, \dots, z_{k-2}) + \Gamma$ на цилиндре отвечает число $\varphi(z_0, z_1, \dots, z_{k-2})$.

Прямую $\mathbb{R}$ в произведении $\mathbb{R} \times \mathbb{R}^{k-2}$ удобно представлять направленной вертикально вверх, а пространство $\mathbb{R}^{k-2}$ считать горизонтальным.

Числа $z \in \mathbb{Z}$ будем считать приписанными к соответствующим целочисленным точкам цилиндра C^{k-1} и его односвязной накрывающей $\mathbb{R}^{k-1}$. В последнем случае одно и то же число z приписывается ко всем точкам некоторого смежного класса по подгруппе Γ . Здесь и далее целочисленными считаем точки с целочисленными координатами или смежные классы по Γ , содержащие такие точки.

Далее часто используется проекция ρ пространства $\mathbb{R}^{k-1} = \mathbb{R} \times \mathbb{R}^{k-2}$ на $\mathbb{R}^{k-2}$ параллельно $\mathbb{R}$, $\rho(\alpha, x) = x$, $\alpha \in \mathbb{R}$, $x \in \mathbb{R}^{k-2}$.

Положим $\tilde{\Gamma} = \rho(\Gamma)$, $\tilde{T}^{k-2} = \mathbb{R}^{k-2}/\tilde{\Gamma}$, $\Gamma_0 = \Gamma \cap \mathbb{R}^{k-2} \subset \tilde{\Gamma}$. Нетрудно убедиться, что $\Gamma_0 = \ker \psi$, где $\psi : \mathbb{Z}^{k-2} \rightarrow \mathbb{Z}$, $\psi(z_1, \dots, z_{k-2}) = \sum_{i=1}^{k-2} s_i z_i$. В этом случае $\tilde{\Gamma} = \ker(\psi \circ \pi)$.

Пусть $\text{НОД}(s_1, \dots, s_{k-2}) = d$. Тогда $\text{Im } \psi = d\mathbb{Z}$,

$$\mathbb{Z}^{k-2}/\Gamma_0 \cong d\mathbb{Z} \subset \mathbb{R}^{k-2}/\Gamma_0 = C^{k-2}, \text{НОД}(d, m) = 1, \text{Im}(\psi \circ \pi) = \mathbb{Z}_m,$$

$\mathbb{Z}^{k-2}/\tilde{\Gamma} \cong \mathbb{Z}_m \subset \mathbb{R}^{k-2}/\tilde{\Gamma} = \tilde{T}^{k-2}$. Таким образом, вершинам $(i, \mathbb{Z}^{k-2})$ приписаны числа из $im + d\mathbb{Z}$, $i \in \mathbb{Z}$. Учитывая взаимную простоту чисел m и d , имеем: $\mathbb{Z} = \bigcup_{i=0}^{d-1} (im + d\mathbb{Z})$, $\Gamma = \Gamma_0 \oplus \langle (d, y) \rangle$ для некоторого $y \in \mathbb{Z}^{k-2}$.

К целочисленным точкам $(k-2)$ -мерного цилиндра $C^{k-2} = \mathbb{R}^{k-2}/\Gamma_0$, вложенного в $C^{k-1} = \mathbb{R}^{k-1}/\Gamma$ в виде винтовой гиперповерхности, приписаны числа из $d\mathbb{Z}$. Это же относится и к целочисленным точкам $(k-2)$ -мерного цилиндра $im + C^{k-2} = im + \mathbb{R}^{k-2}/\Gamma_0$, которым приписаны числа из $im + d\mathbb{Z}$, $i = 1, \dots, d-1$. Данные d винтовых гиперповерхностей покрывают все целочисленные точки C^{k-1} , т. е. всё множество $\mathbb{Z}$. Если точке $x \in \mathbb{R}^{k-2}$ приписано число md , то $\tilde{\Gamma} = \Gamma_0 \oplus \langle x \rangle$ и $\tilde{T}^{k-2} = \mathbb{R}^{k-2}/\tilde{\Gamma} = C^{k-2}/\langle md \rangle$.

Отображение $\rho : \mathbb{R}^{k-1} \rightarrow \mathbb{R}^{k-2}$ индуцирует отображение $\tilde{\pi} : C^{k-1} \rightarrow \tilde{T}^{k-2}$, при этом $z \in \mathbb{Z} \subset C^{k-1}$ переходит в $z(\text{mod } m) \in \mathbb{Z}_m \subset \tilde{T}^{k-2}$, т. е. $\tilde{\pi}|_{\mathbb{Z}} = \pi$. Отметим, что $\tilde{\pi}|_{im + C^{k-2}}$ является бесконечнолистным накрытием тора $\tilde{T}^{k-2}$ при каждом $i = 0, 1, \dots, d-1$.

Пространство $\mathbb{R}^{k-2}$ естественным образом разбивается на элементарные ячейки в виде единичных $(k-2)$ -мерных кубов с целочисленными вершинами, их рёбра параллельны главным осям. Такое разбиение переносится также на цилиндры $im + C^{k-2}$, $i = 0, 1, \dots, d-1$, и на тор $\tilde{T}^{k-2}$. Число $z \in im + C^{k-2}$ дополнительно будем вписывать в куб с вершинами $z, z + s_j$, $j = 1, \dots, k-2$. Напомним, что в соответствии с основной конструкцией число $z = im + \sum_{j=1}^{k-2} s_j z_j$ приписывалось точке $(i, z_1, \dots, z_{k-2}) + \Gamma \in im + C^{k-2} \subset C^{k-1}$, и эту точку согласно установленному вложению $\mathbb{Z} \subset C^{k-1}$ стали обозначать через z . В результате дополнительно в элементарную ячейку с вершиной z вписываем число z . Аналогично, вычет $v \in \mathbb{Z}_m \subset \tilde{T}^{k-2}$ вписываем в куб с вершинами $v, v + \pi(s_j)$, $j = 1, \dots, k-2$, (остальные $2^{k-2} - k + 1$ вершины куба по $k-1$ указанным восстанавливаются однозначно).

Замкнутую гиперповерхность M в цилиндре C^{k-2} , составленную из $(k-3)$ -мерных граней элементарных ячеек, будем называть монотонной, если она гомотопна тору $\tilde{T}^{k-3} = (\mathbb{R}^{k-2} \cap \ker \Phi)/\Gamma_0$ цилиндра C^{k-2} , разбивает этот цилиндр на две части – верхнюю и нижнюю, и для любой точки $z \in M \cap (d\mathbb{Z})$ все точки вида $z + \sum_{i=1}^{k-2} s_i t_i$, $t_i \in \mathbb{N}_0$, $i = 1, \dots, k-2$, содержатся или на самой гиперповерхности M или в верхней части цилиндра C^{k-2} . По определению замкнутая гиперповерхность не имеет самопересечений, и окрестность любой её точки гомеоморфна окрестности $\mathbb{R}^{k-3}$ – внутренности $(k-3)$ -мерного шара. Далее $(k-3)$ -мерные грани элементарных ячеек будем называть стенками.

При наличии каких-либо d монотонных гиперповерхностей $M_0, \dots, M_{d-1}$ в C^{k-2} будем рассматривать также семейство гиперповерхностей $U = \{im + M_j | i \in \mathbb{Z}, j = 0, 1, \dots, d-1\}$. Возможно совпадающие гиперповерхности этого семейства различаем по их номеру $(i, j) \in \mathbb{Z} \times \{0, 1, \dots, d-1\}$. Каждой стенке β приписываем вес $h(\beta)$, равный числу гиперповерхностей семейства U , которым она принадлежит: $h(\beta) = |\{(i, j) \in \mathbb{Z} \times \{0, 1, \dots, d-1\} | \beta \subset im + M_j\}|$.

Семейство U является $\langle md \rangle$ -инвариантным, поэтому введенная система весов переносится на стенки $\tilde{\beta}$ тора $\tilde{T}^{k-2}$. Для $\tilde{\beta} \subset \tilde{T}^{k-2}$ имеем:

$$h(\tilde{\beta}) = \sum_{j=0}^{d-1} |[\tilde{\pi}^{-1}(\tilde{\beta}) \cap M_j]|.$$

(Через $||\dots||$ обозначаем число стенок в соответствующем множестве.) Систему весов на торе $\tilde{T}^{k-2}$ можно определять как и на цилиндре C^{k-2} , используя вместо U семейство $\tilde{U} = \{\tilde{\pi}(M_j) | j = 0, 1, \dots, d-1\}$, при этом нужно только учитывать, что в гиперповерхности $\tilde{\pi}(M_j)$, $j = 0, 1, \dots, d-1$, могут возникать кратные стенки $\tilde{\beta}$, накрываемые несколькими ячейками из M_j . Соответствующую кратность обозначим через $\lambda_j(\tilde{\beta}) = |[\tilde{\pi}^{-1}(\tilde{\beta}) \cap M_j]|$. Для стенок β в C^{k-2} кратности равны нулю или единице: $\lambda_{ij}(\beta) = 1$, если $\beta \subset im + M_j$, и $\lambda_{ij}(\beta) = 0$ иначе. В этих обозначениях для $\tilde{\beta} \subset \tilde{T}^{k-2}$ имеем: $h(\tilde{\beta}) = \sum_{j=0}^{d-1} \lambda_j(\tilde{\beta})$, а для $\beta \subset C^{k-2}$ соответственно имеем:

$$h(\beta) = \sum_{i \in \mathbb{Z}} \sum_{j=0}^{d-1} \lambda_{ij}(\beta) = \sum_{j=0}^{d-1} \lambda_j(\tilde{\pi}(\beta)) = h(\tilde{\pi}(\beta)).$$

Обозначим, наконец, вес стенки между ячейками v и $v + \pi(s_i)$ тора $\tilde{T}^{k-2}$ через $h_i(v)$, $i = 1, \dots, k-2$.

ТЕОРЕМА 5. Для любых d монотонных гиперповерхностей на цилиндре C^{k-2} равенства: $\sigma(0) = 0$, $\sigma(v + \pi(s_i)) = \sigma(v) + s_i - h_i(v)t$, $v \in \mathbb{Z}_m$, $i = 1, \dots, k-2$, корректным образом задают отображение $\sigma : \mathbb{Z}_m \rightarrow \mathbb{Z}$, для которого $\text{Im } \sigma$ является базисным набором. Обратно, любой базисный набор S после возможного сдвига на целое число может быть реализован таким способом для некоторых монотонных гиперповерхностей $M_0, M_1, \dots, M_{d-1}$ в C^{k-2} .

Доказательство этой теоремы на порядок сложнее доказательства теоремы 1, в работе [7] оно потребовало 6 страниц. Из доказательства следует, в частности, что в качестве монотонных гиперповерхностей $M_0, M_1, \dots, M_{d-1}$ на цилиндре C^{k-2} можно брать не произвольные, а только “непересекающиеся”, но, возможно, совпадающие и касающиеся друг друга по нескольким стенкам, при этом следующие друг за другом гиперповерхности $M_1, \dots, M_{d-1}$ находятся между M_0 и $M_d = md + M_0$, гиперповерхность M_i находится между M_{i-1} и M_{i+1} , $i = 1, \dots, d-1$. Гиперповерхности $\tilde{\pi}(M_0), \tilde{\pi}(M_1), \dots, \tilde{\pi}(M_{d-1})$ на торе тоже гомотопны тору $\tilde{T}^{k-3} = (\mathbb{R}^{k-2} \cap \ker \Phi) / \Gamma_0$ и следуют друг за другом, за $\tilde{\pi}(M_{d-1})$ следует $\tilde{\pi}(M_0)$.

Оценка числа базисных наборов (рассматриваемых, напомним, с точностью до сдвига) является отдельной задачей. Пока же, в соответствии с теоремой 2, можно утверждать, что при $k = 4$, $\text{НОД}(s_1, s_2) = 1$ и при достаточно больших $m \geq m(s_1, s_2)$ число базисных наборов равно $\frac{1}{s_1+s_2} \binom{s_1+s_2}{s_1}$. Если же $\text{НОД}(s_1, s_2) = d > 1$, то при $m \rightarrow \infty$ и ограниченных s_1, s_2 асимптотически число базисных наборов совпадает с $\left[\frac{d}{s_1+s_2} \binom{(s_1+s_2)/d}{s_1/d} \right]^d \frac{m^{d-1}}{d!}$. При $k \geq 5$ и ограниченных $s_1, \dots, s_{k-2}$ это число имеет порядок $O(m^{d-1})$. Если $s_1 = 1$, то при любом $k \geq 3$ базисный набор только один, состоит из m подряд идущих номеров.

5. Совершенные базисные наборы

Если в соотношении (3) отображение f является подстановочным по первой переменной при любой фиксации остальных $k - 2$ переменных, то для некоторого отображения $\tilde{f} : X^{k-1} \rightarrow X$ наряду с (3) справедливо соотношение

$$x_i = \tilde{f}(x_{i+s_1}, \dots, x_{i+s_{k-2}}, x_{i+m}), \quad i \in \mathbb{Z}, \quad (8)$$

что указывает на возможность продолжать рекурренту в обратную сторону. В этом случае для конечного подмножества $S \subset \mathbb{Z}$, наряду с $[S] \subset \mathbb{Z}$, будем рассматривать и обозначать через $[[S]] \subset \mathbb{Z}$ совокупность всех номеров $i \in \mathbb{Z}$, для которых x_i представимо формулой, содержащей кроме скобок и запятых символы $\tilde{f}$ и x_t , $t \in S$.

ОПРЕДЕЛЕНИЕ 3. Для рекуррентной последовательности (3), в которой отображение f является подстановочным по первой переменной при любой фиксации остальных $k - 2$ переменных, подмножество $S \subset \mathbb{Z}$ мощности m назовём совершенным базисным набором, если для некоторого достаточно большого $T \in \mathbb{N}$ имеем: $[S] \supset T + \mathbb{N}$ и $[[S]] \supset -(T + \mathbb{N})$.

Перепишав соотношение (8) в виде

$$x_{j-m} = \tilde{f}(x_{j-(m-s_1)}, \dots, x_{j-(m-s_{k-2})}, x_j), \quad j \in \mathbb{Z},$$

по аналогии с теоремой 4 можно утверждать, что для множества $S = \text{Im} \sigma$, отвечающего отображению $\sigma : \mathbb{Z}_m \rightarrow \mathbb{Z}$ с условием $\pi(\sigma(y)) = y$, $y \in \mathbb{Z}_m$, множество $[[S]]$ содержит $T - \mathbb{N} = \{T - 1, T - 2, \dots\}$ при некотором $T \in \mathbb{Z}$ тогда и только тогда, когда

$$\sigma(y) - m + s_i \leq \sigma(y + \pi(s_i)) \quad (9)$$

для всех $y \in \mathbb{Z}_m$ и $i = 1, \dots, k - 2$. Также в случае выполнения неравенств (9), имеем

$$[[S]] = \bigcup_{y \in \mathbb{Z}_m} (\sigma(y) - m\mathbb{N}_0). \quad (10)$$

При одновременном выполнении неравенств (6) и (9), с учётом того, что $\pi(\sigma(y) - m + s_i) = \pi(\sigma(y + \pi(s_i))) = \pi(\sigma(y) + s_i)$, $y \in \mathbb{Z}_m$, $i = 1, \dots, k - 2$, для $\sigma(y + \pi(s_i))$ имеются только две возможности: либо $\sigma(y + \pi(s_i)) = \sigma(y) + s_i$, либо $\sigma(y + \pi(s_i)) = \sigma(y) + s_i - m$. В этом случае, согласно равенствам (7) и (10), получаем: $[S] \cup [[S]] = \mathbb{Z}$, $[S] \cap [[S]] = S$.

В результате справедлива следующая теорема.

ТЕОРЕМА 6. Множество $S = \text{Im} \sigma$ для отображения $\sigma : \mathbb{Z}_m \rightarrow \mathbb{Z}$ с условием $\pi(\sigma(y)) = y$, $y \in \mathbb{Z}_m$, является совершенным базисным набором рекуррентной последовательности (3) тогда и только тогда, когда для всех $y \in \mathbb{Z}_m$ и $i = 1, \dots, k - 2$ либо $\sigma(y + \pi(s_i)) = \sigma(y) + s_i$, либо $\sigma(y + \pi(s_i)) = \sigma(y) + s_i - m$. В случае выполнения этого условия справедливы равенства: $[S] \cup [[S]] = \mathbb{Z}$, $[S] \cap [[S]] = S$.

В условиях теоремы 5 совершенность базисного набора равносильна, тем самым, требованиям: $h_i(v) \in \{0, 1\}$, $v \in \mathbb{Z}_m$, $i = 1, \dots, k - 2$. Другими словами, задающие отображение $\sigma : \mathbb{Z}_m \rightarrow \mathbb{Z}$ и следующие друг за другом гиперповерхности $\tilde{\pi}(M_0)$, $\tilde{\pi}(M_1)$, $\dots$, $\tilde{\pi}(M_{d-1})$ на торе $\tilde{T}^{k-2}$ не только попарно “не пересекаются”, но и исключается

наличие стенок, принадлежащих одновременно двум и более из этих гиперповерхностей, причём ограничения $\tilde{\pi}|_{M_i}$, $i = 0, 1, \dots, d-1$, являются гомеоморфизмами между M_i и $\tilde{\pi}(M_i)$. Последнее означает, что у $\tilde{\pi}(M_i)$ нет кратных стенок.

Особенно просто совершенные базисные наборы устроены при $k = 3$. Они отождествляются с ожерельями из s и $m - s$ бусинок. Как и в случае теоремы 2 для этого достаточно обратиться к введенным в § 3 3-сетям на бесконечном двумерном цилиндре. По аналогии с теоремами 2 и 3 убеждаемся в справедливости следующей теоремы.

ТЕОРЕМА 7. *Для трёхчленной рекуррентной последовательности порядка m подмножество $S \subset \mathbb{Z}$ мощности m является совершенным базисным набором тогда и только тогда, когда S находится на замкнутом гомотопном окружности S цикле, состоящем из $(e_1 + e_2)$ -отрезков и $(-e_1)$ -отрезков общей длиной m . Совокупность $(e_1 + e_2)$ -отрезков на таком цикле имеет общую длину $m - s$, а совокупность $(-e_1)$ -отрезков имеет общую длину s . Число совершенных базисных наборов, рассматриваемых с точностью до сдвигов, равно $\frac{1}{m} \binom{m}{s}$.*

Согласно теореме 3 можно также утверждать, что любой совершенный базисный набор для трёхчленной рекуррентной последовательности с параметрами m, s , $0 < s < m$, $(s, m) = 1$, представляется объединением упорядоченной совокупности из s конечных арифметических прогрессий с разностью s и общей длиной m : $a_i, a_i + s, \dots, b_i - s, b_i$; $b_i - a_i \geq 0$, $i = 0, 1, \dots, s-1$, $\sum_{i=0}^{s-1} \left(\frac{b_i - a_i}{s} + 1 \right) = m$, в которой $b_i - a_{(i+1) \bmod s} = m - s$ для всех $i = 0, 1, \dots, s-1$. Обратно, любое конечное множество целых чисел мощности m указанного вида является совершенным базисным набором. Иначе ещё можно сказать, что совершенный базисный набор при $k = 3$ является конечной последовательностью целых чисел длины m , в которой каждый следующий член, начиная со второго, либо больше предыдущего на s , либо меньше предыдущего на $m - s$, а самый первый член в этой последовательности либо больше её последнего члена на s , либо меньше его на $m - s$.

6. Общий случай порождающих наборов рекуррентных последовательностей

Обратим внимание, что при наличии дополнительного к (3) условия (8) понятие совершенных базисных наборов, не смотря на красивое их описание, связанное с ожерельями, является несколько искусственным. С практической точки зрения логичней для подмножества $S \subset \mathbb{Z}$ рассматривать в качестве его расширения подмножество $\bar{S} \subset \mathbb{Z}$, представляющее собой совокупность всех номеров $i \in \mathbb{Z}$, для которых x_i представимо формулой, содержащей (кроме скобок и запятых) символы $f, \bar{f}$ и x_t , $t \in S$, а базисными наборами логичней считать те подмножества S мощности m , для которых $\bar{S} = \mathbb{Z}$. Множество базисных наборов в этом смысле гораздо шире множества совершенных базисных наборов, являющегося пересечением множества наборов, определяемых неравенствами (6), и множества наборов, определяемых неравенствами (9).

Обобщая приведённую здесь точку зрения, следует рассматривать подмножество

$$\Theta \subset \{0, 1, \dots, k-2\},$$

состоящее из всех таких номеров $j \in \{0, 1, \dots, k-2\}$, что отображение

$$f(x_i, x_{i+s_1}, \dots, x_{i+s_{k-2}})$$

подстановочно по переменной x_{i+s_j} при любой фиксации остальных $k-2$ переменных. Если $j \in \Theta$, то для некоторого отображения

$$f^{(j)} : X^{k-1} \rightarrow X$$

наряду с (3) справедливо соотношение

$$x_{i+s_j} = f^{(j)}(x_i, x_{i+s_1}, \dots, x_{i+s_{j-1}}, x_{i+s_{j+1}}, \dots, x_{i+s_{k-2}}, x_{i+m}), \quad i \in \mathbb{Z}.$$

Если $0 \in \Theta$, то $f^{(0)} = \tilde{f}$.

Определившись с Θ , для подмножества $S \subset \mathbb{Z}$ нужно рассматривать его расширение $\bar{S} \subset \mathbb{Z}$, представляющее собой совокупность всех номеров $i \in \mathbb{Z}$, для которых x_i представимо формулой, содержащей (кроме скобок и запятых) символы: f ; $f^{(j)}$, $j \in \Theta$; x_t , $t \in S$, а Θ -базисными наборами нужно считать такие подмножества S мощности m , что $\bar{S} \supset T + \mathbb{N}$ при некотором достаточно большом T . В этом случае, если $0 \in \Theta$, то автоматически будем получать условие $\bar{S} = \mathbb{Z}$. В настоящем параграфе рассмотрен только случай, когда $\Theta = \emptyset$. Важными, на наш взгляд, являются следующие два крайних случая: $\Theta = \{0\}$ и $\Theta = \{0, 1, \dots, k-2\}$. Следующий параграф посвящён неуменьшаемым множествам $S \subset \mathbb{Z}$, $|S| \geq m$, для которых $\bar{S} = \mathbb{Z}$, в случае $k = 3$ и $\Theta = \{0, 1\}$.

7. Минимальные порождающие наборы трёхчленных рекуррентных последовательностей с квазигрупповыми рекуррентными соотношениями

7.1. В случае трёхчленных рекуррентных последовательностей соотношение (3) предстаёт в виде: $x_{i+m} = f(x_i, x_{i+s})$, $i \in \mathbb{Z}$, $0 < s < m$, $(s, m) = 1$. Отображение $f : X^2 \rightarrow X$ здесь задаёт квазигрупповую операцию на множестве X . Неуменьшаемые порождающие множества $S \subset \mathbb{Z}$, когда $\bar{S} = \mathbb{Z}$, введённые в § 6, в настоящем параграфе рассматриваются относительно $\Theta = \{0, 1\}$. Будем называть их (m, s) -базисами множества целых чисел $\mathbb{Z}$.

Понятие (m, s) -базиса удобно связывать с частичной бинарной операцией $\varpi_{m,s}$ на множестве $\mathbb{Z}$. Значение $\varpi_{m,s}(z_1, z_2)$, $z_1, z_2 \in \mathbb{Z}$, определено только при $|z_1 - z_2| \in \{s, m, m-s\}$, когда имеется единственное $i \in \mathbb{Z}$ такое, что $\{z_1, z_2\} \subset \{i, i+s, i+m\}$, и тогда $\varpi_{m,s}(z_1, z_2) = \{i, i+s, i+m\} \setminus \{z_1, z_2\}$.

Для подмножества $S \subset \mathbb{Z}$ через $[S] \subseteq \mathbb{Z}$ обозначим минимальное содержащее S подмножество в $\mathbb{Z}$, замкнутое относительно операции $\varpi_{m,s}$.

ОПРЕДЕЛЕНИЕ 4. Конечное подмножество $S \subset \mathbb{Z}$ назовём (m, s) -базисом, если $[S] = \mathbb{Z}$, а любое собственное подмножество S этим свойством не обладает.

Если S – (m, s) -базис, то $l + S = \{l + z \mid z \in S\}$ тоже будет (m, s) -базисом для всех $l \in \mathbb{Z}$. Базисные множества рассматриваем поэтому с точностью до сдвигов на целые числа.

В формулировке основной теоремы параграфа используется специальная функция $\psi : \mathbb{N} \rightarrow \mathbb{N}$. Для определения $\psi(m)$, $m \in \mathbb{N}$, аргумент m зададим в виде суммы чисел Фибоначчи (см., например, [39]) φ_i , $i \geq 0$: $\varphi_0 = 1$, $\varphi_1 = 2$, $\varphi_n = \varphi_{n-1} + \varphi_{n-2}$, $n \geq 2$. Если $m = \varphi_{n_0} + \varphi_{n_1} + \varphi_{n_2} + \dots$, $n_0 \mathbf{g} n_1 \mathbf{g} n_2 \mathbf{g} \dots$, то $\psi(m) = 2^{n_0} + 2^{n_1+1} + 2^{n_2+2} + \dots + 2^{n_i+i} + \dots$. Выражение $n_i \mathbf{g} n_{i+1}$ здесь означает, что $n_i - n_{i+1} \geq 2$, $i \geq 0$.

Представление натурального m такой суммой чисел Фибоначчи всегда существует и единственно [39]. В качестве φ_{n_0} берётся максимальное число Фибоначчи, не превосходящее m , в качестве φ_{n_1} – максимальное, не превосходящее $m - \varphi_{n_0}$, и т.д. Единственность проверяется по индукции, поскольку $\varphi_{n_0} \leq m < \varphi_{n_0+1}$. Для такой суммы используется также запись

$$m = 1c_{n-1}c_{n-2} \dots c_1c_0 = \varphi_n + \sum_{i=0}^{n-1} c_i \varphi_i \quad (11)$$

с $n = n_0 \geq 0$, в которой нет двух соседних единиц среди $c_i \in \{0, 1\}$ и обязательно $c_{n-1} = 0$. Запись (11) можно представлять ещё в виде

$$m = 1(\nu_l)1(\nu_{l-1})1 \dots 1(\nu_1)1(\nu_0), \quad (12)$$

где через (ν_j) обозначена серия нулей длины ν_j , $j = 0, 1, \dots, l$, $l \geq 0$, причём $\nu_j > 0$ для $j \geq 1$. При таком представлении m запись $\psi(m)$ в двоичной системе счисления имеет вид

$$\psi(m) = 1(\nu_l - 1)1(\nu_{l-1} - 1)1 \dots 1(\nu_1 - 1)1(\nu_0 + l). \quad (13)$$

Как видим, для получения $\psi(m)$ достаточно по одному нулю из каждой серии нулей между двумя единицами в фибоначчиевом представлении m в (12) перенести в самый конец – в область младших разрядов, а полученную в результате последовательность нулей и единиц (13) воспринимать как двоичное представление натурального числа $\psi(m)$.

Для функции $\psi(m)$ при $m \geq 2$ в работе [8] доказываются неравенства

$$0.719 m^\tau < \psi(m) < \frac{\sqrt{5}^\tau}{4} m^\tau + \frac{1}{\left(\frac{\alpha^2}{2}\right)^n \alpha^4(\alpha - 1)} < 0.797 m^\tau + \frac{1}{4}, \quad (14)$$

где $\alpha = \frac{\sqrt{5}+1}{2}$, $\tau = \log_\alpha 2$, $\varphi_n - \varphi_{n-4} < m \leq \varphi_{n+1} + \varphi_{n-3}$ и $\varphi_i = 0$ при $i < 0$. Здесь $\sqrt{5}^\tau/4 \in (0.7967, 0.7968)$; $\alpha^2/2 \in (1.3, 1.31)$; $\alpha^4(\alpha - 1) \in (4.236, 4.2361)$.

Верхняя оценка в (14) достаточно точная, по крайней мере, для $m = \varphi_n$ значение $\psi(\varphi_n) = 2^n$ является ближайшим целым к $\frac{\sqrt{5}^\tau}{4}(\varphi_n)^\tau$. К сожалению, для нижней оценки в (14) можно утверждать лишь, что $0.721 m^\tau > \psi(m)$ для неограниченного множества значений m вида $m = \varphi_n + \varphi_{n-3} + \varphi_{n-6} + \dots + \varphi_{n-3i} + \dots$. Нам не известно

значение нижнего предела $c_* = \lim_{m \rightarrow \infty} \frac{\psi(m)}{m^\tau} \in (0.719, 0.721)$, и мы не располагаем доказательством того, что $c_* m^\tau \leq \psi(m)$ хотя бы для достаточно больших m .

Довольно объёмная работа [8] практически целиком посвящена доказательству следующей теоремы.

ТЕОРЕМА 8. *Если S – (m, s) -базис, то $m \leq |S| \leq \psi(m)$. Обратно, для любого целого n , $m \leq n \leq \psi(m)$, имеется (m, s) -базис мощности n .*

В случае квазигрупповых рекуррентных соотношений

$$x_{i+m} = f(x_i, x_{i+s_1}, \dots, x_{i+s_{k-2}}), \quad i \in \mathbb{Z},$$

$$0 = s_0 < s_1 < s_2 < \dots < s_{k-2} < s_{k-1} = m, \text{НОД}(s_1, s_2, \dots, s_{k-2}, m) = 1,$$

в работе [8] аналогичным образом определяются $(m, s_1, \dots, s_{k-2})$ -базисы и для $k \geq 4$. При $k = 4$, в отличие от сформулированной теоремы, существуют пары s_1, s_2 , при которых (m, s_1, s_2) -базисы могут иметь сколь угодно большую мощность. В то же время при любых m и $k \leq m + 1$ существуют такие наборы $s_1, s_2, \dots, s_{k-2}$, что мощности $(m, s_1, s_2, \dots, s_{k-2})$ -базисов ограничены константой, зависящей от m .

7.2. Основным средством для доказательства теоремы 8 служит 3-сеть на бесконечном цилиндре, введённая в § 3. Она предоставляет удобное правило построения множества $[S]$ для каждого конкретного подмножества $S \subset \mathbb{Z}$. Для этого заштрихуем половину треугольников, на которые цилиндр разбивается нашей 3-сетью. Заштриховываем треугольники с вершинами $\{i, i + s, i + m\}$, $i \in \mathbb{Z}$. Треугольники с вершинами $\{i, i + s, i - m\}$, $i \in \mathbb{Z}$, оставляем светлыми. Светлые и заштрихованные треугольники будем называть элементарными. Можно считать их равносторонними с углами по 60° и длиной сторон 1.

Правило построения множества $[S]$ заключается в следующем. Прежде всего, $S \subset [S]$. Далее, если две вершины заштрихованного треугольника входят в $[S]$, то третья вершина этого треугольника тоже должна входить в $[S]$.

Описание возможных (m, s) -базисов начнём с введения необходимых понятий, относящихся к треугольникам. Доказательства всех используемых при этом утверждений имеются в работе [8].

Треугольники со сторонами, находящимися на прямых 3-сети, у которых внутри при угловых вершинах стоят заштрихованные элементарные треугольники, называем стандартными. Стандартный треугольник обозначаем через $\Delta_t(i)$ или Δ_t , если его угловыми вершинами являются $i, i + ts, i + tm$, $i \in \mathbb{Z}$, $t \geq 0$. Длину стороны стандартного треугольника Δ обозначаем через $\tau(\Delta)$: $\tau(\Delta_t(i)) = t$, $i \in \mathbb{Z}$, $t \geq 0$. Считаем $\Delta_0(i) = \{i\}$, $i \in \mathbb{Z}$. Заштрихованными являются элементарные треугольники $\Delta_1(i)$, $i \in \mathbb{Z}$.

При $t \leq m - 1$ треугольники $\Delta_t(i)$, $i \in \mathbb{Z}$, располагаются на цилиндре без самопересечений. Треугольники $\Delta_t(i)$ при $t \geq m$ являются самопересекающимися на цилиндре. Уже при $t = m$ вершина $i + ms$ треугольника $\Delta_m(i)$ оказывается на противоположной стороне этого треугольника (с концами i и $i + m^2$). При $t \geq m$ треугольники $\Delta_t(i)$ охватывают цилиндр полностью, они гомологичны окружности C .

Непересекающиеся треугольники $\Delta_{t_1}(i_1)$, $\Delta_{t_2}(i_2)$ считаем близкими, если пересекаются их 0.5-окрестности. Под 0.5-окрестностью треугольника понимается объединение

всех замкнутых кругов диаметра 1 с центрами в этом треугольнике. Для близких треугольников существуют целые $z_1 \in \Delta_{t_1}(i_1)$ и $z_2 \in \Delta_{t_2}(i_2)$, расстояние между которыми равно 1. В этом случае z_1, z_2 являются соседними вершинами 3-сети.

Обратим внимание, что хотя треугольник $\Delta_{m-1}(i)$ и не является самопересекающимся, но его 0.5-окрестность уже самопересекающаяся – охватывает цилиндр полностью. Угловая вершина $i + (m-1)s$ треугольника $\Delta_{m-1}(i)$ является соседней на 3-сети для точек $i + (s-1)m$ и $i + sm$, находящихся на противоположной стороне треугольника с концами i и $i + (m-1)m$.

Последние замечания позволяют заключить, что $[\Delta_t \cap \mathbb{Z}] = \mathbb{Z}$ при $t \geq m-1$ и $[\Delta_t \cap \mathbb{Z}] = \Delta_t \cap \mathbb{Z}$ при $t \leq m-2$.

Построение множества $[S]$ происходит довольно эффективно благодаря специальной операции $*$ над парой стандартных треугольников Δ', Δ'' с $\tau(\Delta') \leq m-2$ и $\tau(\Delta'') \leq m-2$, которые пересекаются или являются близкими. Результатом операции $*$ является минимальный стандартный треугольник $\Delta = \Delta' * \Delta''$, содержащий треугольники Δ' и Δ'' . Нетрудно убедиться, что $[(\Delta' \cap \mathbb{Z}) \cup (\Delta'' \cap \mathbb{Z})] = [\Delta \cap \mathbb{Z}]$. Если $\tau(\Delta) \geq m-1$, то левая и правая части в последнем равенстве совпадают с $\mathbb{Z}$. В редких случаях, когда объединение 0.5-окрестностей треугольников Δ', Δ'' целиком охватывает цилиндр (гомологично окружности C), треугольник Δ задаётся неоднозначно, но конкретный его выбор для нас не принципиален, поскольку в каждом из двух возможных случаев $[\Delta \cap \mathbb{Z}] = \mathbb{Z}$.

7.3. Пусть вначале $S \subset \mathbb{Z}$ произвольное конечное подмножество. Введём неориентированный граф $\Gamma = \Gamma(S)$ с множеством вершин S , соединяя вершины, расстояние между которыми равно единице. Рёбрами будут единичные отрезки прямых 3-сети или, иначе, стороны заштрихованных элементарных треугольников. Если граф $\Gamma(S)$ связан и $[S] \neq \mathbb{Z}$, то $[S]$ совпадает с целочисленными точками минимального стандартного треугольника Δ , содержащего S , с длиной стороны $\tau(\Delta) \leq m-2$: $[S] = \Delta \cap \mathbb{Z}$. Множество $[S] \neq \mathbb{Z}$ тоже называем треугольником, если оно совпадает с совокупностью целочисленных точек минимального стандартного треугольника, содержащего S .

Далее до конца параграфа подмножество $S \subset \mathbb{Z}$ считаем (m, s) -базисом. Пусть S_j , $j \in J$, – множества вершин связных компонент графа $\Gamma = \Gamma(S)$, $S = \bigsqcup_{j \in J} S_j$. Тогда $[S_{j'}] \cap [S_{j''}] = \emptyset$ при $j' \neq j''$.

Приведём два типа примеров связных компонент графа Γ .

Тип I. За основу берётся светлый треугольник $\{i, i+s, i+s-m\}$, $i \in \mathbb{Z}$. Из вершины $i+s$ выходит ветвь из единичных отрезков. Каждый очередной отрезок параллелен одному из векторов e_2 или e_1+e_2 . Единственной точкой ветвления (инцидентной более чем двум рёбрам) на этой ветви является исходная вершина $i+s$, последняя вершина ветви инцидентна только одному ребру. Аналогичная ветвь из единичных отрезков, параллельных $(-e_1)$ или $-e_1-e_2$, выходит из вершины i . Такая же ветвь выходит и из вершины $i+s-m$ с единичными отрезками, параллельными e_1 или $-e_2$. Длина отдельной ветви может быть и нулевой: тогда ветвь отсутствует. Могут отсутствовать две и даже все три ветви. Введённые выше ветви будем называть (e_2, e_1+e_2) -ветвью, $(-e_1, -e_1-e_2)$ -ветвью и $(e_1, -e_2)$ -ветвью соответственно. Вершинами связной компоненты типа I, вместе с $i, i+s, i+s-m$, будут вершины на этих ветвях, а рёбрами, кроме $(i, i+s)$, $(i, i+s-m)$, $(i+s, i+s-m)$, будут отрезки на этих ветвях.

Тип II. За основу берётся вершина $i \in \mathbb{Z}$, из которой выходят $(e_2, e_1 + e_2)$ -ветвь, $(-e_1, -e_1 - e_2)$ -ветвь и $(e_1, -e_2)$ -ветвь. Какие-то из этих ветвей могут отсутствовать, может не быть ни одной ветви. Вершинами и рёбрами связной компоненты типа II будут вершины и отрезки на этих ветвях. При их отсутствии связная компонента состоит из единственной вершины i . Как пример, связная компонента типа II может состоять из одной $(-e_1, -e_1 - e_2)$ -ветви, образующей цикл, целиком охватывающий цилиндр. В этом случае конец $(-e_1, -e_1 - e_2)$ -ветви будет находиться на расстоянии 1 от её начала i .

ТЕОРЕМА 9. Если подмножество $S \subset \mathbb{Z}$ является (m, s) -базисом, то каждая связная компонента $\Gamma_0 = \Gamma(S_0)$ графа $\Gamma(S)$, $S_0 \subset S$, содержит не более m вершин и относится или к типу I или к типу II. Размер треугольника $[S_0]$ равен $|S_0| - 1$ при $|S_0| < m$. Если $|S_0| = m$, то $S = S_0$.

В случае $S = S_0$, $|S| = m$, при опоясывании цилиндра 0.5-окрестностью минимального содержащего S стандартного треугольника Δ размера $m - 1$, его угловая вершина v , принадлежащая сторонам, параллельным векторам e_1 и $e_1 + e_2$, будет находиться на расстоянии 1 от вершин v_1 и v_2 , лежащих на противоположной к v стороне. Если $v \in S$, а $\{v_1, v_2\} \cap S = \emptyset$, то $\Gamma(S)$ состоит из одной $(-e_1, -e_1 - e_2)$ -ветви. Если бы такая ветвь заканчивалась вершиной v_1 или вершиной v_2 (при $|\{v_1, v_2\} \cap S| = 1$), то граф $\Gamma(S)$ был бы циклом, целиком охватывающим цилиндр. На этом цикле из m рёбер $m - s$ параллельны $e_1 + e_2$, а остальные s рёбер параллельны e_1 . В § 5 совокупности целочисленных точек на таких циклах отнесены к совершенным базисным наборам, отвечающим ожерельям из s и $m - s$ бусинок.

7.4. В данном пункте приводится описание строения (m, s) -базисов $S \subset \mathbb{Z}$ минимально возможной мощности m . Вначале же определим последовательность графов $\Gamma^{(0)} = \Gamma(S), \Gamma^{(1)}, \dots, \Gamma^{(r)}$, связанную с произвольным (m, s) -базисом $S \subset \mathbb{Z}$, $|S| \geq m$. Вершинами графов $\Gamma^{(j)}$, $j = 1, \dots, r$, будут стандартные треугольники. Обратная последовательность $\Gamma^{(r)}, \Gamma^{(r-1)}, \dots, \Gamma^{(1)}, \Gamma^{(0)}$ будет задавать структуру (m, s) -базиса.

Выше связные компоненты графа $\Gamma^{(0)}$ параметризовались множеством J . По теореме 9 для дальнейшего рассмотрения представляет интерес только случай, когда $|J| \geq 2$, иначе $r = 0$.

Рассмотрим неориентированный граф $\Gamma^{(1)}$ с множеством вершин J , в котором ребро (j', j'') существует тогда и только тогда, когда треугольники $[S_{j'}]$ и $[S_{j''}]$ пересекаются или являются близкими, т. е. когда пересекаются их 0.5-окрестности. В последнем случае найдутся $v_1 \in [S_{j'}]$ и $v_2 \in [S_{j''}]$, расстояние между которыми равно 1. Эти вершины соединены отрезком 3-сети. Правильнее считать вершинами графа $\Gamma^{(1)}$ сами минимальные стандартные треугольники $[S_j]$, $j \in J$, содержащие связные компоненты графа $\Gamma = \Gamma^{(0)}$.

Вершинами графа $\Gamma^{(i)}$, $i \geq 2$, являются минимальные стандартные треугольники, содержащие связные компоненты графа $\Gamma^{(i-1)}$. Вершины $[S']$ и $[S'']$ в графе $\Gamma^{(i)}$ соединены ребром, если они сами пересекаются или пересекаются их 0.5-окрестности. Замыкающим в последовательности $\Gamma^{(0)}, \Gamma^{(1)}, \dots, \Gamma^{(r)}$, является граф $\Gamma^{(r)}$, $r \geq 0$, состоящий из одной связной компоненты. Задание какого-либо (m, s) -базиса сопряжено с построением цепочки этих графов, но в обратной последовательности:

$$\Gamma^{(r)}, \Gamma^{(r-1)}, \dots, \Gamma^{(1)}, \Gamma^{(0)}.$$

Подробное строение графов $\Gamma^{(i)}$, $i \geq 1$, при $|S| \geq m$ будет приведено в следующем п. 7.5. При $|S| = m$ потребуются два описываемых ниже типа связных компонент графов $\Gamma^{(i)}$, $i \geq 1$, вершинами которых являются стандартные треугольники размера нуль и выше.

Как и в § 3 при описании строения графов вектор $e_1 + e_2$ представляем горизонтальным, направленным вправо, а вектор e_1 – направленным вниз направо, тогда вектор e_2 будет направлен вверх направо. При таком представлении угловые вершины стандартного треугольника при нижнем горизонтальном основании называем соответственно левой и правой, а третью угловую вершину – верхней, одну боковую сторону называем левой, другую – правой.

Тип А. Граф состоит из трёх ветвей, каждая из которых состоит из стандартных треугольников. Первая ветвь, называемая $(e_2, e_1 + e_2)$ -ветвью, выходит из вершины $i + s$, $i \in \mathbb{Z}$, и начинается стандартным треугольником $\Delta^{(1)}$ размера $t \geq 0$ с левой вершиной $i + s$. Пусть v – вершина внутри или на границе угла в 60° , образованного лучами $i + s + u(e_1 + e_2)$, $u \geq 0$, и $i + s + ue_2$, $u \geq 0$, не содержащаяся в $\Delta^{(1)}$, но находящаяся на расстоянии 1 от одной из целочисленных точек в $\Delta^{(1)}$. Для следующего стандартного треугольника $\Delta^{(2)}$ рассматриваемой ветви точка v является левой угловой вершиной. Далее, стандартные треугольники $\Delta^{(j)}$, $j \geq 3$, соотносятся с треугольниками $\Delta^{(j-1)}$ в точности так же, как треугольник $\Delta^{(2)}$ соотносится с $\Delta^{(1)}$. Из вершины i выходит аналогичная $(-e_1, -e_1 - e_2)$ -ветвь, в которой i будет правой угловой вершиной первого треугольника ветви. Из вершины $i + s - m$ выходит $(e_1, -e_2)$ -ветвь, в которой $i + s - m$ будет верхней угловой вершиной первого треугольника ветви. Каждая из этих ветвей может состоять из единственного первого треугольника, один из которых, в свою очередь, может иметь нулевой размер – принадлежать $\{i, i + s, i + s - m\}$.

Тип В. За основу берётся треугольник $\Delta^{(1)}$ с угловыми вершинами $i, i + ls, i + lm$, $i \in \mathbb{Z}$, $l \geq 0$, начиная с которого строятся $(e_2, e_1 + e_2)$ -ветвь, $(-e_1, -e_1 - e_2)$ -ветвь и $(e_1, -e_2)$ -ветвь. Каждая из этих трёх ветвей может состоять из одного единственного треугольника $\Delta^{(1)}$.

ТЕОРЕМА 10. Если $S \subset \mathbb{Z} - (m, s)$ -базис, $|S| = m$, то связные компоненты графов $\Gamma^{(i)}$, $i = 1, \dots, r$, относятся или к типу А или к типу В.

7.5. Для (m, s) -базиса $S \subset \mathbb{Z}$, $|S| \geq m$, в п. 7.4 была определена последовательность неориентированных графов $\Gamma^{(0)} = \Gamma(S), \Gamma^{(1)}, \dots, \Gamma^{(r)}$, $r \geq 0$. Первым связным графом в указанной последовательности (с двумя и более вершинами при $r \geq 1$) является граф $\Gamma^{(r)}$. Структура графа $\Gamma^{(0)}$ была представлена в теореме 9. Приведём пять типов графов для $\Gamma^{(j)}$, $j \geq 1$.

Тип А. За основу берутся три смежных друг с другом стандартных треугольника $\Delta_{(1)}, \Delta_{(2)}, \Delta_{(3)}$ таких, что каждая сторона минимального стандартного треугольника $\bar{\Delta}$, их содержащего, содержит сторону только одного треугольника из трёх исходных, причём последние не содержат угловых вершин $\bar{\Delta}$. Треугольник $\Delta_{(i)}$, $i \in \{1, 2, 3\}$, (возможно нулевого размера) примыкает к стороне окаймляющего треугольника $\bar{\Delta}$, параллельной e_i при $i = 1, 2$ или $e_1 + e_2$ при $i = 3$. Пусть вершинами треугольника $\bar{\Delta}$ являются $i, i + lm, i + ls$, $i \in \mathbb{Z}$, $l > 0$. От треугольника $\Delta_{(1)}$ отходит направленная вправо $(e_2, e_1 + e_2)$ -ветвь $\Delta^{(0)} = \Delta_{(1)}, \Delta^{(1)}, \dots, \Delta^{(h)}$, $h \geq 0$, из стандартных треугольников не обязательно положительного размера, определяемая следующими тремя условиями:

а) треугольники $\Delta^{(j)}$, $j = 0, 1, \dots, h$, не пересекаются с лучами $\{i + te_2 | t \geq 0\}$ и $\{i + t(e_1 + e_2) | t \geq 0\}$;

б) треугольник $\Delta^{(j)}$, $j = 1, \dots, h$, смежен с треугольником $\Delta^{(j-1)}$ и не смежен с треугольниками $\Delta^{(j-2)}, \Delta^{(j-3)}, \dots, \Delta^{(1)}, \Delta^{(0)} = \Delta_{(1)}, \Delta_{(2)}, \Delta_{(3)}$;

в) стороны треугольников $\Delta^{(j)}$, $j = 1, \dots, h$, параллельные e_1 , строго монотонно удаляются от прямой $\{i + ls + te_1 | t \in \mathbb{R}\}$.

Аналогично определяется направленная вниз $(e_1, -e_2)$ -ветвь, начинающаяся с треугольника $\Delta_{(3)}$, и направленная влево $(-e_1, -e_1 - e_2)$ -ветвь, начинающаяся с треугольника $\Delta_{(2)}$. Каждая из трёх ветвей в графе типа А может ограничиваться единственной вершиной $\Delta^{(0)} \in \{\Delta_{(1)}, \Delta_{(2)}, \Delta_{(3)}\}$.

Тип В. За основу берётся стандартный треугольник $\Delta_{(0)}$ и ещё три стандартных треугольника, обозначаемых как $\Delta_{(1)}, \Delta_{(2)}$ и $\Delta_{(3)}$. Последние смежны с $\Delta_{(0)}$ и не смежны друг с другом. Каждая сторона минимального стандартного треугольника $\bar{\Delta}$ с угловыми вершинами $i, i + lm, i + ls$, $i \in \mathbb{Z}$, $l > 0$, содержащего $\Delta_{(1)}, \Delta_{(2)}, \Delta_{(3)}$, содержит сторону только одного из этих треугольников. Треугольник $\Delta_{(0)}$ не пересекается с периметром треугольника $\bar{\Delta}$, содержится строго внутри $\bar{\Delta}$. Треугольник $\Delta_{(i)}$, $i \in \{1, 2, 3\}$, примыкает к стороне треугольника $\bar{\Delta}$, параллельной соответственно e_i или $e_1 + e_2$ при $i = 3$. От треугольника $\Delta_{(1)}$ вправо отходит $(e_2, e_1 + e_2)$ -ветвь, от треугольника $\Delta_{(3)}$ вниз $(e_1, -e_2)$ -ветвь, от треугольника $\Delta_{(2)}$ влево $(-e_1, -e_1 - e_2)$ -ветвь.

Тип С. За основу берётся стандартный треугольник $\Delta_{(0)}$ с нижним основанием на прямой $\{i + t(e_1 + e_2) | t \in \mathbb{R}\}$, $i \in \mathbb{Z}$, смежный со стандартными треугольниками $\Delta_{(1)}$ и $\Delta_{(2)}$. Треугольники $\Delta_{(1)}$ и $\Delta_{(2)}$ не смежны друг с другом. Основание минимального стандартного треугольника $\bar{\Delta}$, содержащего треугольники $\Delta_{(0)}, \Delta_{(1)}, \Delta_{(2)}$, находится на прямой $\{i + t(e_1 + e_2) | t \in \mathbb{R}\}$. Левая сторона треугольника $\bar{\Delta}$ пересекается только с $\Delta_{(2)}$, содержит левую сторону треугольника $\Delta_{(2)}$ и не пересекается с $\Delta_{(0)}$ и $\Delta_{(1)}$. Аналогично, правая сторона треугольника $\bar{\Delta}$ пересекается только с $\Delta_{(1)}$, содержит правую сторону треугольника $\Delta_{(1)}$ и не пересекается с $\Delta_{(0)}$ и $\Delta_{(2)}$. От треугольника $\Delta_{(1)}$ вправо отходит $(e_2, e_1 + e_2)$ -ветвь, а от треугольника $\Delta_{(2)}$ влево $(-e_1, -e_1 - e_2)$ -ветвь. Условия а) и б) в определении ветвей из описания графов типа А здесь несколько ослаблены, они принимают следующий вид:

а') никакая часть какого-либо треугольника из обеих ветвей не может быть ниже прямой $\{i + t(e_1 + e_2) | t \in \mathbb{R}\}$; треугольники $(e_2, e_1 + e_2)$ -ветви, начиная с $\Delta^{(0)} = \Delta_{(1)}$, не пересекаются с лучом $\{v + te_2 | t \geq 0\}$, а треугольники $(-e_1, -e_1 - e_2)$ -ветви не пересекаются с лучом $\{w - te_1 | t \geq 0\}$, если $v = i$ и $w = i + ls$, $l > 0$, суть левая и правая вершины треугольника $\bar{\Delta}$;

б') объединение обеих ветвей и $\Delta^{(0)}$ является простой цепью.

Принципиальное условие в) сохраняется в прежнем виде.

Графы, получающиеся из описанного поворотом на 120° в одну или другую сторону, тоже относятся к типу С.

Тип D. За основу берётся стандартный треугольник $\Delta^{(0)}$ размера $l \geq 0$ с вершинами $i, i + lm, i + ls$, $i \in \mathbb{Z}$, от которого отходит $(-e_1, -e_1 - e_2)$ -ветвь. Условие на ветви а) из описания графов типа А здесь принимает вид:

а") треугольники $\Delta^{(j)}$, $j = 0, 1, \dots, h$, содержатся в углу с вершиной $i + ls$ и лучами $\{i + ls - te_1 | t \geq 0\}$, $\{i + ls - t(e_1 + e_2) | t \geq 0\}$, стороны треугольников $\Delta^{(j)}$, $j = 0, 1, \dots, h$,

могут находиться на лучах угла.

Условия б) и в) сохраняются в прежнем виде.

Графы, получающиеся из описанного поворотом на 120° в одну или другую сторону, тоже относятся к типу D.

Тип Е. Простая замкнутая цепь из стандартных треугольников

$$\Delta^{(j)}, \quad j = 0, 1, \dots, h-1,$$

целиком охватывающая цилиндр. Смежными являются только треугольники

$$\Delta^{(j)}, \Delta^{((j+1) \bmod h)}, \quad j = 0, 1, \dots, h-1,$$

причём левая сторона треугольника $\Delta^{((j+1) \bmod h)}$ располагается строго правее левой стороны треугольника $\Delta^{(j)}$, а прямая e_2 -семейства, содержащая правую вершину треугольника $\Delta^{((j+1) \bmod h)}$ располагается строго правее прямой e_2 -семейства, содержащей правую вершину треугольника $\Delta^{(j)}$.

ТЕОРЕМА 11. Если $S \subset \mathbb{Z}$ является (m, s) -базисом, то каждая связная компонента графов $\Gamma^{(i)}$, $i = 1, \dots, r$, относится к одному из типов A, B, C, D, а граф $\Gamma^{(r)}$ может ещё иметь тип E.

8. Заключение

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Кострикин А. И., Манин Ю. И. Линейная алгебра и геометрия. М.: Наука, 1986. 304 с.
2. Кон П. Универсальная алгебра. М.: Мир, 1968. 352 с.
3. Veblen O. Differential invariants and geometry. //Atti del Congr., Int. Mat., Bologna. 1928.
4. Кириллов А. А. Инвариантные операторы над геометрическими величинами. //Итоги науки и техники. Современные проблемы математики. Т. 16. М. 1980. С. 3 – 29.
5. Малышев Ф. М. Симплициальные системы линейных уравнений. //Алгебра: Сб. ст.-й. Изд-во МГУ им. М. В. Ломоносова. 1980. С. 53–56.
6. Картези Ф. Введение в конечные геометрии. М.: Наука, 1980. 320 с.
7. Малышев Ф. М. Порождающие наборы элементов рекуррентных последовательностей. //Труды по дискретной математике. 2008. Т. 11, № 2. С. 86 – 111.
8. Малышев Ф. М. Базисные множества целых чисел относительно многоместных операций сдвига. //Математические вопросы криптографии. 2011. Т. 2, № 1. С. 29 – 74.

9. Малышев Ф.М. Метрические свойства вложений множества целых чисел в цилиндр. //Математические вопросы криптографии. 2012. Т. 3, № 3. С. 57 – 79.
10. Делоне Б.Н., Сандакова Н.Н. Теория стереоэдров. //Труды Математического института им. В.А. Стеклова. 1961. Т. 64. С. 28 – 51.
11. Wolfram S. Cellular Automaton Supercomputing. // In High-Speed Computing. University of Illinois Press. 1988. P. 40–48.
12. Малышев Ф.М., Кутырёва Е.В. О распределении числа единиц в булевом треугольнике Паскаля. //Дискретная математика. 2006. Т.18, № 2. С. 123 – 131.
13. Малышев Ф.М., Тараканов В.Е. О (v, k) -конфигурациях. //Математический сборник. 2001. Т. 192, № 9. С. 85 – 108.
14. Холл М. Комбинаторика. //М.: Мир, 1970. 424 с.
15. Харари Ф. Теория графов. //М.: Мир, 1973. 302 с.
16. Камерон П., ван Линт Дж. Теория графов, теория кодирования и блок-схемы. //М.: Наука, 1980. 144 с.
17. Сачков В.Н. Комбинаторные методы дискретной математики. //М.: Наука, 1977. 320 с.
18. Тараканов В.Е. Комбинаторные задачи и $(0, 1)$ -матрицы. //М.: Наука, 1985. 192 с.
19. Малышев Ф.М., Фролов А.А. Классификация $(v, 3)$ -конфигураций. //Математические заметки. 2012. Т. 91, № 5. С. 741 – 749.
20. Тришин А.Е. Классификация циркулянтных $(v, 5)$ -матриц. //Обозрение прикладной и промышленной математики. 2004. Т. 11, № 2. С. 258 – 259.
21. Фролов А.А. Классификация неразложимых абелевых $(v, 5)$ -групп. //Дискретная математика. 2008. Т. 20, № 1. С. 94 – 108.
22. Брославский М.В. Примеры (v, k_1, k_2) -конфигураций. //Дипломная работа. М.: в/ч 33965, 2010.
23. Никулин В.В., Шафаревич И.Р. Геометрии и группы. //М.: Наука, 1973. 240 с.
24. Рышков С.С., Барановский Е.П. Классические методы теории решётчатых упаковок. //Успехи математических наук. 1979. Т. 34, № 4(202). С. 3 – 63.
25. Kuzmin A.S., Kurakin V.L., Mikhalev A.V., Nechaev A.A. Linear recurrences over rings and modules. //J. Math. Science (Contemporary Math. and Its Appl. Thematic surveys). V. 76, № 6. P. 2793 – 2915.
26. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Псевдослучайные и полилинейные последовательности. //Труды по дискретной математике. 1997. Т. 1, С. 139 – 202.
27. National Institute of Standards and Technology, U.S.A., Advanced Encryption Standard (AES) FIPS – 197, 2001.

28. Specification of ARIA. National Security Research Institute (NSRI). January, 2005. <http://www.nsri.re.kr/ARIA/index-e.html>.
29. SEED Algorithm Specification. Korea Information Security Agency. 2005. <https://tools.ietf.org/draft-park-seed-01>.
30. Lu J., Ji W., Hu L., Ding J., Pyshkin A., Weinmann R. Analysis of the SMS4 Block Cipher. Proceedings of ACISP'07. LNCS 4586, 2007. P. 306 – 318.
31. Винберг Э.Б., Шварцман О.В. Дискретные группы движений пространств постоянной кривизны. //Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 29. М. 1988. С. 147 – 259.
32. Малышев Ф.М. О замкнутых подмножествах корней и когомологиях регулярных подалгебр. //Математический сборник. 1977. Т. 104(146), № 1(9). С. 140 – 150.
33. Бурбаки Н. Группы и алгебры Ли. М.: Мир, 1972. 336 с.
34. Morgado I. Note on quasi-orders, partial orders and orders. //Notes comuus mat. 1972. № 43. P. 31 – 40.
35. Krishnamurthy. On the number of topologies on a finite set. //Amer. Math. Monthly. 1966. V. 73. P. 154 – 157.
36. Толпыго А.К. О когомологиях параболических алгебр Ли. //Математические заметки. 1972. Т. 12, № 3. С. 251 – 255.
37. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х томах. М.: Мир, 1988. 822 с.
38. Лупанов О.Б. Введение в математическую логику. Конспект лекций. //М.: Мех – мат МГУ им. М.В. Ломоносова. 2007. 199 с.
39. Воробьёв Н.Н. Числа Фибоначчи. М.: Наука, 1978. 144 с.

REFERENCES

1. Kostrikin, A. I. & Manin, Yu. I. 1986, "Lineinaya algebra i geometriya" (Russian) [Linear algebra and geometry] Second edition. "Nauka", Moscow, 304 pp.
2. Kon, P. 1968, "Universal'naya algebra" (Russian) [Universal algebra] Translated from the English by T. M. Baranovic. Edited by A. G. Kurosh "MIR", Moscow 351 pp.
3. Veblen, O. 1928, "Differential invariants and geometry", *Atti del Congr., Int. Mat., Bologna*.
4. Kirillov, A. A. 1980, "Invariant operators over geometric quantities" (Russian) Current problems in mathematics, Vol. 16 (Russian), *Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow*, pp. 3–29, 228.
5. Malyshev, F. M. 1980, "Simpletsialnye system of linear equations", *Algebra, Moscow, Moscow University Press*, pp. 53–56.

6. Kartesi, F. 1980, "Vvedenie v konechnye geometrii" (Russian) [Introduction to finite geometries] Translated from the English by F. L. Varpahovskii and A. S. Solodovnikov., "Nauka", Moscow, 320 pp.
7. Malyshev, F. M. 2008, "Generating sets of elements of recurrent sequences", *Tr. discr. Mat., Fizmatlit, Moscow*, vol. 11, № 2, pp. 86 – 111.
8. Malyshev, F. M. 2011, "Bases of the set of integers with respect to multi-shift operations", *Mat. Issues. kriptogr.*, vol. 2, no. 1, pp. 29–73.
9. Malyshev, F. M. 2012, "Metric properties of the nested set of integers into a cylinder", *Mat. Issues. kriptogr.*, vol. 3, no. 3, pp. 57–79.
10. Delone, B. N. & Sandakova, N. N. 1961, "Theory of stereohedra" (Russian) *Trudy Mat. Inst. Steklov.*, vol. 64, pp. 28–51.
11. Wolfram, S. 1988, "Cellular Automaton Supercomputing", *In High-Speed Computing. University of Illinois Press.*, pp. 40–48.
12. Malyshev, F. M. & Kutyreva, E. V. 2006, "On the distribution of the number of ones in a Boolean Pascal's triangle" (Russian) *Diskret. Mat.*, vol. 18, no. 2, pp. 123–131; translation in *Discrete Math. Appl.*, vol. 16 (2006), no. 3, pp. 271–279.
13. Malyshev, F. M. & Tarakanov, V. E. 2001, "On (v, k) -configurations" (Russian) *Mat. Sb.*, vol. 192, no. 9, pp. 85–108; translation in *Sb. Math.*, vol. 192 (2001), no. 9–10, pp. 1341–1364.
14. Holl, M. 1970, "Kombinatorika" (Russian) [Combinatorial theory] Translated from the English by S. A. Shirokova. Edited by A. O. Gel'fond and V. E. Tarakanov, "MIR", Moscow, 424 pp.
15. Harary, F. 1973, "Teoriya grafov" (Russian) [Graph theory] Translated from the English by V. P. Kozyrev. Edited by G. P. Gavrillov., "MIR", Moscow, 300 pp.
16. Cameron, Peter J. & van Lint, Jacobus Hendricus 1980, "Teoriya grafov, teoriya kodirovaniya i blok-skhemy" (Russian) [Graph theory, coding theory and block designs] Translated from the English by B. S. Stekin. "Nauka", Moscow, 140 pp.
17. Sachkov, V. N. 1977, "Kombinatornye metody diskretnoi matematiki" (Russian) [Combinatorial methods of discrete mathematics], "Nauka", Moscow, 320 pp.
18. Tarakanov, V. E. 1985, "Kombinatornye zadachi i $(0,1)$ -matritsy" (Russian) [Combinatorial problems and $(0,1)$ -matrices], *Problemy Nauki i Tekhnicheskogo Progressa*. [Problems of Science and Technological Progress], "Nauka", Moscow, 192 pp.
19. Malyshev, F. M. & Frolov, A. A. 2012, "Classification of $(v, 3)$ -configurations", Translation of *Mat. Zametki*, vol. 91, no. 5, pp. 741–749. *Math. Notes*, vol. 91 (2012), no. 5-6, pp. 689–696.
20. Trishin, A. E. 2004, "Classification circulant $(v, 5)$ -matrices", *Review of Applied and Industrial Mathematics*, vol. 11, № 2. pp. 258 – 259.

21. Frolov, A. A. 2008, "Classification of indecomposable abelian $(v, 5)$ -groups" (Russian) *Diskret. Mat.*, vol. 20, no. 1, pp. 94–108; translation in *Discrete Math. Appl.*, vol. 18, no. 1, pp. 99–114.
22. Broslavsky, M. V. 2010, "Examples of (v, k_1, k_2) -configurations" Thesis. *Moscow, v/ch 33965* (Russian).
23. Nikulin, V. V. & Shafarevich, I. R. 1983, "Geometrii i gruppy" (Russian) [Geometries and groups], "Nauka", Moscow, 240 pp.
24. Ryshkov, S. S. & Baranovskii, E. P. 1979, "Classical methods of the theory of lattice packings" (Russian) *Uspekhi Mat. Nauk*, vol. 34, no. 4(208), pp. 3–63, 256.
25. Kurakin, V. L., Kuzmin, A. S., Mikhalev, A. V. & Nechaev, A. A. 1995, "Linear recurring sequences over rings and modules", *Algebra, 2. J. Math. Sci.*, vol. 76, № 6, pp. 2793 – 2915.
26. Kuzmin, A. S.; Kurakin, V. L.; Nechaev, A. A. 1997, "Pseudorandom and polylinear sequences" (Russian) *Proceedings in discrete mathematics, Tr. Diskretn. Mat., Nauchn. Izd. TVP, Moscow*, vol. 1, pp. 139–202.
27. National Institute of Standards and Technology, U.S.A., Advanced Encryption Standard (AES) FIPS – 197, 2001.
28. Specification of ARIA. National Security Research Institute (NSRI). January, 2005. <http://www.nsri.re.kr/ARIA/index-e.html>.
29. SEED Algorithm Specification. Korea Information Security Agency. 2005. <https://tools.ietf.org/draft-park-seed-01>.
30. Lu J., Ji W., Hu L., Ding J., Pyshkin A., Weinmann R. Analysis of the SMS4 Block Cipher. Proceedings of ACISP'07. LNCS 4586, 2007. P. 306 – 318.
31. Vinberg, E. B. & Shvartsman, O. V. 1988, "Discrete groups of motions of spaces of constant curvature" (Russian), *Current problems in mathematics. Fundamental directions, Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform.*, Moscow, vol. 29, pp. 147 – 259.
32. Malyshev, F. M. 1977, "Closed subsets of roots and the cohomology of regular subalgebras" (Russian), *Mat. Sb. (N.S.)*, vol. 104(146), no. 1, pp. 140–150, 176.
33. Burbaki, N. 1972, "Gruppy i algebry Li. Gruppy Kokstera i sistemy Titsa. Gruppy, porozhdennye otrazheniyami. Sistemy kornei." (Russian) [Lie groups and algebras. Coxeter groups and Tits systems. Groups generated by reflections. Root systems] Translated from the French by A. I. Kostrikin and A. N. Tjurin. Edited by A. I. Kostrikin. "MIR", Moscow, 334 pp.
34. Morgado, I. 1972, "Note on quasi-orders, partial orders and orders", *Notes comuus mat.*, № 43, pp. 31 – 40.

35. Krishnamurthy, V. 1966, "On the number of topologies on a finite set", *Amer. Math. Monthly.*, vol. 73. pp. 154 – 157.
36. Tolpygo, A. K. 1972, "The cohomology of parabolic Lie algebras" (Russian) *Mat. Zametki*, vol. 12, № 3, pp. 251–255.
37. Lidl, R. & Niderraiter, G. 1988, "Konechnye polya. Tom 1" (Russian) [Finite fields. Vol. 1] Translated from the English by A. E. Zhukov and V. I. Petrov. Translation edited and with a preface by V. I. Nechaev. "MIR", Moscow, 430 pp.; Lidl, R. & Niderraiter, G. 1988, "Konechnye polya. Tom 2" (Russian) [Finite fields. Vol. 2] Translated from the English by A. E. Zhukov and V. I. Petrov. Translation edited by V. I. Nechaev. "MIR", Moscow, pp. 433–822.
38. Lupanov, O. B. 2007, "Introduction to mathematical logic. Lecture notes.", Moscow, *Mekh – mat. MGU M. V. Lomonosov*, 199 p.
39. Vorob'ev, N. N. 1978, "Chisla Fibonachchi" (Russian) [Fibonacci numbers] Fourth edition. Populyarnye Lektsii po Matematike [Popular Lectures on Mathematics], 6. "Nauka", Moscow, 142 pp.

Математический институт им. В. А. Стеклова РАН.
Поступило 30.04.2015