ИЗВЕСТИЯ РАН. ТЕОРИЯ И СИСТЕМЫ УПРАВЛЕНИЯ, 2021, № 4, с. 84–93

СИСТЕМНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

УДК 51-37

Памяти профессора В.Н. Вагина

О СИНТЕЗЕ СИСТЕМ, ИМЕЮЩИХ СТРУКТУРУ КОМБИНАТОРНОЙ БЛОК-СХЕМЫ[1]

© 2021 г. А. О. Клягин[a],*, Н. П. Кочетова[a],, Д. Ю. Темников[a],***, А. Б. Фролов[a],****

[a] *НИУ МЭИ, Москва, Россия*

**e-mail: antik998@mail.ru*

***e-mail: natashka99@yandex.ru*

****e-mail: dnstnt@mail.ru*

*****e-mail: abfrolov@mail.ru*

Поступила в редакцию 18.08.2020 г.
После доработки 25.11.2020 г.
Принята к публикации 25.01.2021 г.

Обоснован метод числовой и алгебраической формализации и решения задачи синтеза систем, имеющих структуру одной из четырех разновидностей комбинаторных блок-схем. Получены аналитические представления блоков и дуальных блоков таких систем при представлении элементов и нумерации блоков и дуальных блоков начальными неотрицательными целыми числами. При этом используются алгебраические идентификаторы блоков, что позволяет строить блоки распределенно, т.е. независимо один от другого. Согласно обоснованному в работе методу формализации содержательных представлений систем, одна и та же комбинаторная блок-схема может быть моделью различных синтезируемых систем. Этот тезис проиллюстрирован примером синтеза вычислительной сети и схемы распределения ключей в беспроводной сенсорной сети.

DOI: 10.31857/S0002338821040077

Введение. В системном анализе используются двухуровневые и трехуровневые структурные модели систем, построенных из однотипных элементов и образованных блоками, характеризуемыми одинаковыми количествами вхождений в них элементов, а также одинаковыми количествами блоков, в которые входят определенные совокупности элементов. Такие модели изучаются в комбинаторном анализе, как так называемые комбинаторные блок-схемы. Теория комбинаторных блок-схем возникла при организации сравнительных экспериментов в аграрной науке: по определенной схеме выбирались наименования культур для их совместного выращивания на определенных полях. Этим достигалось совмещение по времени их испытаний в различных условиях. Далее комбинаторные блок-схемы применялись для тестирования групп крови, в настоящее время подобные исследования практикуются в генетике. В компьютерных науках на их основе изучаются распределенные вычислительные системы и схемы распределения ключей в них. На основе этих моделей отслеживаются связи между элементами сложной системы и при необходимости прогнозируются цепочки таких связей. Теория комбинаторных блок-схем отражена в монографии [1] и учебнике [2], в англоязычных изданиях наиболее востребованы книги [3, 4]. Комбинаторная блок-схема задается множеством элементов и множеством блоков, состоящих из элементов. Множество имен ее блоков принимается в качестве множества элементов двойственной по отношению к ней блок-схемы, множество блоков которой находится во взаимно-однозначном соответствии с множеством элементов исходной блок-схемы, а сами ее блоки являются множествами имен блоков исходной блок-схемы, содержащих элемент, который соответствует блоку двойственной блок-схемы. Например, если элементами выступают индексы сельскохозяйственных культур, а блоки состоят из индексов культур, возделываемых на наделах определенного поля, то каждый блок двойственной блок-схемы (дуальный блок)

[1] Работа выполнена при финансовой поддержке РФФИ (проект № 19-01-00294 а).

содержит имена полей, на наделах которых возделывается соответствующая ему культура. В иной интерпретации элементами могут быть компьютеры компьютерной сети, блоками – совокупности компьютеров отдельных локальных сетей, тогда дуальные блоки содержат локальные сети, в которых присутствует соответствующий дуальному блоку компьютер. Описанное соответствие комбинаторной и двойственной комбинаторной блок-схемы называется в данной работе правилом двойственности. Наряду с явными представлениями совокупностей блоков перечислением входящих в них элементов применяются представления комбинаторных блок-схем бинарными матрицами инцидентности и двудольными мультиграфами. Строки матрицы соответствуют элементам, а столбцы – блокам комбинаторной блок-схемы. Соответственно вершины одной доли двудольного графа суть элементы, а вершины другой доли – блоки. Ребра графа соответствуют вхождениям элементов в блоки. Матричные и графовые представления двойственной комбинаторной блок-схемы получаются транспонированием матрицы инцидентности или перестановкой долей двудольного графа исходной блок-схемы. В российской литературе данное направление прикладного комбинаторного анализа представлено, например, работами [5–7], где изучаются в основном симметричные комбинаторные схемы, в которых количества элементов и узлов совпадают, или так называемые квазиполные двудольные графы. Подобные работы важны для поиска алгоритмов вычисления комбинаторных блок-схем данного вида, инвариантных для применения в других областях. В [5, 7] даются матричные способы построения комбинаторных блок-схем, в любых двух блоках которых имеется единственный общий элемент и каждая пара элементов присутствует точно в одном блоке. Такие комбинаторные блок-схемы называются проективными плоскостями размерности два. В более сложных проективных плоскостях размерности три любые два элемента присутствуют в большем количестве блоков. Этим достигается моделирование множественных связей в сложных системах. Графовые представления таких проективных плоскостей даны в [6]. Трехуровневыми по построению являются линейные и квадратичные трансверсальные комбинаторные блок-схемы [1, 8], применяемые, например, в беспроводных сенсорных сетях [8].

Порядок $n = p^l$ и размерность d комбинаторной блок-схемы являются основными параметрами проективных плоскостей. По ним определяются мощности v множеств элементов и блоков, числа k элементов в блоке, а также количество блоков, в которые входит любая выбранная пара элементов; оно же – число элементов в пересечении любых двух блоков, а также число блоков, всегда имеющих единственный общий элемент. При синтезе трансверсальных блок-схем параметр k, определяющий число элементов в блоке, выбирается независимо, но при ограничении $d \le k \le n$. По порядку $n = p^l$ и размерности d трансверсальной блок-схемы определяются мощность множества элементов и мощность множества блоков, а также порог пересечения – наибольшее возможное число элементов в пересечении двух блоков.

Применение комбинаторных блок-схем позволяет совмещать изучение отдельных элементов параллельно в составе определенным образом собранных их подмножеств. Примером может служить осуществление 376 тестов с комбинаторными блоками, состоящими примерно из 5000 клонов вместо индивидуальных тестов с 220000 клонами, в Лос-Аламосской национальной лаборатории [9]. На основе комбинаторных блок-схем строятся комбинаторные библиотеки кодов аминокислот [10]. Применение комбинаторных методов для синтеза криптографических протоколов отражено в [11, 12]. Применению комбинаторных блок-схем в вычислительной технике посвящены упомянутые выше [5, 6]. В [7] дана интерпретация симметричной комбинаторной блок-схемы при моделировании многокомпонентной системы связи и подчеркнут универсальный характер таких моделей, допускающих подобные интерпретации в различных приложениях. Отметим также, что, согласно [12], изучаемые в настоящей работе алгоритмы синтеза трансверсальных комбинаторных схем применимы к синтезу ортогональных массивов и множественных латинских квадратов.

Приведенные в статье численные примеры получены с использованием системы компьютерной алгебры Sage [13] посредством алгебраического процессора МЭИ [14].

В разд. 1 дана постановка задачи настоящей работы. Раздел 2 является расширенным изложением доклада [15] на XIX Международной конференции “Проблемы теоретической кибернетики”. Здесь рассматриваются числовая и алгебраическая формализации и аналитические решения задач вычисления блоков для циклических и ациклических проективных плоскостей, линейной и квадратичной трансверсальных блок-схем и двойственных схем. В заключение обсуждаются особенности предложенного метода синтеза сложных систем определенного класса и возможности использования предлагаемых методов для решения производных задач.

1. Постановка задачи. Разнообразие технических и иного рода систем, моделируемых комбинаторными блок-схемами, требует единого подхода к их формализации. Универсальным методом унификации представлений систем перечислительного характера является нумерация элементов и блоков. Тогда в качестве множеств элементов, как и номеров блоков, можно принять множества начальных неотрицательных целых чисел. Такая нумерация будет удовлетворять отмеченному выше правилу двойственности, если по номеру блока однозначно вычисляется множество входящих в этот блок элементов (чисел), а по элементу (числу) однозначно вычисляется дуальный блок, т.е. множество номеров блоков, содержащих этот элемент. В настоящей работе описаны нумерации такого рода применительно к циклическим и ациклическим плоскостям, а также трансверсальным схемам, порядок которых есть простое число или степень простого числа. Они несколько различаются, но в каждом случае реализуются на основе алгебраического подхода, когда элементам и блокам взаимно-однозначно сопоставляются просто вычисляемые их алгебраические образы, числовые прообразы которых также легко рассчитываются. Применение нумерации элементов и блоков комбинаторных блок-схем позволяет сделать их представления более наглядными, скрыв особенности их алгебраической природы, а также создать условия для независимого и параллельного вычисления блоков на основе (бесперебoрного) построения алгебраических идентификаторов блоков по заданному номеру блока. В роли таких идентификаторов блоков циклических проективных плоскостей выступают разностное множество Зингера и номер блока. В качестве идентификаторов блоков ациклических проективных плоскостей используются нормированные базисы двумерных или соответственно трехмерных подпространств векторного пространства размерности три или четыре над конечным полем порядка p^l, множества числовых образов нормированных элементов которых как раз и являются блоками проективной плоскости. В качестве элементов выступают числовые нормированные образы базисов одномерных подпространств. Алгебраическими идентификаторами блоков трансверсальных комбинаторных блок-схем являются d-наборы (т.е. пары или тройки) элементов поля порядка p^l. Использование алгебраических идентификаторов позволяет строить блоки распределенно, т.е. независимо один от другого, избегая необходимости анализа их матричных или графовых представлений в полном объеме, как в работах [5–7]. Этим предлагаемый алгебраический подход отличается и от алгебраического метода в публикации [3], где в качестве элементов ациклической проективной плоскости рассматриваются одномерные подпространства, а блоками являются совокупности соответствующих элементам блока одномерных подпространств, объединение которых есть соответствующее блоку двумерное пространство.

Таким образом, задача данной работы – обосновать метод численной и алгебраической формализации в задачах синтеза систем, структура которых соответствует проективным плоскостям указанного выше порядка, а также линейным или квадратичным трансверсальным комбинаторным блок-схемам, и на его основе разработать новые алгебраические и соответствующие алгоритмические подходы к синтезу этих комбинаторных схем, а также их двойственных аналогов.

2. Алгебраические методы построения некоторых комбинаторных блок-схем. Рассмотрим некоторые разновидности комбинаторных блок-схем, используемых в качестве структурных моделей ряда технических или иного рода систем. Уравновешенная неполная блок-схема (УНБС) [1, 2] определяется на конечном множестве элементов $\mathbf{X}$ мощности v и образована как множество $\mathbf{A}$ собственных подмножеств, называемых блоками. Каждый блок состоит из k элементов, каждый элемент из $\mathbf{X}$ присутствует в r блоках, а каждая пара различных элементов встречается в λ блоках. УНБС имеют сокращенное обозначение (v, k, λ)-УНБС. Остальные параметры восстанавливаются по нему на основе элементарных соотношений $bk = vr$ и $r(k-1) = \lambda(v-1)$, где b – число блоков УНБС. Вот некоторые УНБС: $(n^2 + n + 1, n + 1, 1)$-УНБС называется проективной плоскостью размерности два и порядка n. Она обозначается PP(2,n). Проективная плоскость размерности три и порядка n PP(3,n) – это $(n^3 + n^2 + n + 1, n^2 + n + 1, n + 1)$-УНБС. Блоки таких УНБС попарно имеют λ общих элементов. Другой разновидностью комбинаторных блок-схем являются так называемые трансверсальные блок-схемы. Они характеризуются тем, что попарно блоки имеют не более одного общего элемента, но для любых двух непересекающихся блоков найдется μ, $\mu > 0$, других блоков, имеющих по λ общих элементов с каждым из них. Формализованное описание трансверсальных блок-схем будет дано ниже.

2.1. Построение блоков и дуальных блоков циклических проективных плоскостей. Строение блоков циклической проективной плоскости PP(2,n) определяется $(n^2 + n + 1, n + 1, 1)$-разностным множеством – совокупностью $n + 1$ элементов группы Z_{n^2+n+1}, такой, что любой ненулевой элемент этой группы можно получить как разность некото-

рых из этих элементов. Одну из разновидностей такого множества – разностное множество Зингера найдем как множество дискретных логарифмов элементов поля F_n^3, являющихся многочленами степени менее двух [1]. Для этого используется примитивный многочлен степени три над полем GF(n) и его корень x, т.е. примитивный элемент поля GF(n^3). Разностное множество Зингера образуется из показателей степеней j этого элемента, при которых степени многочленов x^j не превышают 1. Множество элементов проективной плоскости PP(2,n) есть множество из $n^2 + n + 1$ неотрицательных целых чисел, в качестве блока номер 0 можно принять множество чисел, составляющих разностное множество Зингера, а блок номер 0 двойственной проективной плоскости PP(2,n) образуется противоположными вычетами, т.е. числами, которые находятся вычитанием элементов нулевого блока проективной плоскости из 0 по модулю $n^2 + n + 1$. Тогда i-й блок, $i \in \{1, ..., n^2 + n\}$, как проективной плоскости, так и двойственной проективной плоскости получается прибавлением единицы по модулю $n^2 + n + 1$ к каждому элементу их $i - 1$-го блока. Поэтому справедливо следующее утверждение.

Утверждение 1 [15]. Блок, имеющий номер j, циклической проективной плоскости PP(2, n) вычисляется последовательным прибавлением его номера по модулю $n^2 + n + 1$ к элементам ($n^2 + n + 1$, $n + 1$, 1)-разностного множества Зингера. Блок, имеющий номер j, циклической двойственной проективной плоскости DPP(2,n) получается последовательным вычитанием из его номера j по модулю $n^2 + n + 1$ элементов этого разностного множества.

Для вычисления блоков циклической проективной плоскости PP(3,n) и двойственной циклической проективной плоскости DPP(3,n) используется ($n^3 + n^2 + n + 1$, $n^2 + n + 1$, $n + 1$)-разностное множество Зингера. Это совокупность $n^2 + n + 1$ элементов группы $Z_{n^3+n^2+n+1}$, такая, что любой ненулевой элемент этой группы можно получить $n + 1$-кратно как разность по модулю $n^3 + n^2 + n + 1$ различных $n + 1$ пар некоторых из этих $n^2 + n + 1$ элементов. Вычисление этого разностного множества Зингера производится как множества дискретных логарифмов элементов поля F_n^4, являющихся многочленами степени менее трех [1]. Для этого используется примитивный многочлен степени четыре над полем GF(n) и его корень x, т.е. примитивный элемент поля GF(n^4). Разностное множество Зингера образуется из показателей степеней j этого элемента, при которых степени многочленов x^j не превышают двух. Алгебраическая среда для этих вычислений удобно образуется средствами системы компьютерной алгебры Sage. Вычисления блоков и дуальных блоков производятся по модулю $n^3 + n^2 + n + 1$. Тогда множество элементов проективной плоскости PP(3,n) есть множество из $n^3 + n^2 + n + 1$ неотрицательных целых чисел, в качестве блока номер 0 можно принять множество чисел, составляющих разностное множество Зингера. Нулевой блок двойственной проективной плоскости DPP(3,n) образуется противоположными вычетами, т.е. числами, которые получаются вычитанием элементов нулевого блока проективной плоскости PP(3,n) из 0 по модулю $n^3 + n^2 + n + 1$. Тогда i-й блок, $i \in \{1, ..., n^3 + n^2 + n\}$, как проективной плоскости PP(3,n), так и двойственной проективной плоскости DPP(3,n) получается прибавлением единицы по модулю $n^3 + n^2 + n + 1$ к каждому элементу их i–1-го блока. Поэтому справедливо следующее утверждение.

Утверждение 2 [15]. Блок, имеющий номер j, циклической проективной плоскости PP(3,n) вычисляется последовательным прибавлением его номера по модулю $n^3 + n^2 + n + 1$ к элементам ($n^3 + n^2 + n + 1$, $n^2 + n + 1$, $n + 1$)-разностного множества Зингера. Блок, имеющий номер j, циклической двойственной проективной плоскости DPP(3.n) получается последовательным вычитанием из его номера j по модулю $n^3 + n^2 + n + 1$ элементов этого разностного множества.

Как видим, алгебраическими идентификаторами блоков циклической проективной плоскости размерности два или три выступают разностное множество Зингера и номер блока.

Пример 1. Циклическая проективная плоскость PP(3,2) – это (15,7,3)-УНБС:

0. [0–2, 4, 5, 8, 10],	1. [1–3, 5, 6, 9, 11],	2. [2–4, 6, 7, 10, 12],	3. [3–5, 7, 8, 11, 13],
4. [4–6, 8, 9, 12, 14],	5. [5–7, 9, 10, 13, 0],	6. [6–8, 10, 11, 14, 1],	7. [7–9, 11, 12, 0, 2],
8. [8–10, 12, 13, 1, 3],	9. [9–11, 13, 14, 2, 4],	10. [10–12, 14, 0, 3, 5],	11. [11–13, 0, 1, 4, 6],
12. [12–14, 1, 2, 5, 7],	13. [13, 14, 0, 2, 3, 6, 8],	14. [14, 0, 1, 3, 4, 7, 9].	

Двойственная циклическая проективная плоскость DPP(3,2) имеет 15 дуальных блоков:

0. [0, 14, 13, 11, 10, 7, 5], 1. [1, 0, 14, 12, 11, 8, 6], 2. [2, 1, 0, 13, 12, 9, 7], 3. [3, 2, 1, 14, 13, 10, 8],
4. [4, 3, 2, 0, 14, 11, 9], 5. [5, 4, 3, 1, 0, 12, 10], 6. [6, 5, 4, 2, 1, 13, 11], 7. [7, 6, 5, 3, 2, 14, 12],
8. [8, 7, 6, 4, 3, 0, 13], 9. [9, 8, 7, 5, 4, 1, 14], 10. [10, 9, 8, 6, 5, 2, 0], 11. [11, 10, 9, 7, 6, 3, 1],
12. [12, 11, 10, 8, 7, 4, 2], 13. [13, 12, 11, 9 , 8, 5, 3], 14. [14, 13, 12, 10, 9, 6, 4].

2.2. Построение блоков и дуальных блоков ациклических проективных плоскостей. Пусть F_n – поле порядка $n = p^k$, а x – его примитивный элемент, $F(n^{d+1})$ – его алгебраическое расширение степени $d + 1$, рассматриваемое как векторное пространство V размерности $d + 1$, а также как поле, порождаемое примитивным полиномом степени $d + 1$ над полем F_n. Множество $V^* = V\backslash\{0\}$ по отношению коллинеарности разбивается на классы эквивалентности. В качестве представителей этих классов удобно выбрать нормированные многочлены множества V^*. Их совокупность V' составляет проективное пространство размерности d. Его элементы являются проективными подпространствами нулевой размерности, или точками (представителями классов коллинеарности – подпространств единичной размерности векторного пространства V). Множества из d различных точек образуют базисы линий проективного пространства и одновременно нормированные базисы подпространств размерности d векторного пространства V. Имеется

$$N_d = (n^{d+1} - 1)/(n - 1) = n^d + nn^{d-1} + \ldots + n + 1$$

точек и такое же количество линий. Множества точек и линий образуют проективную плоскость $PP(d,n)$ размерности d и порядка n. Будем использовать следующие методы нумерации элементов векторных пространств размерности s и проективных пространств размерности $s - 1$. Номерами ненулевых элементов поля F_n считаются их индексы по основанию образующего элемента x, а нулевому элементу присваивается номер 0 (т.е. полагаем, что индекс нулевого элемента поля равен нулю: ind 0=0). Элементам $e = (e_0, \ldots, e_{s-2}, e_{s-1}) \in F(n^s)$ присвоим номера

$$\varphi(e) = \mathrm{ind}e_0 + n\mathrm{ind}e_1 + \ldots + n^{s-2}\mathrm{ind}e_{s-2} + n^{s-1}\mathrm{ind}e_{s-1}.$$

При этом числовым образом векторного пространства F_n^s будет множество $\overline{\{0, n^s - 1\}}$.

Номер $\psi(e)$ элемента $e = (e_0, e_1, \ldots, e_{s-2}, 1)$ проективного пространства размерности $s - 1$ будем определять формулой

$$\psi(e) = \varphi(\hat{e}) + N_{s-2}, \quad s \geq 1,$$

полагая, что $\hat{e} = (e_0, e_1, \ldots, e_{s-2})$, $\psi(1) = 0$, $N_0 = 1$. Нумерации

$$\varphi: F_n^s \to \overline{\{0, n^s - 1\}}$$

и

$$\psi: V' \to \overline{\{0, (n^s - 1)/(n - 1) - 1\}}$$

являются биекциями и, следовательно, обратимы:

$$\varphi^{-1}(M) = \begin{cases} 0, & \text{если} \quad M = 0, \\ (x^{i_0}, \ldots, x^{i_{s-2}}, x^{i_{s-1}}), & \text{если} \quad M > 0, \end{cases}$$

где $(i_0, \ldots, i_{s-2}, i_{s-1})$ есть набор коэффициентов разложения числа M по степеням числа n;

$$\psi^{-1}(M') = \begin{cases} 1, & \text{если} \quad M' = 0, \\ (x^{i_0}, \ldots, x^{i_{s-2}}, 1), & \text{если} \quad M' > 0, \end{cases}$$

где $(i_0, \ldots, i_{s-2})$ есть набор коэффициентов разложения по степеням n числа $M = M' - N_{s-2}$. При такой нумерации получаем каноническое представление проективной плоскости, т.е. $(n^2 + n + 1, n + 1, 1)$-УНБС как комбинаторной блок-схемы: множество $\mathbf{X}$ элементов – это множество неотрицательных целых чисел $\overline{0, n^2 + n}$ (образов точек), а множество $\mathbf{B}$ блоков – это множество наборов B номеров точек, составляющих линии,– образы линий. Ниже будет показано, что блоки

Таблица 1

Порядковый номер t линии	$t = 0$	$t = \overline{1, n}$	$t = jn + i,\ j = \overline{1, n},\ i = \overline{1, n}$
$(\mathbf{e}^{(1)}, \mathbf{e}^{(2)})$	$((1), (0,1))$	$((1), (0, x^{t-1}, 1))$	$((x^{j-1}, 1), (x^{i-1}, 0, 1))$
$(\psi(\mathbf{e}^{(1)}), \psi(\mathbf{e}^{(2)}))$	$(0, 1)$	$(0, 1+ n\ t)$	$(j, n + i)$

также можно упорядочить, пронумеровав их начальными неотрицательными целыми числами $\overline{0, N_2 - 1}$.

Для вычисления блоков будем использовать их алгебраические идентификаторы, базисы линий в проективном пространстве размерности два, образованные парами многочленов $(\mathbf{e}^{(1)}, \mathbf{e}^{(2)})$. Пусть первыми элементами таких пар являются многочлен (1) нулевой степени или нормированные многочлены $(e_0, 1)$ первой степени. Вторые элементы $\mathbf{e}^{(2)}$ базисов остальных блоков подберем из числа многочленов, не принадлежащих алгебраическим замыканиям других базисов с тем же первым элементом $\mathbf{e}^{(1)}$. Пары многочленов, соответствующие базисам линий с номером t, представлены в табл. 1.

Алгебраические замыкания базисов в проективном пространстве суть его линии, а их образы – блоки проективной плоскости на множестве **X.** По номерам $\psi(\mathbf{e}^{(1)})$ и $\psi(\mathbf{e}^{(2)})$ первого и второго элементов базиса можно определить порядковый номер $N(\psi(\mathbf{e}^{(1)}), \psi(\boldsymbol{e}^{(2)}))$ порождаемой им линии и, следовательно, номер ее числового образа, т.е. блока:

$$N(\psi(\mathbf{e}^{(1)}), \psi(\mathbf{e}^{(2)})) = \begin{cases} (\psi(\mathbf{e}^{(2)}) - 1)/n, & \text{если} \quad \psi(\mathbf{e}^{(1)}) = 0, \\ \psi(\mathbf{e}^{(1)})n + \psi(\mathbf{e}^{(2)}) - N_1 + 1, & \text{если} \quad \psi(\mathbf{e}^{(1)}) > 0. \end{cases}$$

При этом блоки получают анонсированные выше номера $\overline{0, N_2 - 1}$.

Алгебраическое замыкание $\langle\{\mathbf{e}^{(1)}, \mathbf{e}^{(2)}\}\rangle$ базиса можно вычислить, добавляя линейные комбинации $\mathbf{e}^{(2)} + x^t\mathbf{e}^{(1)}$, $t = \overline{1, n-1}$, поскольку все элементы блока являются нормированными многочленами. В этом случае вычисляется и соответствующий блок

$$\{\psi(\mathbf{e}^{(1)}), \psi(\mathbf{e}^{(2)}), \psi(\mathbf{e}^{(2)} + x^1\mathbf{e}^{(1)}), \ldots, \psi(\mathbf{e}^{(2)} + x^{n-1}\mathbf{e}^{(1)})\}.$$

Пример 2. Представим числовые образы базисов линий проективной плоскости (21, 5, 1) списком пар элементов, упорядоченных по возрастанию номеров порождаемых базисами блоков:

((0, 1), (0, 5), (0, 9), (0, 13), (0, 17), (1, 5), (1, 6), (1, 7), (1, 8), (2, 5), (2, 6), (2, 7), (2, 8), (3, 5), (3, 6), (3, 7), (3, 8), (4, 5), (4, 6), (4, 7), (4, 8)).

Вычислим, например, блок B_{12} по образу (2,8) линии $(\psi^{-1}(2), \psi^{-1}(8))$ как образ замыкания:

$$\begin{gathered} \langle\psi^{-1}(2), \psi^{-1}(8)\rangle = \langle((x,\ 1), (1,\ 0, 1))\rangle = \\ = \{(x,1), (1,0,1), (1,0,1) + x(x,1), (1,0,1) + (x+1)\ (x,1), (1,0,1) + 1(x,1)\} = \\ = \{(x,\ 1), (1,0,1), (x,x,1), (0, x+1, 1), (x+1, 1, 1)\}. \end{gathered}$$

Отсюда

$$B_{12} = \{\psi(x,1), \psi(1,0,1), \psi(x,x,1), \psi(0, x+1,\ 1), \psi(x+1,\ 1,\ 1)\} = (2,\ 8,\ 10,\ 13,\ 19).$$

По номеру j блока можно определить образы (номера) первого $n_1(j)$ и второго $n_2(j)$ элементов базиса его прообраза:

$$n_1(j) = \begin{cases} 0, & \text{если} \quad j \le n, \\ \left\lfloor \dfrac{j-1}{n} \right\rfloor, & \text{если} \quad j > n, \end{cases} \qquad n_2(j) = \begin{cases} 1 + nj, & \text{если} \quad j \le n, \\ j - (n_1(j) - 1)n, & \text{если} \quad j > n. \end{cases}$$

Таким образом, доказано следующее утверждение.

Таблица 2

Порядковый номер t линии	$t = 0$	$t = \overline{1,n}$	$t = jn + i,$ $j = \overline{1,n},$ $i = \overline{1,n}$	$t = jn^2 + in + r,$ $j = \overline{1,n},$ $i = \overline{1,n},$ $r = \overline{1,n}$
$(\mathbf{e}^{(1)}, \mathbf{e}^{(2)}, \mathbf{e}^{(3)})$	((1), (0,1), (0,0,1))	((1), (0,1), $(0,0,x^{t-1},1)$)	((1), $(0,x^{j-1},1)$, $(0,x^{i-1},0,1)$)	$((x^{j-1},1)$, $(x^{i-1},0,1)$, $(x^{r-1},0,0,1))$
$(\psi(\mathbf{e}^{(1)}), \psi(\mathbf{e}^{(2)}), \psi(\mathbf{e}^{(3)}))$	$(0, 1, n+1)$	$(0, 1, tn^2 + n + 1)$	$(0, nj + 1, n^2 + ni + 1)$	$(j, n + i, n^2 + n + r)$

Утверждение 3 [15]. Блок, имеющий номер j, проективной плоскости можно получить по формуле

$$\psi(\langle\{\psi^{-1}(n_1(j)), \psi^{-1}(n_2(j))\}\rangle).$$

Заметим, что число 0 имеется в блоках $B_0, B_1, B_2, \ldots, B_n$, содержащих числа $\overline{0,n}$, а числа i, $1 < i < n$ включаются в блок B_0 и блоки B_{tn+i}, $t = \overline{1,n}$. Каждое из остальных чисел $j \in \mathbf{X}$ присутствует в $n + 1$ блоках, каждый раз с одним из чисел $\overline{0,n}$. Если $j \le 2n$, то j есть второй элемент блока, т.е. числовой образ $\psi(\mathbf{e}^{(2)})$ второго элемента базиса, который можно определить по j и числовому образу $\psi(\mathbf{e}^{(1)})$ первого элемента базиса:

$$\psi(\mathbf{e}^{(2)}) = \begin{cases} jn + 1, & \text{если} \quad \psi(\mathbf{e}^{(1)}) = 0, \\ j - (\psi(\mathbf{e}^{(1)}) - 1)n, & \text{если} \quad \psi(\mathbf{e}^{(1)}) > 0. \end{cases}$$

Если $j > 2n$, то оно есть образ $3, 4, \ldots n$-го или $n + 1$-го элемента блока. При знании первого элемента, применяя обращенное правило его вычисления по первому и второму элементам, получаем второй элемент блока.

Утверждение 4 [15]. Множество номеров блоков проективной плоскости, содержащих заданный элемент s, представимо формулой

$$B(s) = \begin{cases} \{0\} \cup \{s * n + t : t = \overline{1,n}\}, & \text{если} \quad s \le n, \\ \{B_0(s)\} \cup \{B_k(s) : k = \overline{1,n}\}, & \text{если} \quad s > n, \end{cases}$$

где

$$B_0(s) = \left.\frac{\psi(\psi^{-1}(s) - x^i) - 1}{n}\right|_{\psi(\psi^{-1}(s)-x^i) \bmod n = 1},$$

$$B_k(s) = \psi(\psi^{-1}(s) - x^i\psi^{-1}(k)) + (k-1)n\Big|_{\psi(\psi^{-1}(s)-x^i\psi^{-1}(k)) \le 2n,\ i \in \{\overline{0,n-1}\}}.$$

Проективные плоскости большей размерности строятся аналогично. В частности, базисы прообразов блоков для PP(3,n) представлены в табл. 2.

Исходя из этого можно сформулировать утверждения, аналогичные рассмотренным в данном разделе применительно к проективным плоскостям PP(3,n).

2.3. Построение блока трансверсальной блок-схемы по его номеру и множества блоков, содержащих данный элемент. Линейная трансверсальная комбинаторная блок-схема TD(k,n) [1, 3] строится из элементов k попарно не пересекающихся множеств w_i, содержащих по n элементов, и состоит из n^2 множеств Y_j, $j = \overline{1,n^2}$, содержащих по k элементов. При этом каждое множество Y_j имеет точно один элемент из каждого множества w_i, $i = \overline{0,k-1}$, и если $j \ne s$, то Y_j и Y_s имеют не более одного общего элемента. Таким образом, комбинаторная блок-схема TD(k, n) определена на множестве мощности kn. Если n –

простое число или степень простого числа, то TD(k, n) существует. Тогда в алгебраической интерпретации она определяется на множестве пар (x_1, y), $x_1 \in \mathbf{X_1}$, где $\mathbf{X}_1$ есть множество из k элементов поля F_n, $y \in F_n$; блоки линейной трансверсальной блок-схемы $TD(k, n)$ определяются парой элементов $(a, b) \in F(n^2)$ [8]:

$$B_{a,b} = \{(ax_1 + b, x_1) : x_1 \in \mathbf{X_1}\}.$$

В числовой интерпретации [15] линейная трансверсальная блок-схема TD(k, n) над полем F_n задается на числовом множестве

$$\mathbf{X} = \{s : s = \varphi(x^j, x^i),\ i \in \overline{(0, k-1)},\ j \in \overline{(0, n-1)}\},$$

где x – примитивный элемент поля. Ее блоками являются множества

$$B_{a,b} = \{\varphi(ax^i + b, x^i), i = (0, k-1)\}, \quad a, b \in F_n.$$

Пусть номера блоков $B_{a,\,b}$ представляются числами $N^{(2)}(B_{a,\,b}) = \varphi(a, b)$. Вычислим множество $G_{TD(k,n)}(t)$ номеров блоков $B_{a,\,b}$, содержащих элемент $t \in \mathbf{X}$, т.е. дуальный блок с номером t. Заметим, что $\varphi^{-1}(t) = (x^{(t-\lfloor t/n \rfloor n)}, x^{\lfloor t/n \rfloor})$. Таким образом, получено следующее утверждение.

У т в е р ж д е н и е 4 [8, 15]. Справедливы представления

$$B_{a,b} = (\varphi(ax^i + b, x^i)), \quad i = (0, k-1), \quad a, b \in F_n;$$
$$G_{\mathrm{TD}(k,n)}(t) = \{\varphi(a, b) : \{a, b \in F_n; \varphi(ax^{\lfloor t/n \rfloor} + b, x^{\lfloor t/n \rfloor}) = t\}, \quad t \in \mathbf{X}.$$

Трансверсальная блок-схема TD(t, k, n) – это тройка ($\mathbf{X}$, $\mathbf{H}$, $\mathbf{A}$), где $\mathbf{X}$ – конечное множество мощности kn, $\mathbf{H}$ – разбиение $\mathbf{X}$ на k частей, называемых группами, размера n, $\mathbf{A}$ – множество k-подмножеств множества $\mathbf{X}$, называемых блоками, которая удовлетворяет следующим условиям:

(1) $|H \cap A| = 1$ для каждого $H \in \mathbf{H}$ и каждого $A \in \mathbf{A}$,

(2) каждое t-подмножество множества $\mathbf{X}$ из t различных групп оказывается точно в одном блоке из $\mathbf{A}$.

Если n – простое число или его степень, то TD(t, k, n) существует. В алгебраической интерпретации в этом случае блоки квадратичной трансверсальной блок-схемы TD(3, k, n) определяются тройками элементов $(a, b, c) \in F(n^3)$:

$$B_{a,b,c} = \{(ax_1^{\,2} + bx_1 + c, x_1) : x_1 \in \mathbf{X}_1\},$$

где $\mathbf{X}_1$ есть множество из k элементов поля F_n [8].

В числовой интерпретации [15] квадратичная трансверсальная блок-схема TD(t, k, n) над полем F_n также задается на числовом множестве

$$\mathbf{X} = \{s : s = \varphi(x^j, x^i), i \in \overline{(0, k-1)}, j \in \overline{(0, n-1)}\},$$

где x есть примитивный элемент поля.

Пусть номерами блоков $B_{a,\,b,\,c}$ являются числа $N^{(3)}(B_{a,\,b,\,c}) = \varphi(a, b, c)$. Множество $G_{\mathrm{TD}(3,k,n)}(t)$ номеров блоков $B_{a,\,b,\,c}$, содержащих элемент $t \in \mathbf{X}$, также можно определить, учитывая, что $\varphi^{-1}(t) = (x^{r_0}, x^{r_1}, x^{q_1})$, где

$$r_0 = t - q_0 n \quad \text{при} \quad q_0 = \lfloor t/n \rfloor;$$
$$r_1 = q_0 - q_1 n \quad \text{при} \quad q_1 = \lfloor q_0/n \rfloor.$$

Таким образом, получено следующее утверждение.

У т в е р ж д е н и е 5 [8, 15]. Справедливы представления

$$B_{a,b,c} = \{\varphi(ax^{2i} + bx^i + c, x^i), i \in \overline{\{0, k-1\}}\}, \quad \{a, b, c\} \subseteq F_n;$$

$$G_{\mathrm{TD}(3,k,n)}(t) = \{\varphi(a, b, c) : \{a, b, c\} \subseteq F_n; \varphi(ax^{2\lfloor t/n \rfloor} + bx^{\lfloor t/n \rfloor} + c, x^{\lfloor t/n \rfloor}) = t\}.$$

Полученные аналитические представления блоков комбинаторных блок-схем и их двойственных аналогов легко трансформируются в алгоритмы. Они были протестированы с использованием системы компьютерной алгебры Sage [13], ассоциированной с алгебраическим процессором МЭИ [14].

Пример 3. Схема ячеистой связи по квадратичной трансверсальной блок-схеме TD(3,3,3) и двойственной такой блок-схеме. Здесь $d = 3$, $k = 3$, $n = 3$.

По умолчанию, элементами блок-схемы TD(3,3,3) являются числа $\overline{0,8}$, их количество есть $kn = 9$. В этой блок-схеме $n^3 = 27$ блоков по три элемента:

0. [0, 3, 6], 1. [0, 4, 7], 2. [0, 5, 8], 3. [0, 5, 7], 4. [0, 3, 8], 5. [0, 4, 6], 6. [0, 4, 8], 7. [0, 5, 6], 8. [0, 3, 7], 9. [1, 4, 7], 10. [1, 5, 8], 11. [1, 3, 6], 12. [1, 3, 8], 13. [1, 4, 6], 14. [1, 5, 7], 15. [1, 5, 6], 16. [1, 3, 7], 17. [1, 4, 8], 18. [2, 5, 8], 19. [2, 3, 6], 20. [2, 4, 7], 21. [2, 4, 6], 22. [2, 5, 7], 23. [2, 3, 8], 24. [2, 3, 7], 25. [2, 4, 8], 26. [2, 5, 6].

Имеется $kn = 9$ блоков двойственной трансверсальной блок-схемы DTD(3,3,3), т.е. множеств номеров блоков из TD(3,3,3), содержащих элемент, являющийся номером дуального блока:

0. [0, 1, 2, 3, 4, 5, 6, 7, 8],
1. [9, 10, 11, 12, 13, 14, 15, 16, 17],
2. [18, 19, 20, 21, 22, 23, 24, 25, 26],
3. [0, 4, 8, 11, 12, 16, 19, 23, 24],
4. [1, 5, 6, 9, 13, 17, 20, 21, 25],
5. [2, 3, 7, 10, 14, 15, 18, 22, 26],
6. [0, 5, 7, 11, 13, 15, 19, 21, 26],
7. [1, 3, 8, 9, 14, 16, 20, 22, 24],
8. [2, 4, 6, 10, 12, 17, 18, 23, 25].

Сеть построена из 27 узлов, каждый из которых представляет собой полносвязную сеть из трех компьютеров. Каждый компьютер при этом входит в одну из девяти полносвязных подсетей, включающих по 9 компьютеров, он помечается номером этой подсети. Эти номера суть элементы TD(3, 3, 3), а блоки – тройки номеров, пометки компьютеров узла. Дуальные блоки включают номера блоков, содержащих номер данного дуального блока. Любые два компьютера из разных узлов могут принадлежать одной полносвязной сети из девяти компьютеров (если имеют одинаковые пометки), тогда компьютеры связаны непосредственно. Если же они оба не принадлежат ни одной такой сети (имеют разные пометки), то в узлах, в которые они входят, могут быть компьютеры с одинаковыми пометками или общих пометок нет. Тогда в первом случае необходимы три шага для соединения, а во втором – четыре шага. Таким образом, любые два компьютера либо связаны непосредственно, либо через двух или трех посредников. Эта система трехуровневая: уровни компьютеров (по умолчанию), узлов и полносвязных сетей. Подсистемы второго и третьего уровней соответствуют классам двух разбиений элементов первого уровня. Эта же комбинаторная схема имеет еще одну интерпретацию, представляющую собой формализацию схемы предварительного распределения ключей в беспроводной сенсорной сети. При этом элементы – это номера различных ключей. Блоки соответствуют узлам сети и являются множествами номеров ключей, встроенных в память узла. Дуальные блоки содержат номера узлов, которые имеют ключ, номер которого есть номер дуального блока. Узлы, в блоках которых имеется элемент с данным номером, могут коммутировать с использованием ключа с этим номером. Иначе найдется узел, в блоке которого имеется элемент, содержащийся в блоке первого узла, и другой элемент, содержащийся в блоке второго узла. Тогда возможна коммутация между двумя узлами с использованием этих двух ключей третьего узла, например с зашифрованием в первом узле, расшифрованием и зашифрованием в третьем узле и расшифрованием во втором узле.

Возможны подобные интерпретации любых трансверсальных комбинаторных блок-схем TD(3, k, n) и DTD(3, k, n). Так TD(3, 3, 4) и DTD(3, 3, 4) имеют 64 блока по три элемента и 12 дуальных блоков по 16 элементов.

Заключение. В статье обоснован метод синтеза систем, структура которых соответствует комбинаторной блок-схеме одной из рассматриваемых разновидностей при условии, что порядок блок-схемы является простым числом или степенью простого числа, отличающийся применением числовой и алгебраической формализации таких систем с использованием алгебраических идентификаторов блоков.

Получены аналитические представления, по которым блоки и дуальные блоки как циклических, так и ациклических проективных плоскостей, а также линейных и квадратичных трансверсальных блок-схем вычисляются независимо или параллельно.

Этот метод на содержательном уровне предполагает определение разновидности комбинаторной блок-схемы, которой соответствует структура синтезируемой системы, подбор основных

параметров комбинаторной блок-схемы и ее двойственного аналога. Далее в соответствии с правилом двойственности осуществляется нумерация элементов, блоков и дуальных блоков комбинаторной блок-схемы. При этом строятся и используются характерные для данного типа комбинаторной блок-схемы алгебраические идентификаторы блоков. Вычисляются все или отдельные блоки и дуальные блоки. При реализации системы или ее подсистемы осуществляется предметная интерпретация построенной комбинаторной блок-схемы или отдельных блоков и анализируются свойства синтезированной системы, обусловленные свойствами комбинаторной модели. Различные предметные системы допускают одну и ту же формализацию в виде комбинаторной блок-схемы, и наоборот, конкретная комбинаторная блок-схема может иметь различные предметные интерпретации. Естественно, что рассмотренные подходы позволяют строить аффинные плоскости как остаточные комбинаторные блок-схемы. Наконец, синтез трансверсальных комбинаторных систем по существу эквивалентен построению ортогональных латинских квадратов и ортогональных массивов. Алгебраические идентификаторы блоков могут использоваться также для решения некоторых производных задач, связанных с вычислением пересечений блоков или дуальных блоков или определением блока, имеющего пересечения с каждым из двух данных блоков для выявления характера связей в системе.

СПИСОК ЛИТЕРАТУРЫ

1. *Холл М.* Комбинаторика. М.: Мир, 1970.
2. *Сачков В.Н.* Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004.
3. *Stinson D.* Combinatorial Designs: Constructions and Analysis. Berlin, Germany: Springer, 2003.
4. *Colbourn C., Dinitz J. Eds*. The CRC Handbook of Combinatorial Designs, 2nd Ed. Boca Raton: CRC Press, 2007.
5. *Каравай М.Ф., Пархоменко П.П., Подлазов В.С.* Комбинаторные методы построения двудольных однородных неизбыточных квазиполносвязных графов (симметричных блок-схем) // АиТ. 2009. № 2. С. 133–164.
6. *Пархоменко П.П., Каравай М.Ф.* Кратные комбинаторные блок-схемы // АиТ. 2013. № 6. С. 121–131.
7. *Пархоменко П.П.* Алгоритмизация синтеза комбинаторных блок-схем одного класса // АиТ. 2016. № 7. С. 113 –122.
8. *Lee J., Stinson D.R.* On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs // ACM Transactions on Information and Systems Security. 2008. V. 11. № 2. Article 5.
9. *Du D., Hwang F., Wu W., Znati T.* New Construction for Transversal Design // J. Computational Biology. 2006. V. 13. № 4. P. 990–995.
10. *Andrew B., MacConnel A.B., Price A.K., Brian M., Paege B.M.* An Integrated Microfluidic Processor for DNA-Encoded Combinatorial Library Functional Screening // ACS Comb Sci. 2017. V. 19. № 3. P. 181–192.
11. *Черемушкин А.В.* Комбинаторно-геометрические подходы к построению схем предварительного распределения ключей (обзор). Прикладная математика. Математические методы криптографии. 2008. № 11 (1). С. 55–63.
12. *Paterson M.B., Stinson D.R.* Unified Approach to Combinatorial Key Predistribution Schemes for Sensor Networks // Designs, Codes and Cryptography. 2014. V. 71, Iss. 3. P. 433–457.
13. Sage web site https://www.sagemath.org. (дата последнего обращения 13.11.2019)
14. *Frolov A.B., Vinnikov A.M.* Modeling Cryptographic Protocols Using Computer Algebra Systems 2020 // V Intern. Conf. on Information Technologies in Engineering Education. Moscow, Russia, 2020. P. 1–4.
15. *Фролов А.Б., Клягин А.О., Кочетова Н.П., Темников Д.Ю.* Распределенное вычисление комбинаторных блок-схем // Проблемы теоретической кибернетики. Матер. заочного семинара XIX Междунар. конф. / Под ред. Ю.И. Журавлева. Казань, 2020. С. 126–129.