МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи

Чередник Игорь Владимирович

Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований

Специальность 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата физико-математических наук

Научные руководители
д.ф.-м.н., профессор
Черемушкин Александр Васильевич
к.ф.-м.н.
Галатенко Алексей Владимирович

Москва — 2021

Оглавление

Введение

Актуальность темы. Диссертация посвящена поиску новых решений по синтезу кратно транзитивных классов блочных преобразований, архитектура которых представляет собой уникальную (для класса) сеть, с узлами отвечающими одной бинарной операции.

Эффективно реализуемые кратно транзитивные классы преобразований имеют важное значение для проектирования узлов переработки информации в области защиты конфиденциальных данных, поскольку отсутствие кратной транзитивности у семейства преобразований, выполняемых узлом, фактически означает наличие запретов в выходных последовательностях данных узлов и в некоторых случаях позволяет идентифицировать начальные состояния и/или часть постоянных параметров изучаемых узлов. Это обстоятельство обосновывает актуальность построения эффективно реализуемых кратно транзитивных семейств блочных преобразований.

Степень разработанности темы. В последнее время при разработке систем защиты информации активно исследуется возможность использования неассоциативных алгебраических структур и особое место в таких исследованиях занимают квазигруппы (см., например, обзоры [5, 51] и книги [18, 20]).

В ряде работ [8, 11, 16, 17, 19, 21–25, 28–38, 41, 42, 44–46, 50, 58, 59] с различных позиций исследуются сжимающие отображения, реализуемые «цепными» формулами типа

$$\big((a * x_1) * \dots\big) * x_n, \quad a \in \Omega, \tag{1}$$

а также семейства блочных преобразований $\Omega^n \to \Omega^n$, реализуемые наборами формул вида

$$\Big(a*x_1, (a*x_1)*x_2, \dots, \big((a*x_1)*\dots\big)*x_n\Big), \quad a \in \Omega, \tag{2}$$

где $*$ — квазигрупповая операция на некотором конечном множестве Ω (подробнее об истории развитии данного вопроса можно прочитать в обзорах [5, 51] и работах [16, 19, 21, 41]). При этом в подавляющем большинстве рассматриваемых схем квазигрупповая операция $*$ выбирается из небольшого множества

отобранных квазигрупп и параметризация соответствующего класса преобразований достигается в основном за счет выбора «начального» элемента $a \in \Omega$.

Приведенные выше конструкции в работах [8, 11, 16, 17, 19, 21–25, 28–36, 41, 42, 44–46, 50] предлагается использовать в качестве основы для построения таких различных узлов переработки информации, как поточные шифры [29, 33, 41], шифрсистемы с открытым ключом [25, 32], хеш-функции [8, 16, 17, 23, 24, 30, 34, 36], и пр. [11, 21, 22, 28, 31, 50, 51]. Первичный анализ схем подобного рода и отдельных их составляющих был проведен в [8, 16, 17, 19, 21–25, 28–39, 41, 42, 44–46, 50, 51, 58, 59], а также в ряде других работ. Заметим также, что анализ стойкости узлов защиты и переработки информации, которые основаны на итеративной композиции сжимающих отображений вида (1) и блочных преобразований, реализуемых наборами формул вида (2) во многом сводится к такой классической задаче, как исследование функциональной полноты квазигруппы $*$. И в этом направлении можно отметить фундаментальные и значительные результаты, полученные В. А. Артамоновым [1], а также А. В. Галатенко, А. Е. Панкратьевым и С. Б. Родиным [3, 4].

Однако, как было отмечено выше, для семейств преобразований, используемых в узлах защиты информации, одной из значимых характеристик является кратная транзитивность данного семейства. А в случае преобразований, реализуемых простыми наборами формул вида (2), во-первых, неизвестно являются ли данные классы блочных преобразований хотя бы транзитивными и, во-вторых, отсутствуют практически эффективные методы, которые позволяли бы это выяснить или гарантировать.

Кроме того, при проведении анализа реальных узлов защиты информации редко возникает задача исследования семейств преобразований, которые допускают описание в терминах примитивных формул вида (1) или (2). Поэтому в диссертации рассматривается существенно более общая модель построения классов блочных преобразований, которые определяются фиксированным набором формул и параметрически зависят от выбора бинарной операции.

Пусть Ω — произвольное конечное множество, $\mathcal{B}(\Omega)$ — множество всех бинарных операций, определенных на Ω, $\{x_1, \ldots, x_n\}$ — множество переменных и $*$ — общий символ бинарной операции. Произвольная формула $w(x_1, \ldots, x_n)$ в алфавите $\{x_1, \ldots, x_n, *\}$ при сопоставлении символу $*$ конкретной бинарной операции $F \in \mathcal{B}(\Omega)$ реализует функцию $w^F \colon \Omega^n \to \Omega$, а набор формул $(w_1, \ldots, w_m)$ реализует отображение $(w_1^F, \ldots, w_m^F) \colon \Omega^n \to \Omega^m$.

Объект исследований. Объектом исследований диссертации являются классы блочных преобразований

$$\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{K}\}, \quad \mathcal{K} \subset \mathcal{B}(\Omega),$$

реализуемые произвольным фиксированным набором формул $(w_1, \ldots, w_n)$ при выборе различных бинарных операций $F \in \mathcal{K}$.

Один из способов построения произвольного набора формул $(w_1, \ldots, w_m)$ состоит в последовательном преобразовании набора переменных $(x_1, \ldots, x_n)$. Каждая последовательность преобразований набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$ допускает наглядное представление в виде подходящей бинарной функциональной сети Σ, у которой степень захода каждой вершины не превосходит 2. При этом удобно говорить, что сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$, а при выборе бинарной операции $F \in \mathcal{B}(\Omega)$ реализует отображение $\Sigma^F = (w_1^F, \ldots, w_m^F)$.

Если сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$, при котором каждый промежуточный набор содержит ровно n формул (каждый слой сети Σ содержит ровно n вершин), то будем называть Σ сетью постоянной ширины. Сети постоянной ширины представляют особый интерес с точки зрения удобства практической реализации.

Предложенный «сетевой» подход к описанию класса преобразований

$$\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{K}\}, \quad \mathcal{K} \subset \mathcal{B}(\Omega),$$

является достаточно естественным развитием конструкции классической сети Фейстеля [13, 47, 54, 60] и ее известных обобщений [40, 49, 56, 57] с той отличительной особенностью, что бинарные операции (используемые в узлах сети)

предполагаются зависящими нетривиальным образом от секретных параметров системы защиты информации и уникальными для каждой реализации — указанная особенность не позволяет составить между обрабатываемыми данными и секретными параметрами простые функциональные соотношения, из которых возможно эффективно определить хотя бы часть секретных параметров. Таким образом, предложенную в работе модель классов блочных преобразований $\{\Sigma^F : F \in \mathcal{K}\}$, $\mathcal{K} \subset \mathcal{B}(\Omega)$ можно рассматривать в качестве аппроксимации классов блочных преобразований, которые реализуются в некоторых известных узлах защиты информации [9,52,53]. Также стоит отметить, что конструкция сети Фейстеля давно уже используется не только в качестве базы при проектировании блочных шифров, но и для построения специальных усложняющих преобразований, используемых в узлах обработки и защиты информации [14,15,27], случайных подстановок [43, 48], и даже линейных отображений [12].

Предмет исследований. Как известно, одним из трех основных принципов информационной безопасности является конфиденциальность обрабатываемой/передаваемой информации. Кратная транзитивность множества преобразований узла обработки и защиты информации является практическим приближением и следствием предложенного Шенноном теоретического понятия совершенной секретности и соответственно играет важную роль в обеспечении конфиденциальности. Предметом исследований является построение кратно транзитивных классов блочных преобразований

$$\{\Sigma^F : F \in \mathcal{R}(\Omega)\},$$

которые реализуются произвольной фиксированной бинарной функциональной сетью Σ постоянной ширины, а в качестве параметрического множества бинарных операций $\mathcal{R}(\Omega)$ используются следующие семейства бинарных операций:

- $\mathcal{Q}(\Omega)$ — все бинарные операции обратимые по обеим переменным (бинарные квазигруппы);
- $\mathcal{B}^*(\Omega)$ — все бинарные операции обратимые по правой переменной.

Использование класса $\mathcal{Q}(\Omega)$ в качестве параметризующего множества бинарных операций позволяет исследовать бинарные функциональные сети наибо-

лее общего строения — данное обстоятельство обуславливает теоретическую значимость рассмотрения класса $\mathcal{Q}(\Omega)$. Однако, если обратимость глобальных преобразований, реализуемых сетью, является естественным требованием, то обратимость операции-параметра по обеим переменным в случаях некоторых сетей может оказаться завышенным требованием. Для достаточно широкого класса сетей в качестве параметризующего множества бинарных операций разумно рассматривать класс $\mathcal{B}^*(\Omega)$, который является максимальным в смысле обеспечения обратимости глобальных блочных преобразований, реализуемых сетью. При этом в случае класса $\mathcal{B}^*(\Omega)$ существенно упрощается генерация бинарной операции-параметра — данное обстоятельство обуславливает практическую значимость рассмотрения класса $\mathcal{B}^*(\Omega)$. В заключение, отметим, что в работе показана нецелесообразность использования каких-либо других классов бинарных операций (отличных от $\mathcal{Q}(\Omega)$ и $\mathcal{B}^*(\Omega)$) в качестве множества параметров.

Цели и задачи исследования. Основные цели исследования относятся к сфере анализа и синтеза систем защиты информации. В области анализа целью является разработка методов исследования кратной транзитивности произвольного класса блочных преобразований вида $\{\Sigma^F \,:\, F \in \mathcal{R}(\Omega)\}$. В области синтеза — построение на основе бинарных функциональных сетей кратно транзитивных классов блочных преобразований вида $\{\Sigma^F \,:\, F \in \mathcal{R}(\Omega)\}$.

Для достижения поставленных целей решаются следующие задачи:

1. Описание бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из множества $\mathcal{R}(\Omega)$ (далее $\mathcal{R}$-биективные сети).

2. Разработка эффективных методов проверки кратной транзитивности класса блочных преобразований $\{\Sigma^F \,:\, F \in \mathcal{R}(\Omega)\}$, определяемых произвольной $\mathcal{R}$-биективной сетью Σ.

3. Разработка алгоритмов построения $\mathcal{R}$-биективных сетей Σ, для которых соответствующие классы преобразований $\{\Sigma^F \,:\, F \in \mathcal{R}(\Omega)\}$ обладают требуемой кратной транзитивностью.

4. Построение классов $\mathcal{R}$-биективных сетей Σ с небольшим количеством вершин, для которых соответствующие классы $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ обладают требуемой кратной транзитивностью.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения и списка литературы, включающего 66 наименований.

В первой главе определяются основные понятия бинарных функциональных сетей, приводится описание класса биективных бинарных функциональных сетей постоянной ширины и предлагаются методы исследования бинарных функциональных сетей, которые используются в последующих главах диссертации.

В §1.1 определяются основные понятия бинарных функциональных сетей, которые позволяют наглядно представлять классы блочных преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$ (определения 1.1–1.9).

В §1.2 доказывается критерий $\mathcal{Q}$-биективности произвольной бинарной сети постоянной ширины в терминах ее матрицы смежности (теорема 1.1) и для произвольной $\mathcal{R}$-биективной сети доказывается существование эквивалентного представления в виде произведения элементарных и перестановочной сетей (теоремы 1.2 и 1.5).

В §1.3 вводится понятие разметки $\mathcal{R}$-биективной сети — инструмента, который позволяет обнаруживать особенности $\mathcal{R}$-биективной сети, нарушающие её транзитивность, (определения 1.10–1.14) и доказываются основные утверждения о свойствах разметок, необходимые для дальнейшего исследования свойств классов блочных преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$ (теоремы 1.6 и 1.7). В заключение §1.3, с использованием аппарата разметок доказывается однозначность состава произведения элементарных и перестановочной сетей, описывающего некоторое семейство преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$ (теорема 1.9) и, как следствие, уточняется основная теорема о строении $\mathcal{R}$-биективной сети (следствие 1.8).

Во второй главе продолжается развитие аппарата разметок и с его помощью исследуется вопрос о транзитивности множества блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, реализуемых произвольной $\mathcal{R}$-биективной сетью Σ (далее

просто $\mathcal{R}$-транзитивность).

В §2.1 на языке разметок формулируются и доказываются необходимые и достаточные условия для $\mathcal{B}^*$-транзитивности сети (утверждение 2.2), $\mathcal{Q}$-транзитивности сети (утверждение 2.3), а также универсальный критерий $\mathcal{R}$-транзитивности сети (утверждение 2.4). Кроме того, аппарат разметок позволяет сформулировать и обосновать интересный с теоретической точки зрения способ проверки универсального критерия $\mathcal{R}$-транзитивности (теорема 2.6), который допускает эффективную практическую реализацию (теорема 2.7).

В §2.2 определяется каноническое представление произвольной $\mathcal{R}$-биективной сети (утверждение 2.9 и определение 2.5), которое фактически является естественным упорядочением представлений из теорем 1.2 и 1.5. Введенное понятие канонического представления вместе с разработанным аппаратом разметок позволяют строго описать эффективные алгоритмы построения $\mathcal{Q}$-биективных и $\mathcal{B}^*$-биективных сетей, действующих транзитивным образом для всех достаточно больших множеств (на вход алгоритма подается произвольная $\mathcal{R}$-биективная сеть в своем каноническом представлении; в ходе работы алгоритма, в зависимости от проводимой минимальной свободной $\mathcal{R}$-разметки сети Σ, в каноническое представление сети Σ добавляются подходящие элементарные сети; в результате работы выполнения алгоритма получается $\mathcal{R}$-биективная сеть $\widehat{\Sigma}$, действующая $\mathcal{R}$-транзитивным образом для всех достаточно больших множеств). Корректность данных алгоритмов строго обосновывается с использованием аппарата разметок (теорема 2.10).

В §2.3 доказывается нетривиальная нижняя оценка веса $\mathcal{R}$-транзитивной сети (теорема 2.13). Также в §2.3 определяются универсальные конструкции $\mathcal{B}^*$-биективных сетей ширины n и небольшого веса $2n-1$: Δ_n (пример 2.4) и Ψ_n (пример 2.5). С применением аппарата разметок, доказывается, что каждая из сетей Δ_n и Ψ_n при любом $n \in \mathbb{N}$ является $\mathcal{B}^*$-транзитивной для всех достаточно больших множеств, а сеть Δ_n является также $\mathcal{Q}$-транзитивной для всех достаточно больших множеств. В заключение доказывается, что рассмотренные сети Δ_n, Ψ_n, $n \in \mathbb{N}$ могут быть использованы для эффективного построения широких классов $\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитек-

туры (теорема 2.14).

Третья глава диссертации посвящена исследованию k-транзитивности множества блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ при $k \geqslant 2$.

Аппарат разметок $\mathcal{R}$-биективных сетей, введенный и разработанный в главах 1 и 2, на самом деле позволяет исследовать не только $\mathcal{R}$-транзитивность сетей, но и более сложное свойство $k\mathcal{R}$-транзитивности при $k \geqslant 2$. Однако для удобства проведения рассуждений при исследовании $k\mathcal{R}$-транзитивности $\mathcal{R}$-биективных сетей в §3.1 формулируются естественные k-мерные обобщения основных понятий аппарата разметок (определения 3.2 и 3.3) и доказываются k-мерные аналоги основных технических результатов (теоремы 3.3 и 3.4). Кроме того, в §3.1 определяются несколько различных способов построения свободной k-разметки и доказывается, что все они по существу эквивалентны между собой (теорема 3.2).

В §3.2 с использованием k-мерных инструментов аппарата разметок формулируются и доказываются критерии $k\mathcal{B}^*$-транзитивности сети (утверждение 3.6), $k\mathcal{Q}$-транзитивности сети (утверждение 3.7) и универсальный критерий $k\mathcal{R}$-транзитивности сети (утверждение 3.8). Кроме того, развитый аппарат разметок позволяет сформулировать и обосновать интересный с теоретической точки зрения способ проверки универсального критерия $\mathcal{R}$-транзитивности (теорема 3.10), который допускает эффективную практическую реализацию (теорема 3.12).

В §3.3 на языке разметок излагается и обосновывается эффективный универсальный алгоритм построения $\mathcal{R}$-биективных сетей, действующих кратно транзитивным образом для всех достаточно больших множеств (алгоритм 3 и теорема 3.14). Отметим, что предложенный в настоящей диссертации алгоритм построения $k\mathcal{R}$-транзитивной сети является «гибким» по содержанию выполняемых действий — добавляемые на промежуточных шагах элементарные сети можно выбирать различными способами (что особенно важно при использовании данного алгоритма для построения $k\mathcal{Q}$-транзитивных сетей). Другими словами, предложенный алгоритм следует рассматривать как общую схему, на основе которой можно выстроить целое семейство алгоритмов построения

$k\mathcal{R}$-транзитивных сетей схожей архитектуры, но с различными «оттенками» внутренних элементов.

Кроме того, в §3.3 определяется серия $\mathcal{R}$-биективных сетей ∇_n, $n \in \mathbb{N}$, в которой каждая сеть ∇_n имеет ширину n и вес $4n-4$ (пример 3.1). С использованием аппарата разметок доказывается, что каждая сеть ∇_n, $n \in \mathbb{N}$ является $k\mathcal{R}$-транзитивной при любом $k \geqslant 2$ для всех достаточно больших множеств. В заключение показывается, что рассмотренные сети ∇_n, $n \in \mathbb{N}$ могут быть использованы для эффективного построения широких классов $k\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры (теорема 3.16).

В заключении диссертации приводятся основные выводы исследования.

Научная новизна. Классы блочных преобразований, определяемые фиксированной бинарной функциональной сетью и некоторым семейством бинарных операций, впервые введены автором и ранее не изучались. Вследствие этого все полученные автором теоретические результаты и практические приложения являются новыми, как по исходной теоретической постановке задач, так и по методам их решения.

Теоретическая и практическая значимость. Теоретическая значимость диссертации заключается в построении наглядной модели реализации класса блочных преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ и разработанном аппарате разметки $\mathcal{R}$-биективных сетей, которые позволяют эффективно исследовать кратную транзитивность произвольных семейств преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, а, кроме того, сравнительно просто строить разнообразные классы блочных преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, обладающие требуемой кратной транзитивностью.

С точки зрения анализа, исследуемые в работе классы блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ можно использовать для аппроксимации множества блочных преобразований, реализуемых в некоторых известных узлах защиты информации, — указанное обстоятельство определяет практическую значимость разработанного в диссертации эффективного метода проверки кратной транзитивности произвольного класса преобразований вида $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$. С точки зрения синтеза, классы блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ до-

пускают компактную и простую техническую реализацию, в большинстве своем обладают высокой аналитической сложностью и потому могут быть использованы в качестве определенных компонент узлов защиты информации — указанное обстоятельство определяет практическую значимость предложенных в работе алгоритмов построения кратно транзитивных классов преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$.

Основные методы исследования. Диссертационное исследование проводилось алгебраическими, комбинаторными и другими методами из области дискретной математики, включая использование теории графов.

Основные положения, выносимые на защиту. На защиту выносятся обоснование актуальности решаемой задачи, методология, принятая для исследования, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в Заключении.

1. Предложена формальная модель для построения просто реализуемых классов блочных преобразований, параметрически зависящих от выбора бинарной операции. В рамках данной модели разработан эффективный метод проверки кратной транзитивности полного класса блочных преобразований.

2. Сформулированы и строго обоснованы алгоритмы построения кратно транзитивных классов блочных преобразований, архитектура которых представляет собой уникальную (для класса) сеть с узлами, отвечающими одной бинарной операции.

3. Построены практически значимые кратно транзитивные классы блочных преобразований, архитектура которых представляет собой уникальную (для класса) сеть небольшой сложности с узлами, отвечающими одной бинарной операции из специальной репрезентативной выборки.

Степень достоверности. Достоверность всех полученных результатов обосновывается корректностью постановок задач и строгими математическими доказательствами теоретических утверждений.

Апробация работы. Результаты диссертационного исследования докладывались на следующих семинарах и конференциях:

1. Всероссийская конференция «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» — SIBECRYPT'17 (г. Красноярск, 4–8 сентября 2017 г.)

2. Всероссийская конференция «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» — SIBECRYPT'18 (г. Абакан, 3–8 сентября 2018 г.)

3. семинар «Компьютерная безопасность» под руководством старшего научного сотрудника А.В. Галатенко, механико-математический факультет МГУ имени М. В. Ломоносова, 2020 г.;

4. семинар «Теория автоматов» под руководством д.ф.-м.н., проф. В.Б. Кудрявцева, механико-математический факультет МГУ имени М. В. Ломоносова, 2020 г.;

5. XXII научно-практическая конференция «РусКрипто'2020», (г. Солнечногорск, 27–29 марта 2020 г.).

Публикации по теме диссертации. Основное содержание диссертации опубликовано в 6 работах [61–66], из которых [61–64] — статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в списки Scopus и/или WoS, RSCI, а [65, 66] — публикации в материалах конференций.

Глава 1. Строение биективной сети

В данной главе определяются основные понятия бинарных функциональных сетей, которые позволяют наглядно представлять классы блочных преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$.

В §1.2 доказывается критерий $\mathcal{R}$-биективности произвольной бинарной сети постоянной ширины в терминах ее матрицы смежности и для произвольной $\mathcal{R}$-биективной сети доказывается существование эквивалентного представления в виде произведения элементарных и перестановочной сетей.

В §1.3 вводится понятие разметки $\mathcal{R}$-биективной сети — инструмента, который позволяет обнаруживать особенности $\mathcal{R}$-биективной сети, нарушающие её транзитивность, а кроме того, доказываются основные утверждения о свойствах разметок, необходимые для дальнейшего исследования свойств классов блочных преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$. В заключение §1.3, с использованием аппарата разметок доказывается однозначность состава произведения элементарных и перестановочной сетей, описывающего некоторое семейство преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$ и, как следствие, уточняется основная теорема о строении $\mathcal{R}$-биективной сети.

Результаты данной главы опубликованы в [61, 63, 65].

§1.1 Постановка задачи

Пусть Ω — произвольное конечное множество, $\mathcal{B}(\Omega)$ — множество всех бинарных операций, определенных на Ω, $\{x_1, \ldots, x_n\}$ — множество переменных и $*$ — общий символ бинарной операции. Произвольная формула $w(x_1, \ldots, x_n)$ в алфавите $\{x_1, \ldots, x_n, *\}$ при сопоставлении символу $*$ конкретной бинарной операции $F \in \mathcal{B}(\Omega)$ реализует функцию $w^F \colon \Omega^n \to \Omega$, а набор формул $(w_1, \ldots, w_m)$ реализует отображение $(w_1^F, \ldots, w_m^F) \colon \Omega^n \to \Omega^m$.

Определение 1.1. Пусть $(v_1, \ldots, v_k)$, $(w_1, \ldots, w_m)$ — наборы формул и в наборе $(w_1, \ldots, w_m)$ каждая из формул w_j, $j \in \{1, \ldots, m\}$, либо имеет вид $v_{i_1} * v_{i_2}$ при $i_1 \neq i_2$, $i_1, i_2 \in \{1, \ldots, k\}$, либо является некоторой формулой v_i, $i \in \{1, \ldots, k\}$.

Тогда будем говорить, что набор формул $(w_1, \ldots, w_m)$ является *результатом преобразования* набора формул $(v_1, \ldots, v_k)$.

Один из способов построения произвольного набора формул $(w_1, \ldots, w_m)$ состоит в последовательном преобразовании набора переменных $(x_1, \ldots, x_n)$. Для исследования свойств отображений вида $(w_1^F, \ldots, w_m^F)$ введём дополнительное представление процесса преобразований набора формул в виде сети, которое отличается большей наглядностью.

Определение 1.2. Пусть $t, n_0, n_1, \ldots, n_t \in \mathbb{N}$ и

$$X_0 = \{x_1^{(0)}, \ldots, x_{n_0}^{(0)}\},\ X_1 = \{x_1^{(1)}, \ldots, x_{n_1}^{(1)}\},\ \ldots\ ,\ X_t = \{x_1^{(t)}, \ldots, x_{n_t}^{(t)}\}$$

— семейство попарно непересекающихся конечных непустых множеств. Тогда *бинарной сетью (далее просто сетью) длины* t будем называть простой ориентированный граф Σ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$, содержащий только рёбра вида $(x_i^{(s-1)}, x_j^{(s)})$, с тем ограничением, что степень захода каждой вершины $x_j^{(s)}$, $j \in \{1, \ldots, n\}$, $s \in \{1, \ldots, t\}$ равна 1 или 2. При этом если степень захода вершины $x_j^{(s)}$ равна 2, то рёбра $(x_{i_1}^{(s-1)}, x_j^{(s)})$ и $(x_{i_2}^{(s-1)}, x_j^{(s)})$ имеют различные метки из множества $\{l, r\}$.

Подграф Σ_s сети Σ, основанный на множестве вершин $X_{s-1} \cup X_s$, будем называть *s-м слоем* сети Σ.

Сеть Σ называется *однослойной*, если она имеет длину 1.

Множества X_0 и X_t будем называть множествами начальных и конечных вершин соответственно.

Число $\max\{n_0, \ldots, n_t\}$ будем называть *шириной* сети Σ.

Определение 1.3. Пусть Σ и Σ' — сети с множествами вершин X и X' соответственно, при этом $X = X_0 \cup X_1 \cup \ldots \cup X_s$, $X' = X'_0 \cup X'_1 \cup \ldots \cup X'_t$ и $X_s = X'_0 = X \cap X'$. Тогда естественным образом можно определить сеть длины $s + t$ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_s \cup X'_1 \cup \ldots \cup X'_t$, которую будем называть *произведением* сетей Σ и Σ' и обозначать $\Sigma \cdot \Sigma'$.

Непосредственно из определения 1.2 следует, что произвольная сеть Σ длины t является произведением однослойных сетей: $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$.

Определение 1.4. Пусть $(v_1, \ldots, v_n)$ — произвольный набор формул и Σ — однослойная сеть с множеством вершин $\{x_1^0, \ldots, x_n^{(0)}\} \cup \{x_1^{(1)}, \ldots, x_m^{(1)}\}$. Тогда определим набор формул $(w_1, \ldots, w_m)$, соответствующий данной сети Σ, по следующим правилам:

- если вершине $x_j^{(1)}$ инцидентно единственное ребро $(x_i^{(0)}, x_j^{(1)})$, то полагаем $w_j = v_i$;
- если вершине $x_j^{(1)}$ инцидентны рёбра $(x_{i_1}^{(0)}, x_j^{(1)})$ и $(x_{i_2}^{(0)}, x_j^{(1)})$ с метками l и r соответственно, то полагаем $w_j = v_{i_1} * v_{i_2}$.

При этом будем говорить, что однослойная сеть Σ *описывает преобразование* набора формул $(v_1, \ldots, v_n)$ в набор формул $(w_1, \ldots, w_m)$. Произвольная сеть Σ является произведением своих слоев — однослойных сетей и потому естественным образом описывает последовательность преобразований набора формул.

Пример 1.1. Преобразование набора переменных $(x_1, x_2, x_3, x_4, x_5, x_6)$ в набор формул $((x_1 * x_3) * x_1, x_1 * x_3, x_2 * x_1, (x_4 * x_6) * x_6, (x_4 * x_6) * x_1, x_2 * (x_5 * x_2))$ может быть описано, например, сетью, изображенной на рисунке 1.

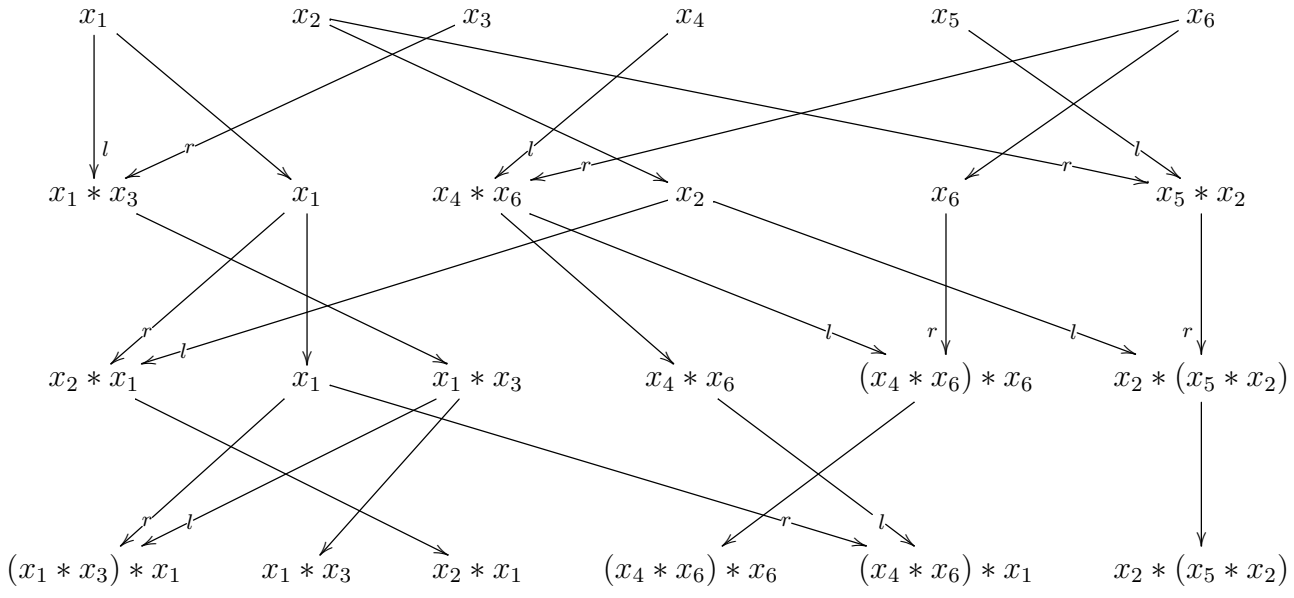

Рис. 1

Пусть $F \in \mathcal{B}(\Omega)$ — произвольная бинарная операция и сеть Σ описывает последовательность преобразований набора переменных $(x_1, \ldots, x_n)$ в набор

формул $(w_1, \ldots, w_m)$. Тогда отображение $(w_1^F, \ldots, w_m^F)\colon \Omega^n \to \Omega^m$ будем кратко обозначать Σ^F.

Нетрудно понять, что для $\Sigma = \Sigma_1 \cdot \Sigma_2$ при выборе произвольной $F \in \mathcal{B}(\Omega)$ справедливо соответствующее равенство отображений $\Sigma^F = \Sigma_1^F \cdot \Sigma_2^F$.

Определение 1.5. Будем говорить, что сети Σ и Σ' *эквивалентны для множества* Ω, если при выборе любой бинарной операции $F \in \mathcal{B}(\Omega)$ отображения Σ^F и Σ'^F совпадают. Будем говорить, что сети Σ и Σ' *эквивалентны*, если они эквивалентны для любого множества Ω.

Замечание 1.1. Если сети Σ и Σ' описывают преобразование набора переменных $(x_1, \ldots, x_n)$ в наборы формул $(w_1, \ldots, w_m)$ и $(w'_1, \ldots, w'_m)$ соответственно, то совпадение указанных наборов формул является достаточным условием для эквивалентности сетей Σ и Σ'.

Так, например, преобразование набора переменных $(x_1, x_2, x_3, x_4, x_5, x_6)$ в набор формул $((x_1 * x_3) * x_1, x_1 * x_3, x_2 * x_1, (x_4 * x_6) * x_6, (x_4 * x_6) * x_1, x_2 * (x_5 * x_2))$, рассмотренное в примере 1.1, может быть также описано сетью, изображенной на рисунке 2. Отсюда следует, что сети, изображенные на рисунках 1 и 2 эквивалентны.

Напомним, что бинарная операция $F\colon \Omega \times \Omega \to \Omega$ называется квазигруппой на множестве Ω, если уравнения вида

$$F(y, b) = c, \quad F(a, y) = c$$

однозначно разрешимы при любых $a, b, c \in \Omega$ [2]. Другими словами, квазигруппа — бинарная операция, обратимая по каждой из переменных. Семейство $\mathcal{Q}(\Omega)$ всех квазигрупп, заданных на множестве Ω, представляет собой довольно интересный с практической точки зрения класс бинарных операций [5, 8, 11, 16, 17, 19, 21–25, 28–38, 41, 42, 44–46, 50, 51, 58, 59]. В связи с этим представляется естественным начать исследование множества преобразований $\{\Sigma^F : F \in \mathcal{B}(\Omega)\}$ с подмножества преобразований $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$.

Определение 1.6. Сеть Σ будем называть $\mathcal{Q}$*-биективной для множества* Ω, если при выборе любой квазигруппы $F \in \mathcal{Q}(\Omega)$ отображение Σ^F является би-

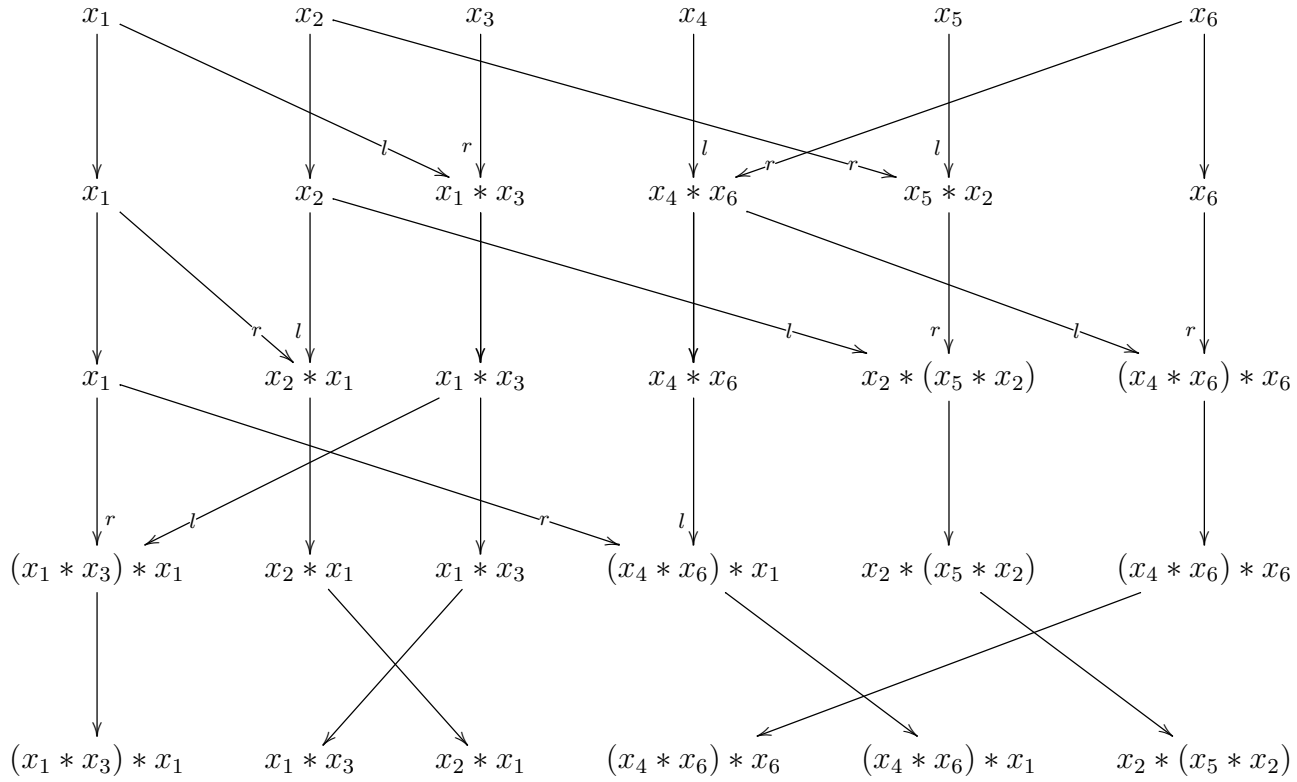

Рис. 2

ективным. Сеть Σ будем называть $\mathcal{Q}$-*биективной*, если она $\mathcal{Q}$-биективна для любого множества Ω.

Пусть Σ — сеть с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$. Вполне очевидно, что $\mathcal{Q}$-биективность сети Σ необходимо влечет равномощность множеств начальных и конечных вершин, то есть $|X_0| = |X_t|$. Кроме того, с практической точки зрения удобства реализации особый интерес представляют сети Σ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$, у которых $|X_0| = |X_1| = \ldots = |X_t|$. По этой причине всюду далее в данной работе рассматриваются только такие сети Σ, у которых $|X_0| = |X_1| = \ldots = |X_t|$.

В заключение отметим, что любая сеть $\mathcal{Q}$-биективна для произвольного одноэлементного множества Ω и, более того, в таком случае любые две сети Σ и Σ' одинаковой ширины представляют одно и то же тождественное отображение $\Omega^n \to \Omega^n$. По этой причине в дальнейшем всегда будем полагать, что $|\Omega| \geqslant 2$.

§1.2 Представление биективных сетей

Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — сеть с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$. Тогда при выборе произвольной квазигруппы $F \in \mathcal{Q}(\Omega)$ выполняется равенство $\Sigma^F = \Sigma_1^F \cdot \ldots \cdot \Sigma_t^F$. Отсюда легко видеть, что Σ — $\mathcal{Q}$-биективна для множества Ω в том и только в том случае, когда каждый слой Σ_s, $s \in \{1, \ldots, t\}$ — $\mathcal{Q}$-биективен для множества Ω. По этой причине естественно начать исследование биективных сетей с однослойных представителей.

Для однослойной сети Σ с множеством вершин

$$X_0 \cup X_1 = \{x_1^{(0)}, \ldots, x_n^{(0)}\} \cup \{x_1^{(1)}, \ldots, x_n^{(1)}\}$$

определим $(0,1)$-матрицу связности $A_\Sigma = (a_{ij})_{n \times n}$ по правилу: $a_{ij} = 1$ в случае, если сеть Σ содержит ребро $(x_i^{(0)}, x_j^{(1)})$, и $a_{ij} = 0$ в противном случае.

Напомним, что диагональю в матрице размера $n \times n$ называют всякую совокупность из n её попарно неколлинеарных элементов, при этом диагональ называется положительной, если все её элементы положительны [6, 7].

Теорема 1.1. *Однослойная сеть Σ является $\mathcal{Q}$-биективной для множества Ω тогда и только тогда, когда матрица A_Σ обладает единственной положительной диагональю.*

Доказательство. Проведём индукцию по ширине сети.

База для сети ширины 1 очевидна. В предположении, что критерий верен для любой однослойной $\mathcal{Q}$-биективной сети ширины строго меньше чем n, докажем его для произвольной однослойной $\mathcal{Q}$-биективной сети Σ ширины n.

Необходимость. По определению сети Σ каждый столбец матрицы A_Σ содержит хотя бы одну единицу. При этом если сеть Σ — $\mathcal{Q}$-биективна для множества Ω, то в матрице A_Σ найдётся хотя бы один столбец, содержащий ровно одну единицу, так как в противном случае при выборе произвольной квазигруппы $F \in \mathcal{Q}(\Omega)$ отображение Σ^F будет действовать следующим образом:

$$(a_1, a_2, \ldots, a_n) \mapsto (F(a_{i_1}, a_{j_1}), F(a_{i_2}, a_{j_2}), \ldots, F(a_{i_n}, a_{j_n})).$$

Легко видеть, что в таком случае при выборе квазигруппы $F \in \mathcal{Q}(\Omega)$ со свойством $F(a,a) = b$ для всех $a \in \Omega$ и некоторого фиксированного $b \in \Omega$ (указанным квазигруппам соответствуют латинские квадраты, у которых на главной диагонали стоит только элемент b), система

$$(F(a,a), F(a,a), \ldots, F(a,a)) = (b, b, \ldots, b)$$

будет иметь $|\Omega| \geqslant 2$ решений, и отображение Σ^F не может быть биективным — противоречие. Значит, в матрице A_Σ существует столбец, содержащий одну единицу. Не ограничивая общности, будем полагать, что это первый столбец, а единица в нём расположена на пересечении с первой строкой.

Пусть в первой строке матрицы A_Σ содержится r единиц. Не ограничивая общности, будем считать, что они стоят на первых r местах. Тогда при выборе произвольной квазигруппы $F \in \mathcal{Q}(\Omega)$ отображение Σ^F будет действовать следующим образом:

$$(a_1, \ldots, a_n) \mapsto (a_1, F^*\{a_1, a_{i_2}\}, \ldots, F^*\{a_1, a_{i_r}\}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}),$$

где $\{i_2, \ldots, i_n, j_{r+1}, \ldots, j_n\} \subseteq \{2, \ldots, n\}$, а запись $F^*\{a_i, a_j\}$ означает либо $F(a_i, a_j)$, либо $F(a_j, a_i)$, либо просто a_i. Поскольку сеть Σ является биективной для множества Ω, очевидно, что действие отображения Σ^F можно уточнить:

$$(a_1, \ldots, a_n) \mapsto (a_1, F\{a_1, a_{i_2}\}, \ldots, F\{a_1, a_{i_r}\}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}),$$

где запись $F\{a_i, a_j\}$ означает либо $F(a_i, a_j)$, либо $F(a_j, a_i)$. Биективность отображения Σ^F равносильна однозначной разрешимости при любых $b_1, \ldots, b_n \in \Omega$ системы уравнений

$$(a_1, F\{a_1, a_{i_2}\}, \ldots, F\{a_1, a_{i_r}\}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}) = (b_1, \ldots, b_n)$$

относительно $a_1, \ldots, a_n \in \Omega$. Это, в свою очередь, равносильно однозначной разрешимости при любых $b_1, b_2 \ldots, b_n \in \Omega$ следующей системы:

$$(F\{b_1, a_{i_2}\}, \ldots, F\{b_1, a_{i_r}\}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}) = (b_2, \ldots, b_n),$$

которую можно переписать в эквивалентном виде

$$\begin{gathered}(a_{i_2}, \ldots, a_{i_r}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}) = \\ = (F^{-1}\{b_1, b_2\}, \ldots, F^{-1}\{b_1, b_r\}, b_{r+1}, \ldots, b_n),\end{gathered}$$

где запись $F^{-1}\{b_1, b_j\}$ означает либо решение уравнения $F(b_1, x) = b_j$, либо решение уравнения $F(x, b_1) = b_j$. Однозначная разрешимость последней системы при любых $b_1, b_2, \ldots, b_n \in \Omega$ равносильна однозначной разрешимости системы

$$(a_{i_2}, \ldots, a_{i_r}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}) = (b'_2, \ldots, b'_r, b_{r+1}, \ldots, b_n)$$

при любых $b'_2, \ldots, b'_r, b_{r+1}, \ldots, b_n \in \Omega$.

Обозначим через Σ' подграф сети Σ, основанный на множестве вершин

$$X'_0 \cup X'_1 = \{x_2^{(0)}, \ldots, x_n^{(0)}\} \cup \{x_2^{(1)}, \ldots, x_n^{(1)}\}.$$

Легко видеть, что Σ' является однослойной сетью ширины $n-1$, и однозначная разрешимость системы

$$(a_{i_2}, \ldots, a_{i_r}, F^*\{a_{i_{r+1}}, a_{j_{r+1}}\}, \ldots, F^*\{a_{i_n}, a_{j_n}\}) = (b'_2, \ldots, b'_r, b_{r+1}, \ldots, b_n)$$

при любых $b'_2, \ldots, b'_r, b_{r+1}, \ldots, b_n \in \Omega$ на самом деле означает биективность отображения Σ'^F. Таким образом, показали, что при выборе любой квазигруппы $F \in \mathcal{Q}(\Omega)$ биективность отображения Σ^F равносильна биективности отображения Σ'^F. Другими словами, сеть Σ является $\mathcal{Q}$-биективной для множества Ω в том и только в том случае, когда сеть Σ' является $\mathcal{Q}$-биективной для множества Ω.

По предположению индукции матрица $A_{\Sigma'} = A_\Sigma \left(\begin{smallmatrix} 2 & \cdots & n \\ 2 & \cdots & n \end{smallmatrix}\right)$ содержит единственную положительную диагональ, которая однозначно продолжается до единственной положительной диагонали матрицы A_Σ.

Достаточность. Пусть матрица A_Σ имеет единственную положительную диагональ. Тогда в матрице A_Σ существует столбец, в котором содержится ровно одна единица, так как в противном случае в результате последовательного вычёркивания всех строк матрицы A_Σ, содержащих ровно одну единицу, вместе с соответствующими им столбцами останется подматрица $A_\Sigma \left(\begin{smallmatrix} i_1 & \cdots & i_l \\ j_1 & \cdots & j_l \end{smallmatrix}\right)$, $2 \leqslant l \leqslant n$, которая содержит в каждой строке не менее двух единиц и в каждом столбце ровно по две единицы. Нетрудно понять, что такая матрица $A_\Sigma \left(\begin{smallmatrix} i_1 & \cdots & i_l \\ j_1 & \cdots & j_l \end{smallmatrix}\right)$ содержит в каждой строке и в каждом столбце ровно две единицы и, следовательно, имеет не менее двух положительных диагоналей, которые продолжаются до

различных положительных диагоналей матрицы A_Σ — противоречие. Значит, в матрице A_Σ существует столбец, содержащий одну единицу, и, не ограничивая общности, можно считать, что это первый столбец, а единица в нём расположена на пересечении с первой строкой.

Пусть в первой строке матрицы A_Σ содержится r единиц. Не ограничивая общности, будем считать, что они стоят на первых r местах. Аналогично предыдущей части доказательства, нетрудно показать, что сеть Σ является $\mathcal{Q}$-биективной для множества Ω в том и только в том случае, когда сеть Σ' является $\mathcal{Q}$-биективной для множества Ω. При этом матрица $A_{\Sigma'} = A_\Sigma \left(\begin{smallmatrix} 2 & \cdots & n \\ 2 & \cdots & n \end{smallmatrix}\right)$ имеет единственную положительную диагональ, поскольку всякая положительная диагональ матрицы A_Σ содержит единственную единицу из первого столбца и является продолжением некоторой положительной диагонали матрицы $A_\Sigma \left(\begin{smallmatrix} 2 & \cdots & n \\ 2 & \cdots & n \end{smallmatrix}\right)$, и, следовательно, по предположению индукции сеть Σ' является $\mathcal{Q}$-биективной для множества Ω. □

Следствие 1.1. *Пусть Σ — $\mathcal{Q}$-биективная однослойная сеть. Тогда:*

1. *сеть Σ содержит вершины со степенью захода 1;*
2. *сеть Σ содержит вершины со степенью исхода 1.*

Доказательство. 1. Согласно доказанной теореме 1.1, матрица A_Σ имеет единственную положительную диагональ, а в доказательстве теоремы 1.1 показано, что существует столбец матрицы A_Σ, в котором содержится одна единица.

2. Согласно доказанному критерию биективности однослойной сети, в матрице A_Σ отсутствуют нулевые строки. Кроме того, невозможно, чтобы каждая строка матрицы A_Σ содержала более одной единицы, так как в этом случае каждый столбец матрицы A_Σ будет содержать ровно две единицы, а сама матрица A_Σ будет иметь не менее двух положительных диагоналей, что противоречит биективности сети Σ. □

Следствие 1.2. *Следующие утверждения являются равносильными:*

1. *сеть Σ является $\mathcal{Q}$-биективной для некоторого множества Ω, $|\Omega| \geqslant 2$;*
2. *сеть Σ является $\mathcal{Q}$-биективной.*

Доказательство. $1 \Rightarrow 2$. Если сеть Σ с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$ является $\mathcal{Q}$-биективной для некоторого множества Ω, то каждый её слой Σ_s, $s \in \{1, \ldots, t\}$, является $\mathcal{Q}$-биективным для данного множества. Из теоремы 1.1 следует, что $\mathcal{Q}$-биективность однослойных сетей Σ_s, $s \in \{1, \ldots, t\}$ для множества Ω не зависит от природы этого множества и его мощности, а зависит только от строения указанных однослойных сетей. Значит, каждый слой Σ_s, $s \in \{1, \ldots, t\}$ является $\mathcal{Q}$-биективным для всех множеств и, следовательно, сама сеть Σ является $\mathcal{Q}$-биективной для всех множеств.

$2 \Rightarrow 1$. Очевидно. □

Определение 1.7. Пусть Σ — однослойная сеть с множеством вершин $X_0 \cup X_1$. Вершину $x_j^{(0)} \in X_0$ сети Σ будем называть *неподвижной*, если Σ содержит ребро $(x_j^{(0)}, x_j^{(1)})$. Однослойную сеть Σ будем называть *элементарной*, если все вершины из множества X_0 неподвижны и ровно одна вершина из множества X_1 имеет степень захода 2.

Элементарную сеть с множеством вершин $X_0 \cup X_1$, которая содержит рёбра $(x_i^{(0)}, x_j^{(1)})$ и $(x_j^{(0)}, x_j^{(1)})$ с метками l и r соответственно, будем называть *элементарной сетью 1-го типа* и обозначать $\Sigma_j^{(i,j)}$.

Элементарную сеть с множеством вершин $X_0 \cup X_1$, которая содержит рёбра $(x_i^{(0)}, x_j^{(1)})$ и $(x_j^{(0)}, x_j^{(1)})$ с метками r и l соответственно, будем называть *элементарной сетью 2-го типа* и обозначать $\Sigma_j^{(j,i)}$.

В тех случаях, когда тип рассматриваемой элементарной сети окажется неизвестен или неинтересен, будем использовать два следующих обозначения элементарных сетей: $\Sigma_j^{(i_1,i_2)}$ и $\Sigma_j^{\{i,j\}}$

Произвольная элементарная сеть всегда является $\mathcal{Q}$-биективной. Ещё один важный пример $\mathcal{Q}$-биективных сетей представляет следующее определение.

Определение 1.8. Сеть с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$, у которой степень захода каждой вершины $x_j^{(s)}$, $s \in \{1, \ldots, t\}$ равна 1, будем называть *перестановочной*.

Произвольная перестановочная сеть определяет отображение $\Omega^n \to \Omega^n$, не зависящее от выбора бинарной операции $F \in \mathcal{B}(\Omega)$ и действующее на мно-

жестве Ω^n как перестановка координат вектора, а потому очевидно, что произвольная перестановочная сеть эквивалентна однослойной перестановочной сети.

Элементарные и перестановочные сети являются примерами простейших $\mathcal{Q}$-биективных сетей, однако, как показывает следующая теорема, этих примитивов достаточно для представления произвольной $\mathcal{Q}$-биективной сети.

Теорема 1.2. *Пусть $\mathcal{Q}$-биективная сеть Σ ширины n описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$ и содержит t вершин со степенью захода 2. Тогда существуют такие элементарные сети $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ $(\Sigma_{L1}, \ldots, \Sigma_{Lt})$ и однослойная перестановочная сеть Π_R (Π_L), что произведение*

$$\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R \quad (\Pi_L \cdot \Sigma_{L1} \cdot \ldots \cdot \Sigma_{Lt}),$$

описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$. Как следствие, сеть Σ эквивалентна данному произведению.

Доказательство. Предварительно докажем два вспомогательных утверждения.

Лемма 1.3. *Пусть Σ — произвольная $\mathcal{Q}$-биективная однослойная сеть, а Π_1, Π_2 — такие однослойные перестановочные сети, что корректно определить произведения $\Pi_1 \cdot \Sigma$ и $\Sigma \cdot \Pi_2$. Тогда справедливы следующие утверждения:*

1. *существует однослойная сеть Σ_1, которая описывает преобразование набора переменных в тот же набор формул, что и произведение $\Pi_1 \cdot \Sigma$;*

2. *существует однослойная сеть Σ_2, которая описывает преобразование набора переменных в тот же набор формул, что и произведение $\Sigma \cdot \Pi_2$;*

3. *существуют однослойная $\mathcal{Q}$-биективная сеть Σ_R, у которой все вершины неподвижны, и однослойная перестановочная сеть Π_R такие, что произведение $\Sigma_R \cdot \Pi_R$ описывает преобразование набора переменных в тот же набор формул, что и сеть Σ;*

4. *существуют однослойная $\mathcal{Q}$-биективная сеть Σ_L, у которой все вершины неподвижны, и однослойная перестановочная сеть Π_L такие, что произ-*

ведение $\Pi_L \cdot \Sigma_L$ *описывает преобразование набора переменных в тот же набор формул, что и сеть* Σ.

Доказательство. Доказательство утверждений 1 и 2 очевидно.

3. Согласно доказанному критерию $\mathcal{Q}$-биективности однослойной сети, матрица A_Σ обладает единственной ненулевой диагональю, расположенной на местах $(1, i_1), \ldots, (n, i_n)$. Пусть Π_R — однослойная перестановочная сеть, соответствующая перестановке $\left(\begin{smallmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{smallmatrix}\right)$. Тогда сеть $\Sigma \cdot \Pi_R^{-1}$ описывает преобразование формул, соответствующее некоторой однослойной сети Σ_R, у которой все вершины неподвижны и, соответственно, сети Σ и $\Sigma_R \cdot \Pi_R$ описывают одно и то же преобразование набора переменных.

4. Доказывается аналогично пункту 3. □

Лемма 1.4. *Пусть* $\mathcal{Q}$*-биективная однослойная сеть* Σ *ширины* n *содержит* $t \geqslant 1$ *вершин со степенью захода 2 и все ее вершины неподвижны. Тогда существуют такие элементарные сети* $\Sigma_1, \ldots, \Sigma_t$*, что произведение* $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ *описывает преобразование набора переменных в тот же набор формул, что и сеть* Σ.

Доказательство. Проведём индукцию по параметру t.

База при $t = 1$ очевидна — Σ является элементарной сетью ширины n. Предположим, что утверждение верно для любой однослойной $\mathcal{Q}$-биективной сети Σ ширины n при условии $t < m$. Докажем утверждение для произвольной однослойной $\mathcal{Q}$-биективной сети Σ ширины n с условием $t = m$.

По определению в точности t столбцов матрицы A_Σ содержат две единицы; не ограничивая общности, будем считать, что это первые t столбцов. Нетрудно понять, что $t < n$, так как в противном случае в $\mathcal{Q}$-биективной сети Σ отсутствуют вершины со степенью захода 1, что противоречит следствию 1.1.

Поскольку все вершины сети Σ неподвижны, то элементы матрицы A_Σ, расположенные на местах $(1, 1), \ldots, (n, n)$, очевидно, образуют положительную диагональ. При этом все $2t$ единиц, расположенных в первых t столбцах, не могут находиться на пересечении с первыми t строками, так как в противном

случае матрица $A_\Sigma \left(\begin{smallmatrix} 1 & \dots & t \\ 1 & \dots & t \end{smallmatrix}\right)$ имеет две различные положительные диагонали, которые продолжаются до различных положительных диагоналей матрицы A_Σ, что противоречит $\mathcal{Q}$-биективности сети Σ. Значит, хотя бы одна из последних $n-t$ строк матрицы A_Σ содержит не менее двух единиц; не ограничивая общности, будем считать, что это строка с номером $t+1$.

Пусть в $(t+1)$-й строке матрицы A_Σ присутствует единица на месте $s \in \{1, \dots, t\}$. Тогда обозначим через Σ' однослойную сеть, полученную из сети Σ удалением ребра $(x_{t+1}^{(0)}, x_s^{(1)})$. Очевидно, что $A_{\Sigma'} = A_\Sigma - E_{(t+1)s}$, где $E_{(t+1)s}$ — $(0,1)$-матрица, у которой единственная единица стоит на пересечении $(t+1)$-й строки и s-го столбца. Поскольку матрица A_Σ обладает единственной положительной диагональю, расположенной на местах $(1,1), \dots, (n,n)$, то матрица $A_{\Sigma'}$ также обладает единственной положительной диагональю, расположенной на местах $(1,1), \dots, (n,n)$. Последнее означает, что сеть Σ' является биективной.

Поскольку сеть Σ' содержит $t-1 < m$ вершин со степенью захода 2, то по предположению индукции существуют такие элементарные сети $\Sigma_1, \dots, \Sigma_{t-1}$, для которых произведение $\Sigma_1 \cdot \ldots \cdot \Sigma_{t-1}$ описывает такое же преобразование набора переменных, что и однослойная сеть Σ'. Остается заметить, что при выборе подходящей элементарной сети $\Sigma_s^{\{s,t+1\}}$ произведение $\Sigma' \cdot \Sigma_s^{\{s,t+1\}}$ описывает такое же преобразование набора переменных, что и сеть Σ а, следовательно, произведение t элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_{t-1} \cdot \Sigma_s^{\{s,t+1\}}$ описывает такое же преобразование набора переменных, что и однослойная сеть Σ. □

Теперь, для завершения доказательства теоремы, остаётся воспользоваться представлением сети Σ в виде произведения собственных слоёв и последовательно применить к ним доказанные леммы 1.3 и 1.4. □

Пример 1.2. В качестве примера применения доказанной теоремы 1.2 отметим, что преобразование набора переменных $(x_1, x_2, x_3, x_4, x_5, x_6)$ в набор формул $((x_1 * x_3) * x_1, x_1 * x_3, x_2 * x_1, (x_4 * x_6) * x_6, (x_4 * x_6) * x_1, x_2 * (x_5 * x_2))$, рассмотренное в примере 1.1 и замечании 1.1, может быть также описано сетью, изображенной на рисунке 3.

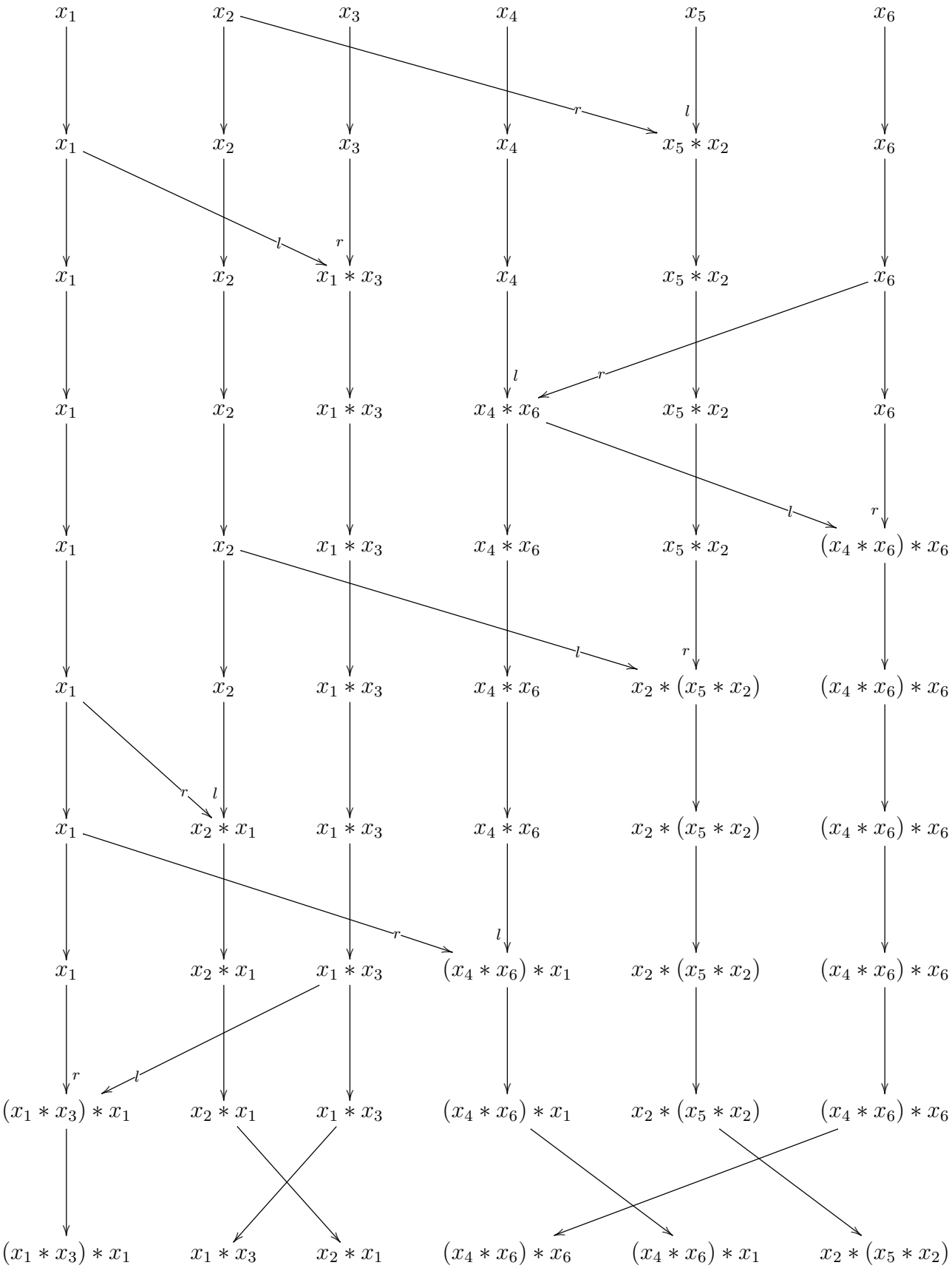
x_1 x_2 x_3 x_4 x_5 x_6
x_1 x_2 x_3 x_4 $x_5 * x_2$ x_6
x_1 x_2 $x_1 * x_3$ x_4 $x_5 * x_2$ x_6
x_1 x_2 $x_1 * x_3$ $x_4 * x_6$ $x_5 * x_2$ x_6
x_1 x_2 $x_1 * x_3$ $x_4 * x_6$ $x_5 * x_2$ $(x_4 * x_6) * x_6$
x_1 x_2 $x_1 * x_3$ $x_4 * x_6$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
x_1 $x_2 * x_1$ $x_1 * x_3$ $x_4 * x_6$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
x_1 $x_2 * x_1$ $x_1 * x_3$ $(x_4 * x_6) * x_1$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
$(x_1 * x_3) * x_1$ $x_2 * x_1$ $x_1 * x_3$ $(x_4 * x_6) * x_1$ $x_2 * (x_5 * x_2)$ $(x_4 * x_6) * x_6$
$(x_1 * x_3) * x_1$ $x_1 * x_3$ $x_2 * x_1$ $(x_4 * x_6) * x_6$ $(x_4 * x_6) * x_1$ $x_2 * (x_5 * x_2)$
l r

Рис. 3

Кроме $\mathcal{Q}(\Omega)$ можно выделить еще один практически значимый класс $\mathcal{B}^*(\Omega)$ всех бинарных операций $F \in \mathcal{B}(\Omega)$, обратимых по правой переменной, для которых уравнения вида $F(a,x) = c$ однозначно разрешимы при любых $a, c \in \Omega$. Во многих узлах переработки информации [22,25,28–36,44–46] вовсе не требуется использование квазигрупп, а достаточно бинарной операции, обратимой по одной, например правой, переменной. При этом основное преимущество класса $\mathcal{B}^*(\Omega)$ перед классом $\mathcal{Q}(\Omega)$ состоит в том, что на практике построение бинарной операции с требуемыми свойствами существенно проще выполнить в пределах класса $\mathcal{B}^*(\Omega)$, нежели в ограничениях $\mathcal{Q}(\Omega)$.

Определение 1.9. Сеть Σ будем называть *$\mathcal{B}^*$-биективной для множества* Ω, если при выборе произвольной операции $F \in \mathcal{B}^*(\Omega)$ отображение Σ^F является биективным. Сеть Σ будем называть *$\mathcal{B}^*$-биективной*, если она $\mathcal{B}^*$-биективна для любого множества Ω.

Несложно понять, что всякая $\mathcal{B}^*$-биективная сеть является также $\mathcal{Q}$-биективной, поскольку $\mathcal{Q}(\Omega) \subset \mathcal{B}^*(\Omega)$. Однако обратное утверждение неверно. Так, например, легко видеть, что любая элементарная сеть 1-го типа является $\mathcal{B}^*$-биективной, но никакая элементарная сеть 2-го типа не $\mathcal{B}^*$-биективна. Отсюда, используя результат теоремы 1.2, нетрудно получить эквивалентное представление произвольной $\mathcal{B}^*$-биективной сети.

Теорема 1.5. *Пусть $\mathcal{B}^*$-биективная сеть Σ ширины n описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$ и содержит t вершин со степенью захода 2. Тогда существуют элементарные сети 1-го типа $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ $(\Sigma_{L1}, \ldots, \Sigma_{Lt})$ и однослойная перестановочная сеть Π_R (Π_L) такие, что произведение*

$$\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R \quad (\Pi_L \cdot \Sigma_{L1} \cdot \ldots \cdot \Sigma_{Lt}),$$

описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$. Как следствие, сеть Σ эквивалентна данному произведению.

Доказательство. Не ограничивая общности, докажем существование произведения $\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R$.

Произвольная $\mathcal{B}^*$-биективная сеть Σ является также $\mathcal{Q}$-биективной, и по теореме 1.2 существуют такие элементарные сети $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ и однослойная перестановочная сеть Π_R, что произведение $\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R$ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_n)$. Однако, в таком случае произведение $\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R$ эквивалентно $\mathcal{B}^*$-биективной сети Σ и потому само является $\mathcal{B}^*$-биективной сетью. Следовательно, каждая из элементарных сетей $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ является $\mathcal{B}^*$-биективной сетью и на самом деле $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ — элементарные сети 1-го типа. □

Следствие 1.3. *Сеть Σ является $\mathcal{B}^*$-биективной тогда и только тогда, когда она является $\mathcal{B}^*$-биективной для некоторого множества Ω, $|\Omega| \geqslant 2$.*

Замечание 1.2. При выборе произвольной операции $F \in \mathcal{B}(\Omega) \backslash \mathcal{B}^*(\Omega)$ любая элементарная сеть 1-го типа реализует небиективное отображение. По этой причине рассмотрение более широкого класса функций $\mathcal{K}(\Omega) \subset \mathcal{B}(\Omega)$, удовлетворяющего условию $\mathcal{B}^*(\Omega) \subsetneq \mathcal{K}(\Omega)$, представляется несодержательным — $\mathcal{K}$-биективными сетями являются лишь перестановочные сети.

Отметим также, что можно рассматривать класс ${}^*\mathcal{B}(\Omega)$ всех бинарных операций на Ω, биективных по левой переменной. При этом описание структурного строения ${}^*\mathcal{B}$-биективных сетей повторяет соответствующее описание строения $\mathcal{B}^*$-биективных сетей с той разницей, что элементарные сети могут быть только 2-го типа.

С учетом сделанного замечания 1.2, всюду далее в данной работе мы будем рассматривать только классы функций $\mathcal{Q}(\Omega)$ и $\mathcal{B}^*(\Omega)$. При определении универсальных понятий и формулировке утверждений, справедливых для обоих классов $\mathcal{Q}(\Omega)$ и $\mathcal{B}^*(\Omega)$, мы будем использовать универсальное обозначение $\mathcal{R}(\Omega)$ подразумевая, что $\mathcal{R}(\Omega) = \mathcal{Q}(\Omega)$ или $\mathcal{R}(\Omega) = \mathcal{B}^*(\Omega)$.

§1.3 Разметка биективных сетей

В данном параграфе вводится понятие разметки сети — инструмента, который позволяет обнаруживать особенности биективной сети, нарушающие её транзитивность.

Учитывая результаты теорем 1.2 и 1.5, всюду далее в этом параграфе будем считать, что произвольная $\mathcal{Q}$-биективная ($\mathcal{B}^*$-биективная) сеть Σ представляет собой произведение $\Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ элементарных сетей (1-го типа) $\Sigma_1, \ldots, \Sigma_t$ и перестановочной сети Π с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t \cup X_{t+1}$ (кратко будем писать $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$). Также, не ограничивая общности, будем считать, что $\Omega \subset \mathbb{N}$.

Частично определённое отображение $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ иногда удобно представлять как тернарное отношение $F \subset \mathbb{N}^3$, обладающее функциональным свойством:

$$((x, y, z), (x, y, z') \in F) \Longrightarrow (z = z')\,. \tag{1.1}$$

Мы осознанно обозначаем отношение тем же символом, что и отображение, потому как между ними нет принципиальной разницы, а из контекста всегда ясно, о каком представлении идет речь.

Определение 1.10. Частично определённое отображение $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, удовлетворяющее условию

$$(F(y_1, y_2) = F(y_1', y_2')) \Longrightarrow ((y_1 = y_1', y_2 = y_2') \text{ или } (y_1 \neq y_1', y_2 \neq y_2'))$$

при всех допустимых $y_1, y_1', y_2, y_2' \in \mathbb{N}$, будем называть *частично определённым отображением без противоречий* или, кратко, *частично определенным $\mathcal{Q}$-отображением.*

Частично определённое отображение $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, удовлетворяющее условию

$$(F(y_1, y_2) = F(y_1, y_2')) \Longrightarrow (y_2 = y_2')$$

при всех допустимых $y_1, y_2, y_2' \in \mathbb{N}$, будем называть *частично определённым отображением обратимым по правой переменной* или, кратко, *частично определенным $\mathcal{B}^*$-отображением.*

Определение 1.11. *Разметкой* сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ будем называть произвольное частичное отображение $\mu\colon X_0 \cup X_1 \cup \ldots \cup X_t \cup X_{t+1} \to \mathbb{N}$, удовлетворяющее следующему условию: если в вершину $x_j^{(s)}$ заходит единственное ребро $(x_i^{(s-1)}, x_j^{(s)})$ и определены оба значения $\mu(x_i^{(s-1)})$, $\mu(x_j^{(s)})$, то необходимо $\mu(x_i^{(s-1)}) = \mu(x_j^{(s)})$.

Разметку, которая определена на всем множестве вершин $X_0 \cup \ldots \cup X_{t+1}$, будем называть *полной*.

С произвольной разметкой μ сети Σ можно связать отношение $F \subset \mathbb{N}^3$, определённое следующим образом: отношение F содержит тройку (y_l, y_r, y_q) в том и только в том случае, когда для некоторого $s \in \{1, \ldots, t\}$ выполняется равенства

$$\Sigma_s = \Sigma_j^{(i_1,i_2)} \quad \text{и} \quad (\mu(x_{i_1}^{(s-1)}), \mu(x_{i_2}^{(s-1)}), \mu(x_j^{(s)})) = (y_l, y_r, y_q).$$

Полную разметку μ будем называть *правильной*, если связанное с ней отношение $F \subset \mathbb{N}^3$ обладает функциональным свойством (1.1). При этом соответствующее частичное отображение $F\colon \mathbb{N}^2 \to \mathbb{N}$ будем называть *минимальным правилом* разметки μ.

Правильную разметку μ будем называть $\mathcal{Q}$*-разметкой* ($\mathcal{B}^*$*-разметкой*), если её минимальное правило является $\mathcal{Q}$-отображением ($\mathcal{B}^*$-отображением).

Определение 1.12. Если для разметки μ сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ выполняется система равенств $\{\mu(x_{i_j}^{(s_j)}) = v_j : j \in J\}$, то будем говорить, что μ — *разметка сети* Σ *с условиями* $\{\mu(x_{i_j}^{(s_j)}) = v_j : j \in J\}$.

Разметку начальных вершин $\mu(x_1^{(0)}) = v_1, \ldots, \mu(x_n^{(0)}) = v_n$ будем называть *начальным условием* разметки μ; при этом также будем говорить, что μ — *разметка с начальным условием* $(v_1, \ldots, v_n)$.

Пусть μ — правильная разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$. Тогда произвольное продолжение ее минимального правила естественно называть *правилом* разметки μ. Действительно, если F — некоторое правило разметки μ, то для каждого $s \in \{1, \ldots, t\}$: при $\Sigma_s = \Sigma_j^{(i_1,i_2)}$ выполняются равенства

$$\mu(x_j^{(s)}) = F(\mu(x_{i_1}^{(s-1)}), \mu(x_{i_2}^{(s-1)})) \quad \text{и} \quad \mu(x_k^{(s)}) = \mu(x_k^{(s-1)}),\ k \neq j.$$

Таким образом, правильная разметка μ сети Σ однозначно определяется своим начальным условием и правилом F.

В случае, когда при некоторой разметке начальных вершин $x_1^{(0)}, \ldots, x_n^{(0)}$ сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ для полного задания правильной разметки не хватает области определения частично определённого отображения F, можно продолжить отображение F «свободным» образом и тем самым определить полную разметку с правилом F. Поясним это подробнее.

Пусть задана начальная разметка $\mu(x_1^{(0)}) = v_1, \ldots, \mu(x_n^{(0)}) = v_n$ сети Σ и $Y = \{y_1, y_2, \ldots\} \subset \mathbb{N} \backslash \{v_1, \ldots, v_n\}$ — счётное множество меток, которые не лежат в области значений F и не являются координатами каких-либо наборов из области определения F (возможно, что метки $v_1, \ldots, v_n$ также не лежат в области значений F и не являются координатами каких-либо наборов из области определения F). Продолжим разметку μ сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ следующим образом:

- последовательно для каждого $s \in \{1, \ldots, t\}$: если $\Sigma_s = \Sigma_j^{(i_1, i_2)}$, то положим $\mu(x_k^{(s)}) = \mu(x_k^{(s-1)})$ при $k \neq j$, а для разметки вершины $x_j^{(s)}$ возможны варианты:
  - если значение $F\left(\mu(x_{i_1}^{(s-1)}), \mu(x_{i_2}^{(s-1)})\right)$ определено, то пометим вершину $x_j^{(s)}$ меткой $F\left(\mu(x_{i_1}^{(s-1)}), \mu(x_{i_2}^{(s-1)})\right)$;
  - в противном случае пометим вершину $x_j^{(s)}$ ранее не использованной меткой y_s и определим $F\left(\mu(x_{i_1}^{(s-1)}), \mu(x_{i_2}^{(s-1)})\right) = y_s$;
- если перестановочная сеть Π содержит рёбра $(x_{i_k}^{(t)}, x_k^{(t+1)})$, $k \in \{1, \ldots, n\}$, то положим $\mu(x_k^{(t+1)}) = \mu(x_{i_k}^{(t)})$, $k \in \{1, \ldots, n\}$.

Описанную процедуру продолжения разметки μ и расширения области определения F будем называть *свободным продолжением начальной разметки* $\mu(x_1^{(0)}) = v_1, \ldots, \mu(x_n^{(0)}) = v_n$ *и отображения* F *относительно сети* Σ. При этом будем говорить, что разметка μ получена в результате свободного продолжения начальной разметки $\mu(x_1^{(0)}) = v_1, \ldots, \mu(x_n^{(0)}) = v_n$ и отображения F относительно сети Σ.

Замечание 1.3. При любом свободном продолжении разметки μ и частично определённого $\mathcal{Q}$-отображения ($\mathcal{B}^*$-отображения) F относительно сети Σ указанное отображение корректным образом продолжается до частично определённого $\mathcal{Q}$-отображения ($\mathcal{B}^*$-отображения) $F_{\Sigma,\mu}$, которое является правилом построенной полной разметки μ.

Пусть η и μ — разметки сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ и для частичного отображения $\sigma_\mu \colon \mathbb{N} \to \mathbb{N}$ справедливо соотношение $\sigma_\mu \circ \eta = \mu$, то есть

$$\sigma_\mu(\eta(x_i^{(s)})) = \mu(x_i^{(s)}), \quad s \in \{0, \ldots, t+1\}, \quad i \in \{1, \ldots, n\}.$$

Тогда будем обозначать это условие как $\sigma_\mu \colon \eta \to \mu$.

Определение 1.13. Правильную разметку η сети Σ с начальным условием $(v_1, \ldots, v_n)$ будем называть *свободной*, если для любой правильной разметки μ сети Σ с начальным условием $(v_1, \ldots, v_n)$ существует отображение σ_μ, удовлетворяющее условию $\sigma_\mu \colon \eta \to \mu$.

Непосредственно из определения свободной разметки следует, что, при условии существования, свободная разметка сети Σ с начальным условием $(v_1, \ldots, v_n)$ определена однозначно с точностью до обратимого переобозначения меток.

Теорема 1.6. *Пусть разметка η получена в результате свободного продолжения начальной разметки $\eta(x_1^{(0)}) = v_1, \ldots, \eta(x_n^{(0)}) = v_n$ и отображения $G \colon \varnothing \to \mathbb{N}$ относительно сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$. Тогда η — свободная разметка сети Σ с начальным условием $(v_1, \ldots, v_n)$, а $\mathcal{Q}$-отображение $G_{\Sigma,\eta}$ — её минимальное правило.*

Доказательство. Из определения процедуры свободного продолжения начальной разметки $\eta(x_1^{(0)}) = v_1, \ldots, \eta(x_n^{(0)}) = v_n$ и отображения $G \colon \varnothing \to \mathbb{N}$ относительно сети Σ непосредственно следует, что полная разметка η является правильной, а её минимальное правило $G_{\Sigma,\eta}$ удовлетворяет условию

$$(G_{\Sigma,\eta}(y_1, y_2) = G_{\Sigma,\eta}(y_1', y_2')) \Longrightarrow ((y_1, y_2) = (y_1', y_2')) \tag{1.2}$$

при всех допустимых $y_1, y_2, y_1', y_2' \in \mathbb{N}$ и, как следствие, $G_{\Sigma,\eta}$ — частично определенное $\mathcal{Q}$-отображение.

Пусть μ — произвольная правильная разметка сети Σ с теми же начальными условиями $(v_1, \ldots, v_n)$, что и разметка η. Тогда для доказательства существования отображения $\sigma_\mu \colon \eta \to \mu$ достаточно показать, что равенство меток $\eta(x_i^{(s)}) = \eta(x_j^{(r)})$ влечет за собой равенство $\mu(x_i^{(s)}) = \mu(x_j^{(r)})$.

Не ограничивая общности, будем считать, что $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Докажем утверждение индукцией по длине произведения $\Sigma_1 \cdot \ldots \cdot \Sigma_t$.

База индукции при $t = 1$ очевидна.

Пусть теперь $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_{t-1} \cdot \Sigma_t$ — сеть длины $t > 1$ и $\Sigma_t = \Sigma_k^{\{l,k\}}$. Рассмотрим все возможные варианты для пары вершин $x_i^{(s)}$ и $x_j^{(r)}$.

1. Если $s, r < t$, то истинность утверждения следует из предположения индукции.

2. Если $s = t$, $i \neq k$ и $r < t$, то выполняется равенство $\eta(x_i^{(s-1)}) = \eta(x_j^{(r)})$ — остаётся воспользоваться предположением индукции.

3. Если $s < t$, $r = t$ и $j \neq k$, то выполняется равенство $\eta(x_i^{(s)}) = \eta(x_j^{(r-1)})$ — остаётся воспользоваться предположением индукции.

4. Если $s = r = t$ и $i \neq k$, $j \neq k$, то, очевидно, выполняется равенство $\eta(x_i^{(s-1)}) = \eta(x_j^{(r-1)})$ — остаётся воспользоваться предположением индукции.

5. В случае, когда $s = t$ и $i = k$, не ограничивая общности, будем считать, что $\Sigma_t = \Sigma_i^{(l,i)}$. Из определения процедуры свободного продолжения разметки необходимо следует, что $\eta(x_i^{(s)}) \notin \{v_1, \ldots, v_n\}$, а минимальное правило разметки η удовлетворяет условию (1.2). Значит, равенство меток $\eta(x_i^{(s)}) = \eta(x_j^{(r)})$ влечёт за собой совпадение упорядоченного набора $(\eta(x_l^{(s-1)}), \eta(x_i^{(s-1)}))$ с некоторым $(\eta(x_{l'}^{(r')}), \eta(x_j^{(r')}))$, где $r' \in \{0, \ldots, r-1\}$ — наибольшее со свойством $\eta(x_j^{(r')}) \neq \eta(x_j^{(r)})$. По предположению индукции упорядоченные наборы меток $(\mu(x_l^{(s-1)}), \mu(x_i^{(s-1)}))$ и $(\mu(x_{l'}^{(r')}), \mu(x_j^{(r')}))$ также совпадают и, следовательно, $\mu(x_i^{(s)}) = \mu(x_j^{(r'+1)}) = \mu(x_j^{(r)})$.

6. Доказательство случая, когда $r = t$ и $j = k$ аналогично доказательству пункта 5.

Теорема доказана. □

Замечание 1.4. Поскольку свободная разметка сети Σ с начальным условием $(v_1, \ldots, v_n)$ определена однозначно с точностью до обратимого переобозначения меток, то, не ограничивая общности, можно считать, что произвольная свободная разметка η сети Σ является результатом свободного продолжения начальной разметки $\eta(x_1^{(0)}) = v_1, \ldots, \eta(x_n^{(0)}) = v_n$ и отображения $G\colon \varnothing \to \mathbb{N}$ относительно сети Σ.

Следующая теорема обосновывает название свободной разметки.

Теорема 1.7. *Пусть η — свободная разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$, μ — правильная разметка сети Σ, и возможно определить отображение σ_μ по правилу: $\sigma_\mu(\eta(x_i^{(0)})) = \mu(x_i^{(0)})$, $i \in \{1, \ldots, n\}$. Тогда отображение σ_μ допускает продолжение, удовлетворяющее условию $\sigma_\mu\colon \eta \to \mu$.*

Доказательство. Достаточно показать, что равенство меток $\eta(x_i^{(s)}) = \eta(x_j^{(r)})$ влечет за собой равенство $\mu(x_i^{(s)}) = \mu(x_j^{(r)})$. Данный факт устанавливается индукцией по длине сети Σ аналогично доказательству теоремы 1.6. □

Следствие 1.4. *В условиях теоремы 1.7, если G и F — минимальные правила разметок η и μ соответственно, то при всех допустимых $z_i, z_j \in \mathbb{N}$ выполняется равенство $\sigma_\mu(G(z_i, z_j)) = F(\sigma_\mu(z_i), \sigma_\mu(z_j))$.*

Среди множества всех свободных разметок сети Σ особенным образом выделяются два типа свободной разметки.

Определение 1.14. Свободную разметку Σ с начальным условием $(v, \ldots, v)$ будем называть *минимальной свободной разметкой сети* Σ и обозначать $\eta_{\min}$.

Свободную разметку сети Σ с начальным условием $(v_1, \ldots, v_n)$, где все метки $v_1, \ldots, v_n$ — различны, будем называть *максимальной свободной разметкой сети* Σ и обозначать $\eta_{\max}$.

Следствие 1.5. *Для произвольной свободной разметки η сети Σ существует отображение $\sigma_\eta\colon \eta \to \eta_{\min}$.*

Следствие 1.6. *Для произвольной свободной разметки η сети Σ существует отображение $\sigma_\eta\colon \eta_{\max} \to \eta$.*

Замечание 1.5. На множестве всех свободных разметок фиксированной сети Σ можно естественным образом ввести отношение эквивалентности $\sim$: класс $[\eta]_\sim$ содержит все свободные разметки сети Σ, которые могут быть получены из свободной разметки η с помощью обратимого переобозначения меток. При этом фактор-множество всех свободных разметок по данному отношению эквивалентности является частично упорядоченным множеством с единственными минимальным и максимальным элементами $[\eta_{\min}]_\sim$ и $[\eta_{\max}]_\sim$ соответственно.

В §1.2 доказано, что произвольная $\mathcal{R}$-биективная сеть допускает представление в виде произведения элементарных и перестановочной сетей. Однако открытыми остались вопросы об однозначности такого представления.

1. Какие элементарные сети в указанном произведении допустимо менять местами?

2. Однозначен ли состав сомножителей в произведении элементарных и перестановочной сетей, представляющем $\mathcal{R}$-биективную сеть?

Ответ на первый вопрос дает следующее очевидное утверждение.

Утверждение 1.8. *Пусть $\Sigma_{j_1}^{\{i_1,j_1\}}$ и $\Sigma_{j_2}^{\{i_2,j_2\}}$ — различные элементарные сети одной ширины. Тогда следующие утверждения равносильны:*

1. *сети $\Sigma_{j_1}^{\{i_1,j_1\}}\cdot\Sigma_{j_2}^{\{i_2,j_2\}}$ и $\Sigma_{j_2}^{\{i_2,j_2\}}\cdot\Sigma_{j_1}^{\{i_1,j_1\}}$ описывают одинаковые преобразования набора переменных;*

2. *$j_1 \neq j_2$ и $i_1 \neq j_2$, $i_2 \neq j_1$;*

3. *сети $\Sigma_{j_1}^{\{i_1,j_1\}} \cdot \Sigma_{j_2}^{\{i_2,j_2\}}$ и $\Sigma_{j_2}^{\{i_2,j_2\}} \cdot \Sigma_{j_1}^{\{i_1,j_1\}}$ — эквивалентны.*

Если для элементарных сетей $\Sigma_{j_1}^{\{i_1,j_1\}}$ и $\Sigma_{j_2}^{\{i_2,j_2\}}$ выполняются условия утверждения 1.8, то будем говорить, что для них *допустима перестановка.*

Подтвердить положительный ответ на второй вопрос позволяет разработанный в данном параграфе аппарат разметки.

Теорема 1.9. *Пусть $\mathcal{R}$-биективные сети Σ и Σ' эквивалентны и представляются в виде $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ и $\Sigma' = \Sigma'_1 \cdot \ldots \cdot \Sigma'_s \cdot \Pi'$. Тогда $\Pi = \Pi'$, а произведения элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ и $\Sigma'_1 \cdot \ldots \cdot \Sigma'_s$ имеют одинаковый состав и могут отличаться только допустимой перестановкой множителей. Как следствие, эквивалентные сети имеют одинаковую сложность.*

Доказательство. Поскольку произвольная $\mathcal{B}^*$-биективная сеть является $\mathcal{Q}$-биективной, то, не ограничивая общности, достаточно доказать утверждение для случая $\mathcal{Q}$-биективной сети. Для этого нам потребуется результат, известный как гипотеза Эванса [26], который в общем случае был независимо доказан в работах [10, 55].

Теорема 1.10 (B. Smetaniuk, 1981)**.** *Если частично определённое непротиворечивое отображение $F\colon \Omega \times \Omega \to \Omega$ определено не более чем на $|\Omega|-1$ наборах, то оно продолжается до квазигруппы на множестве Ω.*

Пусть Σ — сеть ширины n с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t \cup X_{t+1}$, η — максимальная свободная разметка сети Σ с начальным условием $(v_1, \ldots, v_n)$, которая получена в результате свободного продолжения начальной разметки $\eta(x_1^{(0)}) = v_1, \ldots, \eta(x_n^{(0)}) = v_n$ и отображения $G\colon \varnothing \to \mathbb{N}$ относительно сети Σ с использованием множества меток $\{y_1, y_2, \ldots\}$. Тогда, согласно определению свободного продолжения разметки, в свободной разметке η используется множество меток $\Omega = \{v_1, \ldots, v_n, y_1, \ldots, y_t\}$, а её минимальное правило $G_{\Sigma,\eta}\colon \Omega \times \Omega \to \Omega$ определено на t различных наборах. Далее будем считать, что разметка η сети Σ удовлетворяет условиям

$$\eta(x_1{}^{(0)}) = v_1, \ldots, \eta(x_n{}^{(0)}) = v_n, \quad \eta(x_1{}^{(t+1)}) = y_{i_1}, \ldots, \eta(x_n{}^{(t+1)}) = y_{i_n},$$

где $\{y_{i_1}, \ldots, y_{i_n}\} \subset \{y_1, \ldots, y_t\}$.

Пусть Σ' — сеть с множеством вершин $X'_0 \cup X'_1 \cup \ldots \cup X'_s \cup X'_{s+1}$ и разметка η' сети Σ' получена в результате свободного продолжения начальной разметки $\eta'(x'_1{}^{(0)}) = v_1, \ldots, \eta'(x'_n{}^{(0)}) = v_n$ и её правила $G_{\Sigma,\eta}$ относительно сети

Σ' с использованием множества меток $\{y_{t+1}, y_{t+2}, \dots\}$. Тогда, согласно определению свободного продолжения разметки, в разметке η' используются метки из множества $\Omega' = \{v_1, \dots, v_n, y_1, \dots, y_t, \dots, y_d\}$, а её минимальное правило $(G_{\Sigma,\eta})_{\Sigma',\eta'} \colon \Omega' \times \Omega' \to \Omega'$ определено на d различных наборах. Далее будем считать, что разметка η' сети Σ' удовлетворяет условиям

$$\eta'({x'_1}^{(0)}) = v_1, \dots, \eta'({x'_n}^{(0)}) = v_n, \quad \eta'({x'_1}^{(s+1)}) = y_{j_1}, \dots, \eta'({x'_n}^{(s+1)}) = y_{j_n},$$

где $\{y_{j_1}, \dots, y_{j_n}\} \subset \{y_1, \dots, y_t, \dots, y_d\}$.

Согласно гипотезе Эванса, непротиворечивое отображение $(G_{\Sigma,\eta})_{\Sigma',\eta'}$ продолжается до квазигруппы $\overline{G} \in \mathcal{Q}(\Omega')$, и для эквивалентных сетей Σ и Σ' справедливы соотношения

$$\Sigma^{\overline{G}}(v_1, \dots, v_n) = (\eta(x_1^{(t+1)}), \dots, \eta(x_n^{(t+1)})) = (y_{i_1}, \dots, y_{i_n}),$$
$$\Sigma'^{\overline{G}}(v_1, \dots, v_n) = (\eta'({x'_1}^{(s+1)}), \dots, \eta'({x'_n}^{(s+1)})) = (y_{j_1}, \dots, y_{j_n}).$$

По условию теоремы отображения $\Sigma^{\overline{G}}$ и $\Sigma'^{\overline{G}}$ совпадают и, следовательно, $(y_{i_1}, \dots, y_{i_n}) = (y_{j_1}, \dots, y_{j_n})$ — данное равенство означает, что на самом деле при свободном продолжении начальной разметки $\eta'({x'_1}^{(0)}) = v_1, \dots, \eta'({x'_n}^{(0)}) = v_n$ и её правила $G_{\Sigma,\eta}$ относительно сети Σ' дополнительные метки $y_{t+1}, \dots, y_d$ не возникают и правило $(G_{\Sigma,\eta})_{\Sigma',\eta'}$ совпадает с $G_{\Sigma,\eta}$.

Далее потребуется вспомогательное утверждение.

Лемма 1.11. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ и $\Sigma' = \Sigma'_1 \cdot \ldots \cdot \Sigma'_s$ — $\mathcal{Q}$-биективные сети ширины n, η — максимальная свободная разметка сети Σ с минимальным правилом G, а η' — разметка сети Σ' с правилом G и теми же начальными условиями, что и η. Тогда из равенства*

$$\{\eta({x_1}^{(t)}), \dots, \eta({x_n}^{(t)})\} = \{\eta'({x'_1}^{(s)}), \dots, \eta'({x'_n}^{(s)})\}$$

следует, что $t = s$, а произведения элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ и $\Sigma'_1 \cdot \ldots \cdot \Sigma'_s$ отличаются лишь допустимой перестановкой множителей.

Доказательство. Докажем утверждение индукцией по t.

База при $t = 1$ очевидна.

Пусть теперь $t > 1$. Не ограничивая общности, будем считать, что максимальная свободная разметка η сети Σ получена в результате свободного продолжения начальной разметки $\eta(x_1^{(0)}) = y_{-1}, \ldots, \eta(x_n^{(0)}) = y_{-n}$ относительно сети Σ с использованием множества меток $\{y_1, y_2, \ldots\}$. Согласно определению свободного продолжения разметки, минимальное правило G свободной разметки η удовлетворяет условию

$$(G(y_i, y_j) = G(y_d, y_m)) \Longrightarrow ((y_i, y_j) = (y_d, y_m)) \tag{1.3}$$

при всех допустимых $y_i, y_j, y_d, y_m \in \{y_{-n}, \ldots, y_{-1}, y_1, \ldots, y_t\}$; при этом если выполняется равенство $G(y_i, y_j) = y_m$, то $m > \max\{i, j\}$.

Используя указанные свойства отображения G, индукцией по длине сети Σ' можно показать (аналогично доказательству теоремы 1.6), что для разметки η' сети Σ' с правилом G выполняется свойство

$$\left(\eta'(x_i'^{(d)}) = \eta'(x_j'^{(m)})\right) \Longrightarrow (i = j)\,. \tag{1.4}$$

Не ограничивая общности, будем считать, что $\Sigma_t = \Sigma_1^{(1,2)}$ и, соответственно, выполняются равенства

$$y_t = \eta(x_1^{(t)}) = G(\eta(x_1^{(t-1)}), \quad \eta(x_2^{(t-1)})) = G(y_l, y_r).$$

Из условия леммы следует, что $y_t = \eta(x_1^{(t)}) = \eta'(x_{i_1}'^{(s)})$ и $y_r = \eta(x_2^{(t)}) = \eta'(x_{i_2}'^{(s)})$. Кроме того, согласно (1.4), метку y_t могут иметь только вершины из множества $\{x_{i_1}'^{(1)}, \ldots, x_{i_1}'^{(s)}\}$, а метку y_r — только вершины из множества $\{x_{i_2}'^{(0)}, \ldots, x_{i_2}'^{(s)}\}$. Выберем наименьшее $l \in \{1, \ldots, s\}$ со свойством $\eta'(x_{i_1}'^{(l)}) = y_t$. Тогда все вершины $x_{i_1}'^{(l)}, \ldots, x_{i_1}'^{(s-1)}$ сети Σ' имеют степень исхода 1, и одинаковую метку $\eta'(x_{i_1}'^{(l)}) = \ldots = \eta'(x_{i_1}'^{(s)}) = y_t$, которая не содержится в области определения правила G. Кроме того, согласно (1.3) в правильной разметке η' из равенства

$$G(\eta(x_{i_1}'^{(l-1)}), \eta(x_{i_2}'^{(l-1)})) = \eta'(x_{i_1}'^{(l)}) = y_t = G(y_l, y_r).$$

следует, что $\eta(x_{i_2}'^{(l-1)}) = y_r = \eta(x_{i_2}'^{(s)})$ — данное равенство означает, что все вершины $x_{i_2}'^{(l)}, \ldots, x_{i_2}'^{(s)}$ имеют степень захода 1.

Таким образом, согласно утверждению 1.8, произведение $\Sigma'_1 \cdot \ldots \cdot \Sigma'_s$ эквивалентно произведению $\Sigma'_1 \cdot \ldots \cdot \Sigma'_{l-1} \cdot \Sigma'_{l+1} \cdot \ldots \cdot \Sigma'_s \cdot \Sigma'_l$, и легко видеть, что для сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_{t-1}$ и $\Sigma'_1 \cdot \ldots \cdot \Sigma'_{l-1} \cdot \Sigma'_{l+1} \cdot \ldots \cdot \Sigma'_s$ выполняется предположение индукции: разметка η является максимальной свободной разметкой сети $\Sigma_1 \cdot \ldots \cdot \Sigma_{t-1}$, её минимальное правило также является правилом для разметки η' сети $\Sigma'_1 \cdot \ldots \cdot \Sigma'_{l-1} \cdot \Sigma'_{l+1} \cdot \ldots \cdot \Sigma'_s$ и выполняется равенство

$$\{\eta({x_1}^{(t-1)}), \ldots, \eta({x_n}^{(t-1)})\} = \{\eta'({x'_1}^{(s-1)}), \ldots, \eta'({x'_n}^{(s-1)})\}.$$

Значит, по предположению индукции $t-1 = s-1$, а произведения элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_{t-1}$ и $\Sigma'_1 \cdot \ldots \cdot \Sigma'_{l-1} \cdot \Sigma'_{l+1} \cdot \ldots \cdot \Sigma'_s$ отличаются лишь допустимой перестановкой множителей. Остается заметить, что в таком случае $\Sigma_t = \Sigma'_l$. □

Вернемся к доказательству теоремы. Из условия

$$(\eta(x_1^{(t+1)}), \ldots, \eta(x_n^{(t+1)})) = (y_{i_1}, \ldots, y_{i_n}) = (\eta'({x'_1}^{(s+1)}), \ldots, \eta'({x'_n}^{(s+1)})) \qquad (1.5)$$

следует, что $\{\eta({x_1}^{(t)}), \ldots, \eta({x_n}^{(t)})\} = \{y_{i_1}, \ldots, y_{i_n}\} = \{\eta'({x'_1}^{(s)}), \ldots, \eta'({x'_n}^{(s)})\}$, и при этом минимальное правило G максимальной свободной разметки η сети $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ с начальным условием $(v_1, \ldots, v_n)$ является правилом разметки η' сети $\Sigma'_1 \cdot \ldots \cdot \Sigma'_s$ с начальным условием $(v_1, \ldots, v_n)$. Значит, согласно доказанной леммы 1.11, произведения элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ и $\Sigma'_1 \cdot \ldots \cdot \Sigma'_s$ имеют одинаковый состав и могут отличаться лишь допустимой перестановкой множителей. Как следствие, выполняется равенство

$$(\eta({x_1}^{(t)}), \ldots, \eta({x_n}^{(t)})) = (\eta'({x'_1}^{(s)}), \ldots, \eta'({x'_n}^{(s)})).$$

Теперь, ввиду равенства (1.5), очевидно, что $\Pi = \Pi'$. □

Ранее мы отмечали и неоднократно пользовались тем, что две сети одинаковой ширины, которые описывают преобразование набора переменных в один и тот же набор формул, являются эквивалентными. Теперь можно доказать обращение данного утверждения для случая $\mathcal{R}$-биективных сетей.

Следствие 1.7. *Пусть Σ и Σ' — $\mathcal{R}$-биективные сети ширины n. Тогда следующие утверждения равносильны:*

1. *сети* Σ *и* Σ' *эквивалентны для множества* Ω, $|\Omega| \geqslant \|\Sigma\| + \|\Sigma'\| + n$;

2. *сети* Σ *и* Σ' *описывают преобразование набора переменных в один и тот же набор формул;*

3. *сети* Σ *и* Σ' *эквивалентны.*

Доказательство. $1 \Rightarrow 2$. Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ и $\Sigma' = \Sigma'_1 \cdot \ldots \cdot \Sigma'_s \cdot \Pi'$. В доказательстве теоремы 1.9 показано, что эквивалентности сетей Σ и Σ' для множества Ω, $|\Omega| \geqslant \|\Sigma\| + \|\Sigma'\| + n$, достаточно для того, чтобы гарантировать совпадение состава и отличие лишь в допустимой перестановке множителей произведений $\Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi$ и $\Sigma'_1 \cdot \ldots \cdot \Sigma'_s \cdot \Pi'$. Остается заметить, что, согласно утверждению 1.8, оба указанных произведения описывают одно и то же преобразование набора переменных.

$2 \Rightarrow 3$. Очевидно.

$3 \Rightarrow 1$. Очевидно. □

Доказанная теорема 1.9 также позволяет уточнить результаты теорем 1.2 и 1.5 об эквивалентных представлениях $\mathcal{Q}$-биективной и $\mathcal{B}^*$-биективной сетей.

Следствие 1.8. *Пусть* $\mathcal{R}$*-биективная сеть* Σ *ширины* n *описывает преобразование набора переменных* $(x_1, \ldots, x_n)$ *в набор формул* $(w_1, \ldots, w_n)$. *Тогда существуют такие элементарные сети* $\Sigma_{R1}, \ldots, \Sigma_{Rt}$ $(\Sigma_{L1}, \ldots, \Sigma_{Lt})$ *и однослойная перестановочная сеть* Π_R (Π_L), *что произведение*

$$\Sigma_{R1} \cdot \ldots \cdot \Sigma_{Rt} \cdot \Pi_R \quad (\Pi_L \cdot \Sigma_{L1} \cdot \ldots \cdot \Sigma_{Lt}),$$

описывает преобразование набора переменных $(x_1, \ldots, x_n)$ *в набор формул* $(w_1, \ldots, w_n)$. *При этом указанное произведение определено однозначно с точностью до возможной перестановки элементарных сетей, а количество элементарных сетей в данном произведении равно количеству вершин сети* Σ *со степенью захода 2.*

Количество вершин $\mathcal{R}$-биективной сети Σ со степенью захода 2 будем называть *весом сети* Σ или её *сложностью* и обозначать $\|\Sigma\|$.

Выводы по главе

Основные результаты данной главы заключаются в следующем:

1. для процесса преобразования набора формул введено наглядное представление в виде бинарной функциональной сети;
2. получен эффективно проверяемый критерий $\mathcal{R}$-биективности произвольной бинарной сети постоянной ширины в терминах ее матрицы смежности;
3. для произвольной $\mathcal{R}$-биективной сети доказано существование эквивалентного представления в виде произведения элементарных и перестановочной сетей;
4. введено понятие разметки $\mathcal{R}$-биективной сети и доказаны базовые технические утверждения о свойствах разметок;
5. с использованием аппарата разметок доказывается однозначность состава произведения элементарных и перестановочной сетей, описывающего некоторое семейство преобразований вида $\{(w_1^F, \ldots, w_m^F) : F \in \mathcal{R}(\Omega)\}$.

Глава 2. Транзитивные сети

В данной главе продолжается развитие аппарата разметок и с его помощью исследуется вопрос о транзитивности множества блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, реализуемых произвольной $\mathcal{R}$-биективной сетью Σ.

В §2.1 на языке разметок формулируются и доказываются критерии $\mathcal{B}^*$-транзитивности, $\mathcal{Q}$-транзитивности и универсальный критерий $\mathcal{R}$-транзитивности сетей. Кроме того, аппарат разметок позволяет сформулировать и обосновать эффективный с практической точки зрения способ проверки универсального критерия $\mathcal{R}$-транзитивности.

В §2.2 на языке разметок излагаются и обосновываются эффективные алгоритмы построения $\mathcal{Q}$-биективных и $\mathcal{B}^*$-биективных сетей, действующих транзитивным образом для всех достаточно больших множеств.

В §2.3 доказывается нетривиальная нижняя оценка веса $\mathcal{R}$-транзитивной сети и определяются две универсальные конструкции $\mathcal{R}$-биективных сетей Δ и Ψ, которые имеют небольшую сложность и являются $\mathcal{R}$-транзитивными для всех достаточно больших множеств. В заключение показывается, что предложенные конструкции Δ и Ψ могут быть использованы для эффективного построения широких классов $\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры.

Результаты данной главы опубликованы в [61, 63, 65].

§2.1 Транзитивность биективных сетей

Определение 2.1. $\mathcal{R}$-биективную сеть Σ будем называть *$\mathcal{R}$-транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ является транзитивным.

Нетрудно понять, что сама природа множества Ω в данном определении не играет никакой роли, и поэтому будет корректным говорить, что $\mathcal{R}$-биективная сеть Σ является $\mathcal{R}$-транзитивной для множеств мощности q. По-прежнему

будем считать, что $\Omega \subset \mathbb{N}$, а для множества $\{1, \ldots, q\}$ будем использовать обозначение Ω_q.

Поскольку отображение, реализуемое перестановочной сетью, не зависит от выбора операции $F \in \mathcal{B}(\Omega)$, представляется очевидным следующее

Утверждение 2.1. *Пусть Σ — произвольная $\mathcal{R}$-транзитивная для множества Ω сеть, Π_1, Π_2 — произвольные перестановочные сети, для которых корректно определить произведения $\Pi_1 \cdot \Sigma$ и $\Sigma \cdot \Pi_2$. Тогда сети $\Pi_1 \cdot \Sigma$ и $\Sigma \cdot \Pi_2$ также являются $\mathcal{R}$-транзитивными для множества Ω.*

Учитывая результаты теорем 1.2 и 1.5, а также утверждения 2.1 всюду далее в данной главе, не ограничивая общности, будем полагать, что произвольная $\mathcal{Q}$-биективная ($\mathcal{B}^*$-биективная) сеть Σ представляет собой произведение $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ элементарных сетей (1-го типа) с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$ (кратко будем писать $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$).

Определение 2.2. Разметку μ сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ с условиями

$$\mu(x_1^{(0)}) = v_1 \ , \ldots , \ \mu(x_n^{(0)}) = v_n, \quad \mu(x_1^{(t)}) = w_1 \ , \ldots , \ \mu(x_n^{(t)}) = w_n$$

будем называть *разметкой сети Σ с ограничениями* $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix} \right)$. При этом будем говорить, что сеть Σ *допускает* разметку μ с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix} \right)$.

Если $\mathcal{R}$-биективная сеть Σ является $\mathcal{R}$-транзитивной для некоторого множества Ω, то для любых $(v_1, \ldots, v_n), (w_1, \ldots, w_n) \in \Omega^n$ существует такая бинарная операция $F \in \mathcal{R}(\Omega)$, что $\Sigma^F(v_1, \ldots, v_n) = (w_1, \ldots, w_n)$. В таком случае операция F определяет $\mathcal{R}$-разметку сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix} \right)$. Поэтому существование $\mathcal{R}$-разметки сети Σ при произвольных ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix} \right)$ из множества Ω является необходимым условием для того, чтобы сеть Σ являлась $\mathcal{R}$-транзитивной для множества Ω. Более того, в случае $\mathcal{R}(\Omega) = \mathcal{B}^*(\Omega)$ данное условие является достаточным.

Утверждение 2.2. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{B}^*$-биективная сеть ширины n. Тогда для любого множества Ω следующие утверждения эквивалентны:*

1. *сеть Σ является $\mathcal{B}^*$-транзитивной для множества Ω;*

2. *сеть* Σ *допускает* $\mathcal{B}^*$*-разметку элементами множества* Ω *при любых ограничениях* $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ *из множества* Ω.

Доказательство. $1 \Rightarrow 2$. $\mathcal{B}^*$-транзитивность сети Σ для некоторого множества Ω означает, что для любых $(v_1, \dots, v_n), (w_1, \dots, w_n) \in \Omega^n$ существует такая операция $F \in \mathcal{B}^*(\Omega)$, что $\Sigma^F(v_1, \dots, v_n) = (w_1, \dots, w_n)$. В таком случае операция $F \in \mathcal{B}^*(\Omega)$ естественным образом определяет $\mathcal{B}^*$-разметку сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$. Другими словами, существование правильной $\mathcal{B}^*$-разметки сети Σ элементами множества Ω при произвольных ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из множества Ω является необходимым условием для того, чтобы сеть Σ была $\mathcal{B}^*$-транзитивной для множества Ω.

$2 \Rightarrow 1$. Каждой $\mathcal{B}^*$-разметке сети Σ элементами множества Ω с ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из Ω соответствует минимальное правило — частично определенное $\mathcal{B}^*$-отображение, которое является сужением некоторой операции $F \in \mathcal{B}^*(\Omega)$. Теперь нетрудно понять, что $\Sigma^F(v_1, \dots, v_n) = (w_1, \dots, w_n)$. □

В случае класса $\mathcal{Q}(\Omega)$ связь между $\mathcal{Q}$-транзитивностью сети Σ и существованием $\mathcal{Q}$-разметок со всевозможными ограничениями несколько сложнее. Как известно, не каждое частичное $\mathcal{Q}$-отображение $F\colon \Omega \times \Omega \to \Omega$ может быть продолжено до квазигруппы на множестве Ω и, в общем случае, условие существования $\mathcal{Q}$-разметок сети Σ со всеми возможными ограничениями из множества Ω^n не является достаточным для транзитивности множества $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$. Однако связь между существованием $\mathcal{Q}$-разметок сети Σ и её $\mathcal{Q}$-транзитивностью все же можно установить, добавив некоторые ограничения на размер множества Ω.

Утверждение 2.3. *Пусть* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ *—* $\mathcal{Q}$*-биективная сеть ширины* n. *Тогда для произвольного множества* Ω, *мощность которого строго больше чем* $\|\Sigma\|$, *следующие утверждения эквивалентны:*

1. *сеть* Σ *является* $\mathcal{Q}$*-транзитивной для множества* Ω;

2. *сеть* Σ *допускает* $\mathcal{Q}$*-разметку элементами множества* Ω *при любых ограничениях* $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ *из множества* Ω.

Доказательство. $1 \Rightarrow 2$. Аналогично доказательству утверждения 2.2.

$2 \Rightarrow 1$. Каждой $\mathcal{Q}$-разметке сети Σ элементами множества Ω с ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из множества Ω соответствует минимальное правило, определённое не более чем на $\|\Sigma\| \leqslant |\Omega| - 1$ наборах. Данное правило, согласно гипотезе Эванса (теорема 1.10), продолжается до некоторой квазигруппы $F \in \mathcal{Q}(\Omega)$ и при этом $\Sigma^F(v_1, \dots, v_n) = (w_1, \dots, w_n)$. □

Замечание 2.1. В общем случае утверждение 2.3 нельзя усилить, поскольку гипотеза Эванса также не допускает усиления оценки в общем случае.

Сформулированные в утверждениях 2.2 и 2.3 критерии $\mathcal{R}$-транзитивности сети Σ для множества Ω в терминах существования $\mathcal{R}$-разметок элементами множества Ω со всеми возможными ограничениями из данного множества представляются достаточно трудными для проверки. Однако при введении дополнительных ограничений на мощность множества Ω имеющиеся критерии $\mathcal{R}$-транзитивности сети можно дополнить эквивалентной формулировкой, которая, как будет показано далее, допускает эффективную проверку. В следующем утверждении приводится универсальный критерий $\mathcal{R}$-транзитивности сети в терминах наличия $\mathcal{R}$-разметок.

Утверждение 2.4. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $t + n$, следующие утверждения эквивалентны:*

1. *сеть Σ является $\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества $\mathbb{N}$ при любых ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из множества $\mathbb{N}$.*

Теперь приступим к обоснованию того, что условие 3 из формулировки утверждения 2.4 можно проверять достаточно эффективным образом.

Для практического построения $\mathcal{R}$-разметки с требуемыми ограничениями мы будем использовать процедуру $\mathcal{R}$-приведения. Во избежание путаницы опишем данную процедуру отдельным образом для случаев $\mathcal{R} = \mathcal{Q}$ и $\mathcal{R} = \mathcal{B}^*$.

Процедура $\mathcal{Q}$-приведения. Пусть η_0 — произвольная разметка $\mathcal{Q}$-биективной сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Если в отношении G_0, соответствующем разметке η_0, содержатся две тройки, отличающиеся только в одной координате, например (y_l, y_r, y_q) и $(y_l, y_r, y_{q'})$, то, заменив в разметке η_0 все метки $y_{q'}$ на y_q, получим разметку η_1, в которой используется на одну метку меньше, чем в разметке η_0. Если в отношении G_1, соответствующем разметке η_1, присутствуют две тройки, отличающиеся только в одной координате, то повторим описанные выше действия, и так далее.

Таким образом, построим последовательность разметок $\eta_0, \eta_1, \ldots$ сети Σ, в которой каждая следующая разметка использует на одну метку меньше, чем предыдущая. Указанная последовательность разметок, очевидно, оборвётся на некотором конечном шаге с номером k в том смысле, что в отношении G_k, соответствующем разметке η_k, не найдётся двух троек, отличающихся только в одной координате. Построенная разметка η_k, очевидно, будет $\mathcal{Q}$-разметкой сети Σ, а соответствующее отображение G_k — её минимальным правилом.

Описанную процедуру будем называть *$\mathcal{Q}$-приведением разметки η_0*. При этом будем говорить, что разметка η_k *получена $\mathcal{Q}$-приведением разметки η_0*.

Процедура $\mathcal{B}^*$-приведения. Пусть η_0 — произвольная разметка $\mathcal{B}^*$-биективной сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Если в отношении G_0, соответствующем разметке η_0, содержатся две тройки (y_l, y_r, y_q) и (y_l, y'_r, y_q), отличающиеся только во второй координате, то заменим в разметке η_0 все метки y'_r на y_r; аналогичным образом, если в отношении G_0 содержатся две тройки (y_l, y_r, y_q) и (y_l, y_r, y'_q), отличающиеся только в третьей координате, то заменим в разметке η_0 все метки y'_q на y_q. В обоих случаях получим разметку η_1, в которой используется на одну метку меньше, чем в разметке η_0. Если в отношении G_1, соответствующем разметке η_1, присутствуют две тройки, отличающиеся только во второй или в третьей координате, то повторим описанные выше действия, и так далее.

Таким образом, построим последовательность разметок $\eta_0, \eta_1, \ldots$ сети Σ, в которой каждая следующая разметка использует на одну метку меньше, чем предыдущая. Указанная последовательность разметок, очевидно, оборвётся на некотором конечном шаге с номером k в том смысле, что в отношении G_k, соответствующем разметке η_k, не найдётся двух троек, отличающихся только во второй или только в третьей координате. Построенная разметка η_k, очевидно, будет $\mathcal{B}^*$-разметкой сети Σ, а соответствующее отображение G_k — её минимальным правилом.

Описанную процедуру будем называть *$\mathcal{B}^*$-приведением разметки* η_0. При этом будем говорить, что разметка η_k *получена $\mathcal{B}^*$-приведением разметки* η_0.

Лемма 2.5. *Пусть μ — $\mathcal{R}$-разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$, η_0 — произвольная разметка сети Σ и существует отображение $\sigma_\mu \colon \eta_0 \to \mu$. Тогда для любой разметки η, полученной $\mathcal{R}$-приведением разметки η_0, также выполняется условие $\sigma_\mu \colon \eta \to \mu$.*

Доказательство. Пусть $\eta_0, \eta_1, \ldots, \eta_k = \eta$ — последовательность разметок сети Σ, полученная в результате последовательного $\mathcal{R}$-приведения разметки η. Для доказательства утверждения методом математической индукции достаточно показать, что для разметки η_1 также выполняется условие $\sigma_\mu \colon \eta_1 \to \mu$.

Не ограничивая общности, проведем доказательство для случая $\mathcal{R} = \mathcal{Q}$. При построении разметки η_1 в отношении G_0, соответствующем разметке η_0, выбираются две тройки, отличающиеся только в одной координате:

- если выбрана пара (y_l, y_r, y_q) и (y_l, y'_r, y_q), то $\sigma_\mu(y_r) = \sigma_\mu(y'_r)$, поскольку μ является $\mathcal{Q}$-разметкой. В таком случае при замене в разметке η_0 всех меток y'_r на y_r получается разметка η_1, для которой, очевидно, выполняется условие $\sigma_\mu \colon \eta_1 \to \mu$.

- если выбрана пара (y_l, y_r, y_q) и (y_l, y_r, y'_q), то $\sigma_\mu(y_q) = \sigma_\mu(y'_q)$, поскольку μ является $\mathcal{Q}$-разметкой. В таком случае при замене в разметке η_0 всех меток y'_q на y_q получается разметка η_1, для которой, очевидно, выполняется условие $\sigma_\mu \colon \eta_1 \to \mu$.

- если выбрана пара (y_l, y_r, y_q) и (y'_l, y_r, y_q), то $\sigma_\mu(y_l) = \sigma_\mu(y'_l)$, поскольку μ является $\mathcal{Q}$-разметкой. В таком случае при замене в разметке η_0 всех меток y'_l на y_l получается разметка η_1, для которой, очевидно, выполняется условие $\sigma_\mu\colon \eta_1 \to \mu$.

Лемма доказана. □

Следствие 2.1. *Пусть η_0 — произвольная разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Тогда $\mathcal{R}$-разметка η, полученная $\mathcal{R}$-приведением разметки η_0, определена однозначно с точностью до обратимого переобозначения меток.*

Доказательство. Пусть η и η' — две $\mathcal{R}$-разметки, полученные в результате $\mathcal{R}$-приведения разметки η_0. Тогда существуют отображения σ_η и $\sigma_{\eta'}$, удовлетворяющие условиям $\sigma_\eta\colon \eta_0 \to \eta$ и $\sigma_{\eta'}\colon \eta_0 \to \eta'$. Согласно лемме 2.5, отображения σ_η и $\sigma_{\eta'}$ также удовлетворяют условиям $\sigma_\eta\colon \eta' \to \eta$ и $\sigma_{\eta'}\colon \eta \to \eta'$, что и доказывает утверждение следствия. □

Напомним, что, согласно утверждению 2.4, необходимым и достаточным условием для $\mathcal{R}$-транзитивности сети Σ над достаточно большим множеством Ω является существование $\mathcal{R}$-разметок сети Σ при всех возможных ограничениях из $\mathbb{N}$. Следующий результат предоставляет эффективный с теоретической точки зрения способ проверки указанного условия, который в дальнейшем будет доведен до достаточно эффективной с практической точки зрения реализации.

Теорема 2.6. *Сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ допускает $\mathcal{R}$-разметки при всех возможных ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из $\mathbb{N}$ в том и только в том случае, когда сеть Σ допускает $\mathcal{R}$-разметки при всех возможных ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из Ω_2.*

Доказательство. Необходимость очевидна, докажем достаточность. Пусть

$$Y = \{y_1, y_2, \ldots\} = \mathbb{N}\backslash\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$$

и η_0 — свободная разметка сети Σ, полученная в результате свободного продолжения начальной разметки $\eta_0(x_1^{(0)}) = v_1, \ldots, \eta_0(x_n^{(0)}) = v_n$ с использованием меток множества Y. Заменив в разметке η_0 метки $\eta_0(x_1^{(t)}), \ldots, \eta_0(x_n^{(t)})$ на $w_1, \ldots, w_n$ соответственно, получим разметку η_1 сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$. Проведём процедуру $\mathcal{R}$-приведения разметки η_1 с двумя уточнениями:

- при отождествлении меток v_i и y_j будем заменять метку y_j на v_i;
- при отождествлении меток w_i и y_j будем заменять метку y_j на w_i.

Пусть η — $\mathcal{R}$-разметка сети Σ, полученная $\mathcal{R}$-приведением разметки η_1. Тогда, согласно уточнениям, все метки $\eta(x_1^{(0)})$, …, $\eta(x_n^{(0)})$, $\eta(x_1^{(t)})$, …, $\eta(x_n^{(t)})$ содержатся в множестве $\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$, но при этом в ограничениях разметки η могли появиться отождествления следующих типов:

1. $\eta(x_i^{(0)}) = v_j \neq v_i$;
2. $\eta(x_i^{(0)}) = w_j \neq v_i$;
3. $\eta(x_i^{(t)}) = v_j \neq w_i$;
4. $\eta(x_i^{(t)}) = w_j \neq w_i$.

Методом от противного покажем, что на самом деле правильная $\mathcal{R}$-разметка η будет разметкой с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$.

Рассмотрим первый случай: $\eta(x_i^{(0)}) = v_j \neq v_i$. По условию теоремы, существует $\mathcal{R}$-разметка μ с ограничениями

$$\begin{pmatrix} \delta_{v_1,v_j}+1 & \ldots & \delta_{v_n,v_j}+1 \\ \delta_{w_1,v_j}+1 & \ldots & \delta_{w_n,v_j}+1 \end{pmatrix}$$

из Ω_2 и при этом возможно определить отображение σ_μ по правилу

$$\sigma_\mu(v_i) = \delta_{v_i,v_j} + 1, \quad \sigma_\mu(w_i) = \delta_{w_i,v_j} + 1, \quad i \in \{1, \ldots, n\}.$$

В таком случае, согласно теореме 1.7, отображение σ_μ продолжается таким образом, что удовлетворяет условию $\sigma_\mu \colon \eta_0 \to \mu$ и, как следствие, $\sigma_\mu \colon \eta_1 \to \mu$. Значит, по лемме 2.5, разметка η, полученная $\mathcal{R}$-приведением разметки η_1, также удовлетворяет условию $\sigma_\mu \colon \eta \to \mu$ — получили противоречие:

$$\sigma_\mu(\eta(x_i^{(0)})) = \sigma_\mu(v_j) = 2 \neq 1 = \delta_{v_i,v_j} + 1 = \mu(x_i^{(0)}).$$

Отсутствие отождествлений остальных типов устанавливается аналогично. □

Теперь с учетом утверждения 2.4 легко вывести следующие критерии $\mathcal{R}$-транзитивности сети.

Следствие 2.2. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $t+n$, следующие утверждения эквивалентны:*

1. *сеть Σ является $\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из множества $\Omega_2 \subset \Omega$;*
4. *множество преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ действует транзитивным образом на подмножестве $\Omega_2^n \subset \Omega^n$.*

Замечание 2.2. Результат теоремы 2.6 можно усилить, воспользовавшись очевидным соображением: если сеть Σ допускает $\mathcal{R}$-разметку с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из Ω_2 и π — подстановка на множестве Ω_2, то сеть Σ допускает $\mathcal{R}$-разметку с ограничениями $\left(\begin{smallmatrix} \pi(v_1) & \ldots & \pi(v_n) \\ \pi(w_1) & \ldots & \pi(w_n) \end{smallmatrix}\right)$. Таким образом, для проверки того, что сеть Σ допускает $\mathcal{R}$-разметку при любых ограничениях из Ω_2, достаточно убедиться в существовании 2^{2n-1} $\mathcal{R}$-разметок сети Σ с ограничениями из Ω_2.

Данное усиление результата теоремы 2.6 примечательно тем, что оно не улучшаемо в общем случае. Так, например, $\mathcal{R}$-биективная сеть $\Sigma_1^{(2,1)} \cdot \Sigma_1^{(2,1)} \cdot \Sigma_2^{(1,2)}$ допускает $\mathcal{R}$-разметку при всех ограничениях $\left(\begin{smallmatrix} v_1 & v_2 \\ w_1 & w_2 \end{smallmatrix}\right)$ из Ω_2, за исключением $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right)$ и соответственно $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ (см. рис. 4).

Далее мы покажем, что существует эффективный способ доказательства отсутствия разметок с требуемыми ограничениями (теорема 2.7), однако в данном примере нетрудно проверить, что при проведении любой разметки с ограничениями $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right)$ или $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ необходимо возникает отождествление меток 1 и 2.

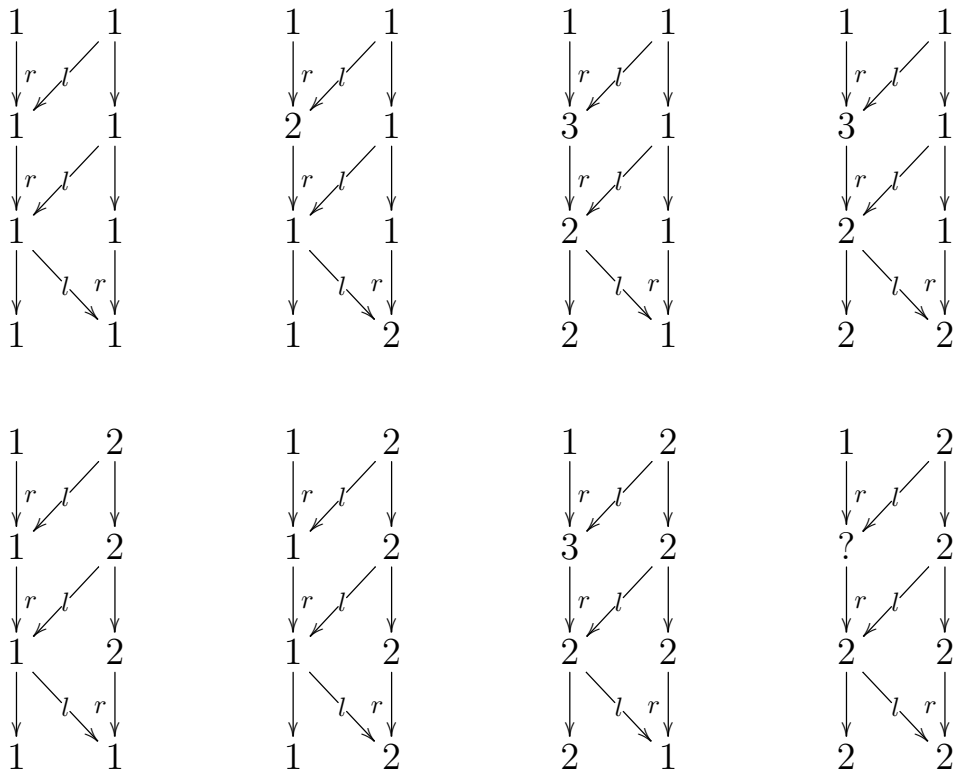

Рис. 4

Для проведения дальнейших исследований в области $\mathcal{R}$-транзитивности сетей нам потребуется следующий инструмент.

Определение 2.3. $\mathcal{R}$-разметку η сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ будем называть *свободной $\mathcal{R}$-разметкой сети Σ с ограничениями* $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$, если для любой $\mathcal{R}$-разметки μ сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ существует отображение $\sigma_\mu \colon \eta \to \mu$.

Из определения следует, что, при условии существования, свободная $\mathcal{R}$-разметка сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ определена однозначно с точностью до обратимого переобозначения меток.

С одной стороны, понятие свободной $\mathcal{R}$-разметки является достаточно естественным продолжением понятия свободной разметки, которая использовалась в качестве универсальной разметки — возможного прообраза произвольной $\mathcal{R}$-разметки. Однако, как показывают следующие примеры 2.1 и 2.2, в определении 2.3 свободной $\mathcal{R}$-разметки с ограничениями нельзя отказаться от того условия, что μ является именно $\mathcal{R}$-разметкой. Другими словами, свободная

$\mathcal{R}$-разметка с ограничениями не является «свободной» в классе всех правильных разметок с теми же ограничениями.

Пример 2.1. Рассмотрим $\mathcal{Q}$-биективную сеть $\Sigma = \Sigma_1^{(2,1)} \cdot \Sigma_1^{(1,2)} \cdot \Sigma_2^{(1,2)}$ ширины 2. Частично определенное правило F:

$$F(1,2) = 1,\ F(2,1) = 3,\ F(3,2) = 1$$

определяет правильную разметку μ сети Σ с ограничениями $\left(\begin{smallmatrix}1 & 2\\ 1 & 1\end{smallmatrix}\right)$, которая не является $\mathcal{Q}$-разметкой. При этом свободная $\mathcal{Q}$-разметка η сети Σ с теми же ограничениями $\left(\begin{smallmatrix}1 & 2\\ 1 & 1\end{smallmatrix}\right)$ определяется правилом $G:\ G(1,2) = 1,\ G(2,1) = 1$.

Пример 2.2. Рассмотрим $\mathcal{B}^*$-биективную сеть $\Sigma = \Sigma_1^{(2,1)} \cdot \Sigma_1^{(2,1)} \cdot \Sigma_3^{(2,3)}$ ширины 3. Частично определенное правило F:

$$F(1,1) = 3,\ F(1,2) = 1,\ F(1,3) = 1$$

определяет правильную разметку μ сети Σ с ограничениями $\left(\begin{smallmatrix}1 & 1 & 2\\ 1 & 1 & 1\end{smallmatrix}\right)$, которая не является $\mathcal{B}^*$-разметкой. При этом свободная $\mathcal{B}^*$-разметка η сети Σ с теми же ограничениями определяется правилом $G:\ G(1,1) = 2,\ G(1,2) = 1$.

Теорема 2.7. *Пусть $\mathcal{R}$-биективная сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ допускает $\mathcal{R}$-разметку с ограничениями $\left(\begin{smallmatrix}v_1 & \ldots & v_n\\ w_1 & \ldots & w_n\end{smallmatrix}\right)$. Тогда существует свободная $\mathcal{R}$-разметка η сети Σ с указанными ограничениями $\left(\begin{smallmatrix}v_1 & \ldots & v_n\\ w_1 & \ldots & w_n\end{smallmatrix}\right)$.*

Если для $\mathcal{R}$-разметки μ сети Σ с ограничениями $\left(\begin{smallmatrix}\bar{v}_1 & \ldots & \bar{v}_n\\ \bar{w}_1 & \ldots & \bar{w}_n\end{smallmatrix}\right)$ возможно определить отображение σ_μ по правилу: $\sigma_\mu(v_i) = \bar{v}_i$, $\sigma_\mu(w_i) = \bar{w}_i$ для всех $i \in \{1, \ldots, n\}$, то указанное отображение σ_μ допускает продолжение, удовлетворяющее условию $\sigma_\mu \colon \eta \to \mu$.

Доказательство. Для удобства дальнейшего изложения будем считать, что

$$Y = \{y_1, y_2, \ldots\} = \mathbb{N} \backslash \{v_1, \ldots, v_n, w_1, \ldots, w_n, \bar{v}_1, \ldots, \bar{v}_n, \bar{w}_1, \ldots, \bar{w}_n\}.$$

Пусть η_0 — свободная разметка сети Σ, полученная в результате свободного продолжения начальной разметки $\eta_0(x_1^{(0)}) = v_1, \ldots, \eta_0(x_n^{(0)}) = v_n$ с использованием меток множества Y. Тогда, согласно определению свободной разметки, для любой $\mathcal{R}$-разметки ϑ с ограничениями $\left(\begin{smallmatrix}v_1 & \ldots & v_n\\ w_1 & \ldots & w_n\end{smallmatrix}\right)$ существует отображение σ_ϑ, удовлетворяющее условию $\sigma_\vartheta \colon \eta_0 \to \vartheta$. Заменим в разметке η_0 метки

$\eta_0(x_1^{(t)}), \ldots, \eta_0(x_n^{(t)})$ на $w_1, \ldots, w_n$ соответственно и продолжим отображение σ_ϑ по правилу $\sigma_\vartheta(w_i) = w_i$, $i \in \{1, \ldots, n\}$. Таким образом, построили разметку η_1 сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ и показали, что для произвольной $\mathcal{R}$-разметки ϑ сети Σ с такими же ограничениями существует отображение σ_ϑ, удовлетворяющее условию $\sigma_\vartheta \colon \eta_1 \to \vartheta$. Проведём процедуру $\mathcal{R}$-приведения разметки η_1 с двумя уточнениями:

- при отождествлении меток v_i и y_j будем заменять метку y_j на v_i;
- при отождествлении меток w_i и y_j будем заменять метку y_j на w_i.

Пусть η — $\mathcal{R}$-разметка сети Σ, полученная $\mathcal{R}$-приведением разметки η_1. Тогда, согласно уточнениям, все метки $\eta(x_1^{(0)})$, $\ldots$, $\eta(x_n^{(0)})$, $\eta(x_1^{(t)})$, $\ldots$, $\eta(x_n^{(t)})$ содержатся в множестве $\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$ и при этом, по лемме 2.5, для любой $\mathcal{R}$-разметки ϑ с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ соответствующее отображение σ_ϑ удовлетворяет условию $\sigma_\vartheta \colon \eta \to \vartheta$. Значит, разметка η является свободной $\mathcal{R}$-разметкой сети Σ с указанными ограничениями.

Рассмотрим теперь $\mathcal{R}$-разметку μ с ограничениями $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$, при которых возможно определить отображение σ_μ по правилу $\sigma_\mu(v_i) = \bar{v}_i$, $\sigma_\mu(w_i) = \bar{w}_i$, $i \in \{1, \ldots, n\}$. Согласно теореме 1.7, указанное отображение σ_μ продолжается таким образом, что удовлетворяет условию $\sigma_\mu \colon \eta_0 \to \mu$. Заменив в разметке η_0 метки $\eta_0(x_1^{(t)}), \ldots, \eta_0(x_n^{(t)})$ на $w_1, \ldots, w_n$ соответственно, получим разметку η_1 сети Σ с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ и при этом выполняется условие $\sigma_\mu \colon \eta_1 \to \mu$. Согласно лемме 2.5, свободная $\mathcal{R}$-разметка η с ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$, полученная $\mathcal{R}$-приведением разметки η_1 также удовлетворяет условию $\sigma_\mu \colon \eta \to \mu$. □

Следствие 2.3. *В условиях теоремы 2.7, если G и F — минимальные правила разметок η и μ соответственно, то при всех допустимых $z_i, z_j \in \mathbb{N}$ выполняется равенство $\sigma_\mu(G(z_i, z_j)) = F(\sigma_\mu(z_i), \sigma_\mu(z_j))$.*

Теорема 2.7 позволяет дополнить ряд критериев $\mathcal{R}$-транзитивности сети Σ, перечисленных в следствии 2.2, еще одним утверждением, которое, очевидно, допускает достаточно эффективную проверку.

Следствие 2.4. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $t+n$, следующие утверждения эквивалентны:*

1. *сеть Σ является $\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из множества $\Omega_2 \subset \Omega$;*
4. *сеть Σ допускает свободную $\mathcal{R}$-разметку элементами множества $\mathbb{N}$ при любых ограничениях $\left(\begin{smallmatrix} \bar{v}_1 & \ldots & \bar{v}_n \\ \bar{w}_1 & \ldots & \bar{w}_n \end{smallmatrix}\right)$ из множества Ω_2.*

Замечание 2.3. Доказательство теоремы 2.7 конструктивно и предоставляет полиномиальный по сложности ($\mathcal{O}(t^3)$) способ построения свободной $\mathcal{R}$-разметки с требуемыми ограничениями. Таким образом, общую сложность проверки критерия из пункта 4 следствия 2.4 можно оценить величиной $\mathcal{O}(2^{2n} \cdot t^3)$.

В дальнейшем нам потребуются следующее естественное обобщение понятия свободной $\mathcal{R}$-разметки с ограничениями и соответствующие результаты.

Определение 2.4. $\mathcal{R}$-разметку η сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ будем называть *свободной $\mathcal{R}$-разметкой сети Σ с условиями*

$$\eta(x_1^{(0)}) = v_1,\ \ldots,\ \eta(x_n^{(0)}) = v_n, \quad \eta(x_{i_1}^{(t)}) = w_{i_1},\ \ldots,\ \eta(x_{i_k}^{(t)}) = w_{i_k},$$

если для любой $\mathcal{R}$-разметки μ сети Σ с аналогичными условиями

$$\mu(x_1^{(0)}) = v_1,\ \ldots,\ \mu(x_n^{(0)}) = v_n, \quad \mu(x_{i_1}^{(t)}) = w_{i_1},\ \ldots,\ \mu(x_{i_k}^{(t)}) = w_{i_k}$$

существует такое отображение σ_μ, что $\sigma_\mu \colon \eta \to \mu$.

Аналогично теореме 2.7 доказывается следующий результат.

Теорема 2.8. *Пусть сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ допускает $\mathcal{R}$-разметку ϑ с условиями*

$$\vartheta(x_1^{(0)}) = v_1,\ \ldots,\ \vartheta(x_n^{(0)}) = v_n, \quad \vartheta(x_{i_1}^{(t)}) = w_{i_1},\ \ldots,\ \vartheta(x_{i_k}^{(t)}) = w_{i_k}.$$

Тогда существует единственная, с точностью до переобозначений, свободная $\mathcal{R}$-разметка η сети Σ с аналогичными условиями:

$$\eta(x_1^{(0)}) = v_1,\ \ldots,\ \eta(x_n^{(0)}) = v_n, \quad \eta(x_{i_1}^{(t)}) = w_{i_1},\ \ldots,\ \eta(x_{i_k}^{(t)}) = w_{i_k}.$$

Если для $\mathcal{R}$-разметки μ сети Σ с условиями

$$\mu(x_1^{(0)}) = \bar{v}_1,\ \ldots,\ \mu(x_n^{(0)}) = \bar{v}_n, \quad \mu(x_{i_1}^{(t)}) = \bar{w}_{i_1},\ \ldots,\ \mu(x_{i_k}^{(t)}) = \bar{w}_{i_k}$$

возможно определить отображение σ_μ: $\sigma_\mu(v_i) = \bar{v}_i$, $\sigma_\mu(w_i) = \bar{w}_i$, $i \in \{1, \ldots, n\}$, то указанное отображение σ_μ допускает продолжение, удовлетворяющее условию $\sigma_\mu \colon \eta \to \mu$.

Следствие 2.5. *В условиях теоремы 2.8, если G и F — минимальные правила разметок η и μ соответственно, то при всех допустимых $z_i, z_j \in \mathbb{N}$ выполняется равенство $\sigma_\mu(G(z_i, z_j)) = F(\sigma_\mu(z_i), \sigma_\mu(z_j))$.*

В частности, если метка $\mu(x_j^{(s)})$ не является координатой какого-либо набора из области определения F, то метка $\eta(x_j^{(s)})$ не является координатой какого-либо набора из области определения G.

§2.2 Построение транзитивных сетей

В данном параграфе нам потребуется продолжение результатов следствия 1.8 о представлении произвольной $\mathcal{R}$-биективной сети в виде произведения элементарных и перестановочной сетей.

Утверждение 2.9. *Произвольная $\mathcal{R}$-биективная сеть Σ эквивалентна произведению*

$$\Pi_L \cdot (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}) \cdot \Pi_R,$$

в котором Π_L, Π_R — перестановочные сети, а $\Sigma_{11}, \ldots, \Sigma_{1k_1}, \ldots, \Sigma_{n1}, \ldots, \Sigma_{nk_n}$ — элементарные сети, удовлетворяющие условию: при всех $s \in \{2, \ldots, n\}$ и $r \in \{1, \ldots, k_s\}$ вершины $x_1^{(k_1+\ldots+k_{s-1}+r)}, \ldots, x_{s-1}^{(k_1+\ldots+k_{s-1}+r)}$ сети Σ_{sr} имеют степень захода 1.

Доказательство. Согласно следствию 1.8, $\mathcal{R}$-биективная сеть Σ эквивалентна произведению $\Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi_R$, где $\Sigma_1, \ldots, \Sigma_t$ — элементарные сети, а Π_R — перестановочная сеть. Пусть $i_1, \ldots, i_n$ — такая последовательность номеров от 1 до n, что при всех $s \in \{2, \ldots, n\}$ и $l \in \{1, \ldots, t\}$ для вершин сети $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ выполняется условие

$$(\deg^- x_{i_s}^{(l)} = \ldots = \deg^- x_{i_s}^{(t)} = 1) \implies (\deg^- x_{i_{s-1}}^{(l)} = \ldots = \deg^- x_{i_{s-1}}^{(t)} = 1).$$

Другими словами, $i_1, \ldots, i_n$ — порядок «окончания преобразований» вершин произведения $\Sigma_1 \cdot \ldots \cdot \Sigma_t$. Нетрудно понять, что при выборе перестановочной сети Π_L, соответствующей подстановке $\left(\begin{smallmatrix} i_1 & \ldots & i_n \\ 1 & \ldots & n \end{smallmatrix}\right)$, произведение $\Pi_L^{-1} \cdot \Sigma_1 \cdot \ldots \cdot \Sigma_t \cdot \Pi_L$ эквивалентно произведению элементарных сетей

$$(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}),$$

где $\Sigma_{11}, \ldots, \Sigma_{1k_1}, \ldots, \Sigma_{n1}, \ldots, \Sigma_{nk_n}$ — такие элементарные сети, что при всех $s \in \{2, \ldots, n\}$ и $r \in \{1, \ldots, k_s\}$ вершины $x_1^{(k_1+\ldots+k_{s-1}+r)}, \ldots, x_{s-1}^{(k_1+\ldots+k_{s-1}+r)}$ сети Σ_{sr} имеют степень захода 1.

Утверждение можно считать доказанным, поскольку исходная сеть Σ эквивалентна произведению $\Pi_L \cdot (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}) \cdot (\Pi_L^{-1} \Pi_R)$. □

Определение 2.5. Указанное в утверждении 2.9 произведение

$$\Pi_L \cdot (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}) \cdot \Pi_R$$

будем называть *каноническим представлением* $\mathcal{R}$-биективной сети Σ. При этом произведение $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$, $s \in \{1, \ldots, n\}$, будем называть *s-м слоем* канонического представления $\mathcal{R}$-биективной сети Σ. Слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ называется *вырожденным*, если $k_s = 0$.

Замечание 2.4. В каноническом представлении произвольной $\mathcal{R}$-биективной сети вырожденные слои присутствуют в том и только в том случае, когда для некоторого s все вершины $x_s^{(i)}$, $i \geqslant 0$, имеют степень захода 1. При этом, очевидно, пустыми могут быть только первые несколько подряд идущих слоев.

Не ограничивая общности, всюду далее в этом параграфе будем считать, что произвольная $\mathcal{R}$-биективная сеть Σ задается своим каноническим представлением

$$(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$$

с множеством вершин $X_0 \cup X_{11} \cup \ldots \cup X_{1k_1} \cup \ldots \cup X_{n1} \cup \ldots \cup X_{nk_n}$.

В данном параграфе предлагаются:

1. алгоритм модификации канонического представления произвольной $\mathcal{Q}$-биективной сети, в результате работы которого получается $\mathcal{Q}$-биективная сеть, действующая $\mathcal{Q}$-транзитивным образом для всех достаточно больших множеств;

2. алгоритм модификации канонического представления произвольной $\mathcal{B}^*$-биективной сети, в результате работы которого получается $\mathcal{B}^*$-биективная сеть, действующая $\mathcal{B}^*$-транзитивным образом для всех достаточно больших множеств.

Алгоритм 1. (построение $\mathcal{Q}$-транзитивной сети)
Вход: произвольная $\mathcal{Q}$-биективная сеть Σ в каноническом представлении

$$\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}) .$$

Шаг $s \in \{1, \ldots, n-1\}$**.** Пусть первые $(s-1)$ слоев канонического представления сети Σ уже модифицированы

$$\widehat{\Sigma}_{s-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}),$$

и μ — свободная $\mathcal{Q}$-разметка сети $\widehat{\Sigma}_{s-1}$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \mu(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = v.$$

Продолжим $\mathcal{Q}$-разметку μ сети $\widehat{\Sigma}_{s-1}$ свободным образом до $\mathcal{Q}$-разметки сети

$$\widehat{\Sigma}'_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s})$$

и выберем любую вершину $x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$, $j \in \{s, \ldots, n\}$, у которой метка $\mu(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)})$ не является координатой какого-либо набора из области определения $F_{\widehat{\Sigma}'_s}$ — минимального правила разметки μ сети $\widehat{\Sigma}'_s$.

Если $s \leqslant n-2$ **и** $j = s$**, то** выберем произвольные $l, m \in \{s+1, \ldots, n\}$, $l \neq m$ и модифицируем s-й слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ следующим образом:

$$\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s} = \Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s} \cdot \Sigma_l^{(s,l)} \cdot \Sigma_s^{(s,l)} \cdot \Sigma_m^{(l,m)}.$$

Если $s \leqslant n-2$ **и** $j \neq s$**, то** выберем произвольный $m \in \{s+1, \ldots, n\}$, $m \neq j$ и модифицируем s-й слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ следующим образом:

$$\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s} = \Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s} \cdot \Sigma_s^{(s,j)} \cdot \Sigma_m^{(s,m)} \cdot \Sigma_s^{(j,s)}.$$

Если $s = n-1 = j$**, то** модифицируем $(n-1)$-й слой $\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}}$ следующим образом:

$$\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}} = \Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}} \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n-1,n)} \cdot \Sigma_n^{(n,n-1)}.$$

Если $s = n-1$ **и** $j = n$**, то** модифицируем $(n-1)$-й слой $\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}}$ следующим образом:

$$\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}} = \Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \Sigma_n^{(n,n-1)} \cdot \Sigma_{n-1}^{(n-1,n)}.$$

Выход: $(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$ — «почти» каноническое представление $\mathcal{Q}$-биективной сети $\widehat{\Sigma}$, сложности не более $\|\Sigma\| + 3n - 3$.

Теорема 2.10. *Пусть* $\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$ *— произвольная* $\mathcal{Q}$*-биективная сеть ширины* n*. Тогда её модификация* $\widehat{\Sigma}$ *является* $\mathcal{Q}$*-транзитивной для произвольного множества* Ω*, мощность которого не менее чем* $\|\Sigma\| + 4n - 3$*.*

Доказательство. Всюду далее будем полагать, что каждая свободная $\mathcal{Q}$-разметка получена при свободном продолжении соответствующих начальных условий с использованием множества меток $Y = \{y_1, y_2, \ldots\}$.

Для доказательства корректности действий, выполняемых на произвольном шаге алгоритма нам потребуется следующее вспомогательное утверждение о свойстве процедуры свободного продолжения разметки.

Лемма 2.11. *Пусть* $\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$ *и* μ *— разметка сети*

$$\Sigma_{s-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)k_{s-1}})$$

с минимальным правилом $F_{\Sigma_{s-1}}$. *Тогда если среди* $x_s^{(k_1+\ldots+k_{s-1})}, \ldots, x_n^{(k_1+\ldots+k_{s-1})}$ *найдётся вершина* $x_i^{(k_1+\ldots+k_{s-1})}$, *метка которой не является координатой какого-либо набора из области определения* $F_{\Sigma_{s-1}}$, *то при свободном продолжении разметки* μ *до разметки сети*

$$\Sigma_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)k_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s})$$

среди $x_s^{(k_1+\ldots+k_s)}, \ldots, x_n^{(k_1+\ldots+k_s)}$ *найдётся вершина* $x_j^{(k_1+\ldots+k_s)}$, *метка которой не является координатой какого-либо набора из области определения* F_{Σ_s} *— минимального правила разметки* μ *сети* Σ_s.

Доказательство. Проведем индукцию по длине слоя $(\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s})$.

База при $k_s = 0$ очевидна.

Пусть теперь $k_s \geqslant 1$ и $\Sigma_{sk_s} = \Sigma_l^{\{l,r\}}$, $l \in \{s, \ldots, n\}$. Тогда по предположению индукции среди вершин $x_s^{(k_1+\ldots+k_s-1)}, \ldots, x_n^{(k_1+\ldots+k_s-1)}$ найдётся вершина $x_j^{(k_1+\ldots+k_s-1)}$, метка которой не содержится в области определения $F_{\Sigma'_s}$ — минимального правила разметки μ сети

$$\Sigma'_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)k_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s(k_s-1)}).$$

Рассмотрим два возможных случая.

Случай 1. Если одна из вершин $x_l^{(k_1+\ldots+k_s-1)}$ или $x_r^{(k_1+\ldots+k_s-1)}$ имеет метку, не содержащуюся в области определения $F_{\Sigma'_s}$, то, согласно определению процедуры свободного продолжения разметки, вершина $x_l^{(k_1+\ldots+k_s)}$ будет иметь метку, не содержащуюся в области определения F_{Σ_s}.

Случай 2. Если метки обеих вершин $x_l^{(k_1+\ldots+k_s-1)}$ и $x_r^{(k_1+\ldots+k_s-1)}$ содержатся в области определения $F_{\Sigma'_s}$, то очевидно, что метка вершины $x_j^{(k_1+\ldots+k_s-1)}$ отличается от меток вершин $x_l^{(k_1+\ldots+k_s-1)}$ и $x_r^{(k_1+\ldots+k_s-1)}$. Значит вершина $x_j^{(k_1+\ldots+k_s-1)}$ и, соответственно, вершина $x_j^{(k_1+\ldots+k_s)}$ будут иметь метку, не содержащуюся в области определения F_{Σ_s}. □

Корректность действий, выполняемых на произвольном шаге с номером $s \in \{1, \ldots, n-1\}$**.**

Пусть первые $s-1$ слоёв канонического представления сети Σ уже модифицированы таким образом, что сеть

$$\widehat{\Sigma}_{s-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}})$$

допускает свободную $\mathcal{Q}$-разметку η при любых условиях

$$\eta(x_1^{(0)}) = v_1, \ \ldots, \ \eta(x_n^{(0)}) = v_n, \quad \eta(x_1^{(\widehat{k}_1)}) = w_1, \ \ldots, \ \eta(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = w_{s-1} \quad (2.1)$$

и при этом среди $x_s^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}, \ldots, x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}$ существует вершина $x_i^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}$, метка которой $\eta(x_i^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})})$, независимо от условий (2.1), не является координатой какого-либо набора из области определения $G_{\widehat{\Sigma}_{s-1}}$ — минимального правила $\mathcal{Q}$-разметки η сети $\widehat{\Sigma}_{s-1}$. Тогда, в частности, для свободной $\mathcal{Q}$-разметки μ сети $\widehat{\Sigma}_{s-1}$ с условиями

$$\mu(x_1^{(0)}) = v, \ \ldots, \ \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ \ldots, \ \mu(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = v$$

метка $\mu(x_i^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})})$ не является координатой какого-либо набора из области определения минимального правила $F_{\widehat{\Sigma}_{s-1}}$, и при продолжении разметки μ сети $\widehat{\Sigma}_{s-1}$ свободным образом до разметки сети

$$\widehat{\Sigma}'_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}),$$

согласно лемме 2.11, среди вершин $x_s^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}, \ldots, x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$ найдётся такая вершина $x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$, $j \in \{s, \ldots, n\}$, метка которой $\mu(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)})$ не является координатой какого-либо набора из области определения $F_{\widehat{\Sigma}'_s}$ — минимального правила $\mathcal{Q}$-разметки μ сети $\widehat{\Sigma}'_s$. Значит, согласно следствию 2.5, для свободного продолжения свободной $\mathcal{Q}$-разметки η сети $\widehat{\Sigma}'_s$ с условиями (2.1) метка $\eta(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}) \in Y$, независимо от условий (2.1), не является координатой какого-либо набора из области определения $G_{\widehat{\Sigma}'_s}$ — минимального правила $\mathcal{Q}$-разметки η сети $\widehat{\Sigma}'_s$.

Если $s \leqslant n-2$**, то** в каждом из возможных вариантов модификации сети $\widehat{\Sigma}'_s$ свободная $\mathcal{Q}$-разметка η сети $\widehat{\Sigma}'_s$ с условиями (2.1) свободным образом

продолжается до свободной $\mathcal{Q}$-разметки η сети

$$\widehat{\Sigma}_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s})$$

с любым условием $\eta(x_s^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) = w_s$; при этом в каждом из подслучаев либо $\eta(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) \in Y$, либо $\eta(x_m^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) \in Y$, независимо от условия $\eta(x_s^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) = w_s$, не является координатой какого-либо набора из области определения $G_{\widehat{\Sigma}_s}$ — минимального правила $\mathcal{Q}$-разметки η сети $\widehat{\Sigma}_s$.

Если $s = n-1$**, то** в каждом из возможных вариантов модификации сети $\widehat{\Sigma}'_{n-1}$ свободная $\mathcal{Q}$-разметка η сети $\widehat{\Sigma}'_{n-1}$ с условиями (2.1) свободным образом продолжается до свободной $\mathcal{Q}$-разметки η сети

$$\widehat{\Sigma}_{n-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-2)1} \cdot \ldots \cdot \Sigma_{(n-2)\widehat{k}_{n-2}}) \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$$

с любыми условиями $\eta(x_{n-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-1})}) = w_{n-1}$ и $\eta(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-1})}) = w_n$.

Таким образом, в результате работы алгоритма каноническое представление исходной сети Σ модифицируется до «почти» канонического представления

$$(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$$

новой $\mathcal{Q}$-биективной сети $\widehat{\Sigma}$, сложность которой не более $\|\Sigma\| + 3n - 3$. Кроме того, показано, что построенная сеть $\widehat{\Sigma}$ допускает свободную $\mathcal{Q}$-разметку с произвольными ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из $\mathbb{N}$. Поскольку $\|\widehat{\Sigma}\| \leqslant \|\Sigma\| + 3n - 3$, то для проведения свободной $\mathcal{Q}$-разметки сети $\widehat{\Sigma}$ с произвольными ограничениями $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из $\mathbb{N}$ требуется не более чем $\|\Sigma\| + 4n - 3$ различных меток, а значит, при выборе любого множества Ω мощности не менее чем $\|\Sigma\| + 4n - 3$, можно считать, что сеть $\widehat{\Sigma}$ допускает свободную $\mathcal{Q}$-разметку элементами множества Ω при произвольных ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из Ω. Последнее условие, согласно утверждению 2.4, равносильно $\mathcal{Q}$-транзитивности сети $\widehat{\Sigma}$ для множества Ω. □

Следствие 2.6. *Для любого $n \geqslant 2$ существует $\mathcal{Q}$-биективная сеть $\widehat{\Sigma}$ ширины n и веса $3n-3$, которая $\mathcal{Q}$-транзитивна для всех множеств, мощность которых не менее чем $4n-3$.*

Пример 2.3. Следующая $\mathcal{Q}$-биективная сеть ширины 4

$$\Sigma_2^{(1,2)} \cdot \Sigma_1^{(1,2)} \cdot \Sigma_3^{(2,3)} \cdot \Sigma_2^{(2,3)} \cdot \Sigma_4^{(2,4)} \cdot \Sigma_2^{(3,2)} \cdot \Sigma_3^{(4,3)} \cdot \Sigma_4^{(4,3)} \cdot \Sigma_3^{(3,4)}$$

является результатом работы изложенного алгоритма применительно к пустой сети, реализующей тождественное преобразование. Указанная сеть допускает свободную $\mathcal{Q}$-разметку при любых ограничениях $\left(\begin{smallmatrix} v_1 & v_2 & v_3 & v_4 \\ w_1 & w_2 & w_3 & w_4 \end{smallmatrix}\right)$ из $\mathbb{N}$:

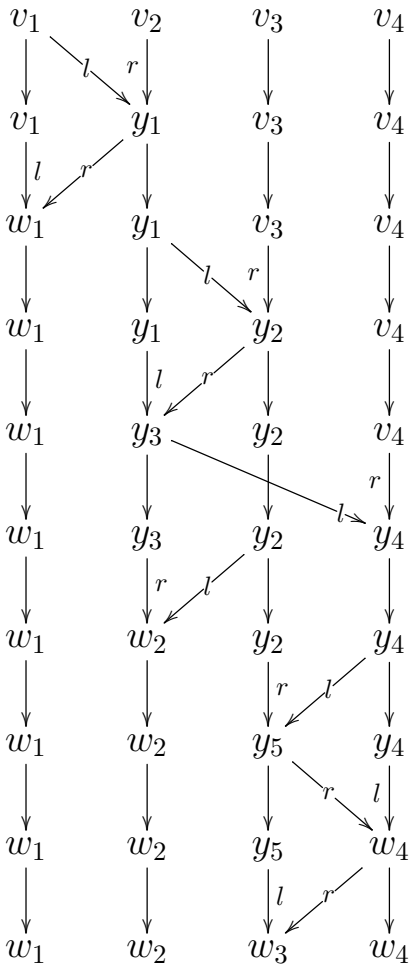

Рис. 5

Минимальное правило свободной $\mathcal{Q}$-разметки с ограничениями $\left(\begin{smallmatrix} v_1 & v_2 & v_3 & v_4 \\ w_1 & w_2 & w_3 & w_4 \end{smallmatrix}\right)$ схематично можно изобразить в виде таблицы 1. Нетрудно видеть, что при любых ограничениях $\left(\begin{smallmatrix} v_1 & v_2 & v_3 & v_4 \\ w_1 & w_2 & w_3 & w_4 \end{smallmatrix}\right)$ все внутренние метки $y_1, \ldots, y_5$ остаются различными — это гарантирует «свободное» непротиворечивое расположение всех элементов в таблице минимального правила соответствующей свободной $\mathcal{Q}$-разметки.

	v_1	v_2	v_3	v_4	w_4	y_1	y_2	y_3	y_4	y_5
v_1		y_1				w_1				
v_2										
v_3										
v_4										
w_4										
y_1			y_2				y_3			
y_2								w_2		
y_3				y_4						
y_4							y_5			w_4
y_5					w_4					

Таб. 1.

В результате работы рассмотренного алгоритма построения $\mathcal{Q}$-транзитивной сети получается $\mathcal{Q}$-биективная сеть, которая, вообще говоря, не является $\mathcal{B}^*$-биективной. По этой причине данный алгоритм невозможно использовать для построения $\mathcal{B}^*$-транзитивной сети. Однако центральная идея указанного алгоритма достаточно универсальна — внесение небольших изменений в структуру алгоритма приводит к тому, что алгоритм становится пригодным для построения $\mathcal{B}^*$-транзитивной сети и при этом все параметры работы останутся неизменными.

Алгоритм 2. (построение $\mathcal{B}^*$-транзитивной сети)
Вход: произвольная $\mathcal{B}^*$-биективная сеть Σ в каноническом представлении

$$\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}) .$$

Шаг $s \in \{1, \ldots, n-1\}$**.** Пусть первые $(s-1)$ слоев канонического представления сети Σ уже модифицированы

$$\widehat{\Sigma}_{s-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}),$$

и μ — свободная $\mathcal{B}^*$-разметка сети $\widehat{\Sigma}_{s-1}$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \mu(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = v.$$

Продолжим $\mathcal{B}^*$-разметку μ сети $\widehat{\Sigma}_{s-1}$ свободным образом до $\mathcal{B}^*$-разметки сети

$$\widehat{\Sigma}'_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s})$$

и выберем любую вершину $x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$, $j \in \{s, \ldots, n\}$, у которой метка $\mu(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)})$ не является координатой какого-либо набора из области определения $F_{\widehat{\Sigma}'_s}$ — минимального правила разметки μ сети $\widehat{\Sigma}'_s$.

Если $j \neq s$**, то** модифицируем s-й слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ следующим образом:

$$\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s} = \Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s} \cdot \Sigma_j^{(s,j)} \cdot \Sigma_s^{(j,s)} \cdot \Sigma_j^{(s,j)}.$$

Если $j = s$**, то** выберем произвольный $m \in \{s+1, \ldots, n\}$ и модифицируем s-й слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ следующим образом:

$$\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s} = \Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s} \cdot \Sigma_m^{(s,m)} \cdot \Sigma_s^{(m,s)} \cdot \Sigma_m^{(s,m)}.$$

Выход: $(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$ — каноническое представление биективной сети $\widehat{\Sigma}$, сложности не более чем $\|\Sigma\| + 3n - 3$.

Теорема 2.12. *Пусть* $\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$ — *произвольная* $\mathcal{B}^*$*-биективная сеть ширины* n*. Тогда её модификация* $\widehat{\Sigma}$ *является* $\mathcal{B}^*$*-транзитивной для любого множества* Ω*, мощность которого не менее чем* $\|\Sigma\| + 4n - 3$*.*

Доказательство. Аналогично доказательству теоремы 2.10. □

Следствие 2.7. *Для любого* $n \geqslant 2$ *существует сеть* $\widehat{\Sigma}$ *ширины* n *и веса* $3n-3$*, которая* $\mathcal{B}^*$*-транзитивна для всех множеств мощности не менее чем* $4n-3$*.*

Замечание 2.5. Отметим, что предложенный алгоритм построения $\mathcal{B}^*$-транзитивной сети невозможно использовать для построения $\mathcal{Q}$-транзитивных сетей из произвольных $\mathcal{Q}$-биективных сетей, поскольку результатом применения данного алгоритма к произвольной $\mathcal{B}^*$-биективной сети будет $\mathcal{B}^*$-транзитивная сеть, которая может оказаться не $\mathcal{Q}$-транзитивной.

Так, например, следующая $\mathcal{Q}$-биективная сеть ширины 3

$$\Sigma_3^{(1,3)} \cdot \Sigma_1^{(3,1)} \cdot \Sigma_3^{(1,3)} \cdot \Sigma_3^{(2,3)} \cdot \Sigma_2^{(3,2)} \cdot \Sigma_3^{(2,3)}$$

является результатом работы изложенного алгоритма применительно к пустой сети, реализующей тождественное преобразование. Указанная сеть допускает свободную $\mathcal{B}^*$-разметку при любых ограничениях $\left(\begin{smallmatrix} v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{smallmatrix}\right)$ из $\mathbb{N}$, что наглядно показано на левой части рисунка 6. При этом минимальное правило такой разметки схематично можно изобразить в виде следующей таблицы:

	v_1	v_2	v_3	w_1	w_2	y_1	y_2	y_3
v_1			y_1					
v_2							y_3	
v_3								
w_1						y_2		
w_2								w_3
y_1	w_1							
y_2								
y_3		w_2						

Таб. 2.

Нетрудно видеть, что при любых ограничениях $\left(\begin{smallmatrix} v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{smallmatrix}\right)$ все внутренние метки y_1, y_2, y_3 остаются различными — это гарантирует «свободное» непротиворечивое расположение всех элементов в таблице минимального правила соответствующей свободной $\mathcal{B}^*$-разметки.

Однако указанная сеть не является $\mathcal{Q}$-транзитивной, поскольку не допускает свободную $\mathcal{Q}$-разметку при ограничениях $\left(\begin{smallmatrix} v_1 & v_1 & v_3 \\ w_1 & w_1 & w_3 \end{smallmatrix}\right)$ с различными $v_3 \neq w_3$, что наглядно показано на правой части рисунка 6.

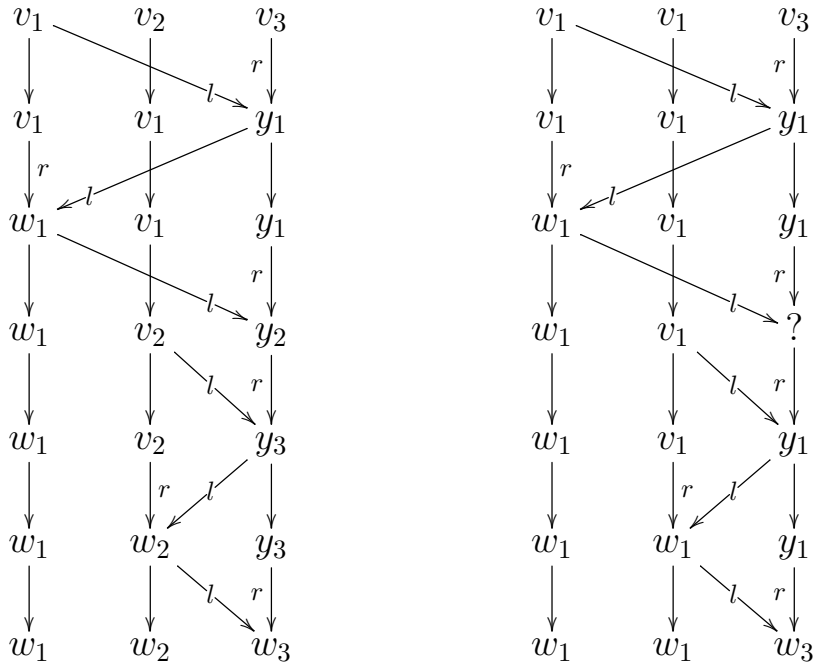

Рис. 6

§2.3 Нижняя оценка веса транзитивных сетей

Вполне очевидно, что произвольная $\mathcal{R}$-транзитивная сеть ширины n никак не может иметь вес меньше чем n. Следующий результат представляет менее тривиальную нижнюю оценку веса произвольной $\mathcal{R}$-транзитивной сети.

Теорема 2.13. *Пусть $\mathcal{R}$-биективная сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ имеет ширину n и является $\mathcal{R}$-транзитивной для множества Ω, $|\Omega| \geqslant 2$. Тогда $t \geqslant \frac{3}{2}n$.*

Доказательство. Пусть $v, w_1, \ldots, w_n \in \mathbb{N}$ — различные элементы и η_0 — свободная разметка сети Σ, полученная в результате свободного продолжения начальной разметки $\eta_0(x_1^{(0)}) = v, \ldots, \eta_0(x_n^{(0)}) = v$ с помощью меток множества $Y = \{y_1, y_2, \ldots\}$. Заменив в разметке η_0 метки $\eta_0(x_1^{(t)}), \ldots, \eta_0(x_n^{(t)})$ на $w_1, \ldots, w_n$ соответственно, мы получим разметку η сети Σ с ограничениями $\left(\begin{smallmatrix} v & \cdots & v \\ w_1 & \cdots & w_n \end{smallmatrix}\right)$.

Если в отношении G, связанном с разметкой η, содержится тройка вида (v, v, w_{j_r}) (в частности, при $n = 2$), то при отождествлении метки w_{j_r} с v и последующем $\mathcal{R}$-приведении разметки η потребуется все метки w_j, $j \neq j_r$

отождествить с v. Таким образом, получили противоречие: по условию теоремы существует $\mathcal{R}$-разметка сети Σ (элементами множества Ω) с ограничениями $\left(\begin{smallmatrix} v & \dots & v & \dots & v \\ w & \dots & v & \dots & w \end{smallmatrix}\right)$, $v \neq w$, а, следовательно, по теореме 2.7 существует свободная разметка сети Σ с указанными ограничениями, которая, согласно доказательству теоремы 2.7, может быть получена при замене в разметке η метки w_{j_r} на метку v и последующем $\mathcal{R}$-приведении полученной разметки, что невозможно, ввиду отождествления всех меток w_j, $j \neq j_r$ с v.

Аналогичным образом обнаруживаются противоречия в случаях, когда $n \geqslant 3$ и в отношении G, связанном с разметкой η, содержится тройка вида (w_i, v, w_k) или (v, w_j, w_k).

Далее полагаем, что $n \geqslant 3$ и отношение G не содержит троек вида (v, v, w_{j_r}), (w_i, v, w_k) или (v, w_j, w_k).

Докажем утверждение методом «от противного», отдельно рассмотрев случаи $\mathcal{B}^*$-транзитивной и $\mathcal{Q}$-транзитивной сетей.

Случай $\mathcal{B}^*$-транзитивной сети Σ. При $t < \frac{3}{2}n$ в разметке η, очевидно, используется $k < \frac{1}{2}n$ меток множества Y и связанное с разметкой η соотношение G очевидно содержит $2n - t > \frac{1}{2}n$ троек

$$(v, y_{i_1}, w_{j_1}), \dots, (v, y_{i_{2n-t}}, w_{j_{2n-t}}).$$

Нетрудно понять, что для некоторых $1 \leqslant r \neq s \leqslant 2n-t$ выполняется равенство $y_{i_r} = y_{i_s}$ и при $\mathcal{B}^*$-приведении разметки η необходимо требуется отождествление меток w_{j_r} и w_{j_s}.

Таким образом, пришли к противоречию: по условию теоремы существует $\mathcal{B}^*$-разметка сети Σ (элементами множества Ω) с ограничениями $\left(\begin{smallmatrix} v & \dots & v & \dots & v \\ v & \dots & w_{i_r} & \dots & v \end{smallmatrix}\right)$, а, следовательно, по теореме 2.7 существует свободная разметка сети Σ с указанными ограничениями, которая, согласно доказательству теоремы 2.7, может быть получена при замене в разметке η меток w_j, $j \neq j_r$ на метку v и последующем $\mathcal{B}^*$-приведении полученной разметки, что невозможно ввиду отождествления w_{j_r} с v.

Случай $\mathcal{Q}$-транзитивной сети Σ. При $t < \frac{3}{2}n$ в разметке η используется $k < \frac{1}{2}n$ меток множества Y и связанное с разметкой η соотношение G, очевидно,

содержит $2n - t > \frac{1}{2}n$ троек вида

$$(v, y_{i_1}, w_{j_1}), \ldots, (v, y_{i_l}, w_{j_l}) \quad \text{и} \quad (y_{i_{l+1}}, v, w_{j_{l+1}}), \ldots, (y_{i_{2n-t}}, v, w_{j_{2n-t}}).$$

Не ограничивая общности, полагаем, что $l \geqslant 2$. В таком случае при отождествлении меток w_{j_r} и w_{j_s}, $1 \leqslant j_r, j_s \leqslant l$ и последующем $\mathcal{Q}$-приведении разметки η необходимо требуется отождествление меток y_{i_r} и y_{i_s}. Если при этом

$$i_r = i_{d_1},\ i_s = i_{d_2},\ l + 1 \leqslant d_1, d_2 \leqslant 2n - t,$$

то в отношении G содержится пара троек $(y_{i_r}, v, w_{j_{d_1}})$, $(y_{i_s}, v, w_{j_{d_2}})$ и при дальнейшем $\mathcal{Q}$-приведении разметки η очевидно потребуется отождествление меток $w_{j_{d_1}}$ и $w_{j_{d_2}}$ — получили противоречие с $\mathcal{Q}$-транзитивностью сети Σ. В противном случае будет получена разметка η_1 сети Σ, в которой используется $k - 1$ меток множества Y и связанное с разметкой η_1 отношение G_1, очевидно, содержит $2n - t - 1$ троек вида

$$(v, y_{i_1}, w_{j_1}), \ldots, (v, y_{i_l}, w_{j_l}) \quad \text{и} \quad (y_{i_{l+1}}, v, w_{j_{l+1}}), \ldots, (y_{i_{2n-t}}, v, w_{j_{2n-t-1}}).$$

Применяя к данной и последующим разметкам аналогичные рассуждения, получаем последовательность разметок $\eta, \eta_1, \ldots$, которая либо обрывается на некотором конечном шаге с номером d в том смысле, что применение к разметке η_d аналогичных рассуждений необходимо требует отождествления различных меток из множества W — получили противоречие с $\mathcal{Q}$-транзитивностью сети Σ, либо останавливается на шаге с номером $k - 1$. Во втором случае построенная разметка η_{k-1} содержит единственную метку множества Y и связанное с данной разметкой отношение G_{k-1}, очевидно, содержит 2 тройки

$$(v, y, w_{j_1}) \quad \text{и} \quad (y, v, w_{j_2}).$$

Однако, дополнительно, в отношении G_{k-1} содержится не менее одной тройки вида

$$(w_m, y, w_{m_1}) \quad \text{или} \quad (y, w_m, w_{m_2}).$$

Легко видеть, что при отождествлении метки w_m с v и дальнейшем $\mathcal{Q}$-приведении полученной разметки необходимо требуется отождествление меток w_{m_*} и w_{j_*} — получили противоречие с $\mathcal{Q}$-транзитивностью сети Σ. $\square$

Рассмотрим два интересных примера $\mathcal{R}$-транзитивных сетей ширины n и небольшого веса $2n-1$, которые, могут быть использованы для эффективного построения широкого класса $\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры.

Пример 2.4. Рассмотрим $\mathcal{B}^*$-биективную сеть Δ_n ширины n, которая представляется в виде следующего произведения $2n-1$ элементарных сетей:

$$\Delta_n = \Sigma_2^{(1,2)} \cdot \Sigma_3^{(2,3)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_1^{(n,1)} \cdot \Sigma_n^{(n-1,n)} \cdot \ldots \cdot \Sigma_3^{(2,3)} \cdot \Sigma_2^{(3,2)}.$$

Данная сеть Δ_n допускает свободную $\mathcal{R}$-разметку при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ из $\mathbb{N}$, что наглядно показано на рисунке 7.

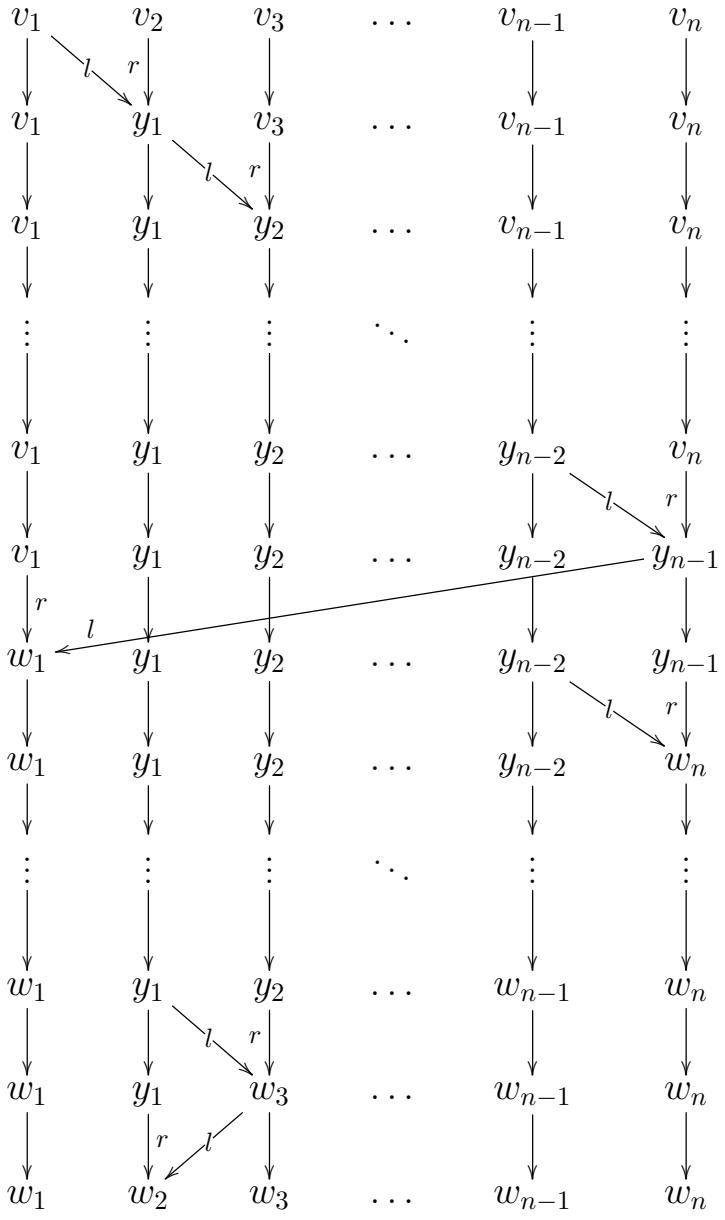

Рис. 7.

Минимальное правило такой разметки схематично можно изобразить в виде следующей таблицы:

	v_1	v_2	v_3	v_4	$\ldots$	v_n	y_1	y_2	y_3	$\ldots$	y_{n-1}
v_1		y_1									
v_2											
$\vdots$											
v_n											
w_3							w_2				
y_1			y_2					w_3			
y_2				y_3					w_4		
$\vdots$					$\ddots$					$\ddots$	
y_{n-2}						y_{n-1}					w_n
y_{n-1}	w_1										

Таб. 3.

Легко видеть, что при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ элементы $y_1, \ldots, y_{n-1}$ остаются различными и отличаются от $v_1, \ldots, v_n, w_1, \ldots, w_n$, а потому каждая стока рассмотренной таблицы никогда не содержит одинаковых элементов и минимальное правило разметки является $\mathcal{R}$-отображением. Для большей наглядности укажем вид, который примет данная таблица в крайнем случае, когда $w_3 = v_1 = \ldots = v_n$:

	w_3	y_1	y_2	y_3	$\ldots$	y_{n-1}
w_3	y_1	w_2				
y_1	y_2		w_3			
y_2	y_3			w_4		
$\vdots$	$\vdots$				$\ddots$	
y_{n-2}	y_{n-1}					w_n
y_{n-1}	w_1					

Таб. 4.

Итак, сеть Δ_n допускает свободную $\mathcal{R}$-разметку при любых ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$. Поскольку каждая $\mathcal{R}$-разметка сети Δ_n содержит не более $3n-1$ различных меток, то можно полагать, что для любого множества Ω, мощность которого не менее $3n-1$, сеть Δ_n допускает $\mathcal{R}$-разметку элементами множества Ω при любых ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из Ω. Последнее утверждение, согласно утверждению 2.4, равносильно $\mathcal{R}$-транзитивности сети Δ_n для множества Ω.

Пример 2.5. Рассмотрим $\mathcal{B}^*$-биективную сеть Ψ_n ширины n, которая представляется в виде следующего произведения $2n-1$ элементарных сетей:

$$\Psi_n = \Sigma_n^{(1,n)} \cdot \Sigma_1^{(n,1)} \cdot \Sigma_n^{(2,n)} \cdot \Sigma_2^{(n,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \Sigma_n^{(n-1,n)}.$$

Данная сеть Ψ_n допускает свободную $\mathcal{B}^*$-разметку при любых ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из $\mathbb{N}$, что наглядно показано на рисунке 8.

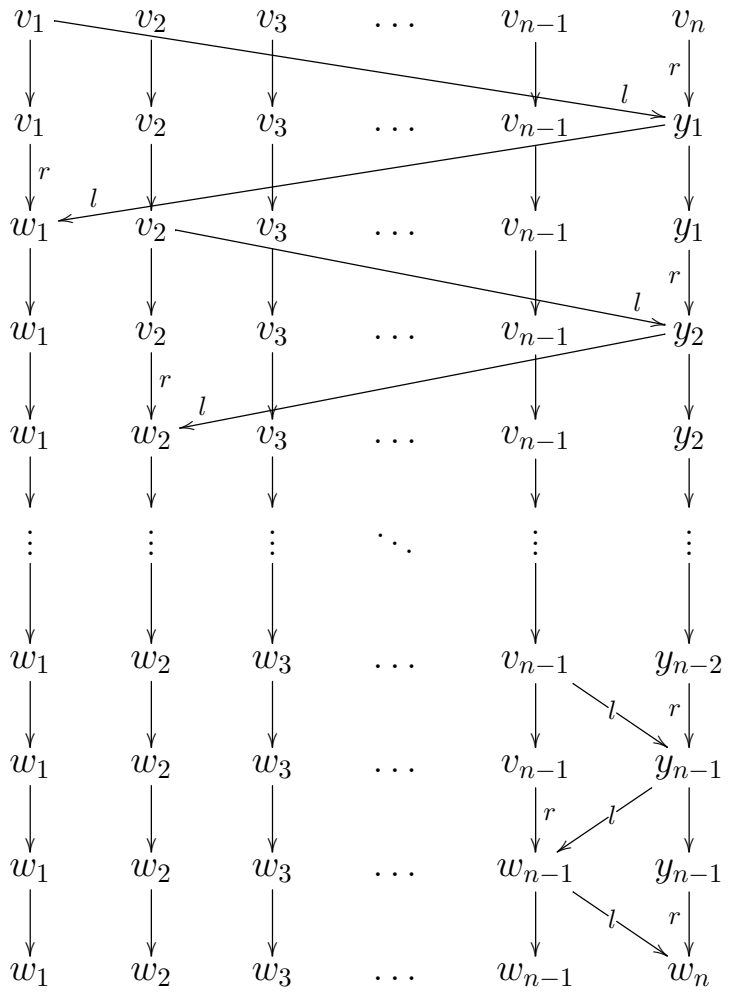

Рис. 8

Минимальное правило такой разметки схематично можно изобразить в виде следующей таблицы:

	v_1	v_2	$\ldots$	v_{n-1}	v_n	w_{n-1}	y_1	y_2	$\ldots$	y_{n-2}	y_{n-1}
v_1					y_1						
v_2							y_2				
v_3								y_3			
$\vdots$			$\ddots$						$\ddots$		
v_{n-1}										y_{n-1}	
w_{n-1}											w_n
y_1	w_1										
y_2		w_2									
$\vdots$			$\ddots$								
y_{n-1}				w_{n-1}							

Таб. 5.

Легко видеть, что при любых ограничениях $\left(\begin{smallmatrix} v_1 & \ldots & v_n \\ w_1 & \ldots & w_n \end{smallmatrix}\right)$ элементы $y_1, \ldots, y_{n-1}$ остаются различными и отличаются от $v_1, \ldots, v_n, w_1, \ldots, w_n$, а потому каждая строка рассмотренной таблицы никогда не содержит одинаковых элементов и минимальное правило разметки является $\mathcal{B}^*$-отображением. Для большей наглядности укажем вид, который примет данная таблица в крайнем случае, когда $w_{n-1} = v_1 = \ldots = v_n$:

	w_{n-1}	y_1	y_2	y_3	$\ldots$	y_{n-2}	y_{n-1}
w_{n-1}	y_1	y_2	y_3	y_4	$\ldots$	y_{n-1}	w_n
y_1	w_1						
y_2	w_2						
y_3	w_3						
$\vdots$	$\vdots$						
y_{n-2}	w_{n-2}						
y_{n-1}	w_{n-1}						

Таб. 6.

Итак, сеть Ψ_n допускает свободную $\mathcal{B}^*$-разметку при любых ограничениях $\binom{v_1 \ \dots \ v_n}{w_1 \ \dots \ w_n}$. Поскольку каждая $\mathcal{B}^*$-разметка сети Ψ_n содержит не более $3n-1$ различных меток, то можно полагать, что для любого множества Ω, мощность которого не менее $3n-1$, сеть Ψ_n допускает $\mathcal{B}^*$-разметку элементами множества Ω при любых ограничениях $\binom{v_1 \ \dots \ v_n}{w_1 \ \dots \ w_n}$ из Ω. Последнее утверждение, согласно утверждению 2.4, равносильно $\mathcal{B}^*$-транзитивности сети Ψ_n для множества Ω.

В заключение отметим, что сеть Ψ_n, в отличие от сети Δ, не допускает $\mathcal{Q}$-разметку с ограничениями $\binom{1 \ \dots \ 1}{2 \ \dots \ 2}$ и потому не является $\mathcal{Q}$-транзитивной ни для какого множества Ω, $|\Omega| \geqslant 2$.

Архитектуры $\mathcal{B}^*$-транзитивных сетей Δ_n и Ψ_n, рассмотренных в примерах 2.4 и 2.5 соответственно, отличаются существенным образом. Однако можно выделить одну общую особенность указанных сетей — независимо от ограничений $\binom{v_1 \ \dots \ v_n}{w_1 \ \dots \ w_n}$, соответствующие свободные $\mathcal{R}$-разметки сетей Δ_n и Ψ_n содержат различные метки $y_1, \dots, y_{n-1}$ — можно сказать, что сети Δ_n и Ψ_n не допускают «сокращений» внутренних меток. Отмеченная особенность позволяет свободно «разместить» произвольные элементы $w_1, \dots, w_n$ в таблице минимального правила соответствующей свободной разметки и, как показывает следующая теорема, делает сети Δ_n и Ψ_n пригодными для простого построения широкого класса $\mathcal{R}$-транзитивных сетей.

Теорема 2.14. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n и при проведении свободной разметки μ сети Σ с начальным условием $(v, \dots, v)$ метка $\mu(x_1^{(t)})$ не является координатой какого-либо набора из области определения ее минимального правила $F_{\Sigma,\mu}$. Тогда произведение $\Sigma \cdot \Delta_n$ является $\mathcal{R}$-транзитивным для любого множества Ω мощности не менее чем $t+3n-1$.*

Если, дополнительно, Σ — $\mathcal{B}^*$-биективная сеть, то произведение $\Sigma \cdot \Psi_n$ является $\mathcal{B}^*$-транзитивным для любого множества Ω мощности не менее чем $t+3n-1$.

Доказательство. Докажем $\mathcal{R}$-транзитивность произведения $\Sigma \cdot \Delta_n$:

$$\Sigma \cdot \Delta_n = \Sigma \cdot \Sigma_2^{(1,2)} \cdot \Sigma_3^{(2,3)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_1^{(n,1)} \cdot \Sigma_n^{(n-1,n)} \cdot \ldots \cdot \Sigma_3^{(2,3)} \cdot \Sigma_2^{(3,2)}.$$

Поскольку при проведении свободной разметки μ сети Σ с начальным условием $(v,\dots,v)$ метка $\mu(x_1^{(t)})$ не является координатой какого-либо набора из области определения ее минимального правила $F_{\Sigma,\mu}$, то, согласно следствию 2.5, при проведении произвольной свободной разметки η сети Σ с начальным условием $(v_1,\dots,v_n)$ метка $\eta(x_1^{(t)})$ не является координатой какого-либо набора из области определения ее минимального правила $G_{\Sigma,\eta}$.

Продолжив свободную разметку η сети Σ свободным образом до окончания сети $\Sigma\cdot\Delta_n$, получим, что метки $\eta(x_1^{(t+n-1)}),\dots,\eta(x_n^{(t+n-1)})$ — различны и при последующей замене меток $\eta(x_1^{(t+2n-1)}),\dots,\eta(x_n^{(t+2n-1)})$ на произвольные элементы $w_1,\dots,w_n$ соответственно, в новой разметке не возникает никаких противоречий (подобно тому, как это было с сетью Δ). Таким образом, можно построить свободную разметку сети $\Sigma\cdot\Delta_n$ с произвольными ограничениями $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$, для которой требуется не более $n+t+2n-1$ различных меток.

Остается заметить, что для любого множества Ω мощности не менее $t+3n-1$ сеть $\Sigma\cdot\Delta_n$ допускает $\mathcal{R}$-разметку элементами множества Ω при произвольных ограничениях $\left(\begin{smallmatrix} v_1 & \dots & v_n \\ w_1 & \dots & w_n \end{smallmatrix}\right)$ из Ω, что, согласно утверждению 2.4, равносильно $\mathcal{R}$-транзитивности сети $\Sigma\cdot\Delta_n$ для множества Ω.

$\mathcal{B}^*$-транзитивность произведения $\Sigma\cdot\Psi_n$ доказывается аналогично. □

Замечание 2.6. Вообще говоря, ограничение на сеть Σ, сформулированное в условии теоремы 2.14, не такое уж сильное. Так, согласно лемме 2.11, при проведении свободной разметки μ произвольной $\mathcal{R}$-биективной сети Σ хотя бы одна из меток $\mu(x_1^{(t)}),\dots,\mu(x_n^{(t)})$ не является координатой какого-либо набора из области определения ее минимального правила F.

Следствие 2.8. *При всех натуральных r сеть Δ_n^r — $\mathcal{R}$-транзитивна, а сеть Ψ_n^r — $\mathcal{B}^*$-транзитивна для любого множества Ω, мощность которого не менее чем $r(2n-1)+n$.*

Замечание 2.7. В данной главе с использованием аппарата разметок удалось сформулировать и обосновать несколько эффективных способов построения таких $\mathcal{R}$-биективных сетей Σ, которые являются $\mathcal{R}$-транзитивными для всякого множества Ω мощности не менее чем $\|\Sigma\|+n$, где n — ширина Σ.

При этом, стоит отметить, что в качестве транзитивного класса преобразований, реализуемого сетью Σ, можно использовать не только полный класс $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, но и специальные репрезентативные выборки $\{\Sigma^F : F \in \mathcal{K}\}$, где $\mathcal{K} \subset \mathcal{R}(\Omega)$ и $|\mathcal{K}| \leq |\Omega|^{2n}$, которые также действуют транзитивным образом на множестве наборов Ω^n. Поясним как построить подобную выборку.

Если сеть Σ — $\mathcal{R}$-транзитивна для множества Ω, то она при любых ограничениях $\left(\begin{smallmatrix} v_1 & \cdots & v_n \\ w_1 & \cdots & w_n \end{smallmatrix}\right)$ из Ω допускает разметку элементами Ω, а правило данной разметки можно продолжить до некоторой бинарной операции $F \in \mathcal{R}(\Omega)$:

$$\Sigma^F(v_1, \ldots, v_n) = (w_1, \ldots, w_n).$$

Таким образом, построив для каждых ограничений $\left(\begin{smallmatrix} v_1 & \cdots & v_n \\ w_1 & \cdots & w_n \end{smallmatrix}\right)$ из Ω произвольную $\mathcal{R}$-разметку элементами множества Ω (например, свободную $\mathcal{R}$-разметку с ограничениями $\left(\begin{smallmatrix} v_1 & \cdots & v_n \\ w_1 & \cdots & w_n \end{smallmatrix}\right)$) и продолжив ее минимальное правило до некоторой бинарной операции $F \in \mathcal{R}(\Omega)$, мы определим класс $\mathcal{K} \subset \mathcal{R}(\Omega)$, $|\mathcal{K}| \leq |\Omega|^{2n}$, для которого множество преобразований $\{\Sigma^F : F \in \mathcal{K}\}$ действует транзитивным образом на множестве наборов Ω^n.

Замечание 2.8. В заключение отметим, что до сих пор не удалось построить пример $\mathcal{R}$-транзитивной сети ширины n и веса строго меньше чем $2n-1$ — на данный момент вопрос о существовании таких сетей остается открытым.

При неудачных попытках построения примера $\mathcal{R}$-транзитивной сети ширины n и веса строго меньше чем $2n-1$ первоначально возникло предположение, что нижняя граница веса $\mathcal{R}$-транзитивной сети ширины n равна величине $2n-1$ и все $\mathcal{R}$-транзитивные сети с указанными параметрами не допускают «сокращений» (при выборе любых ограничений не возникает необходимость отождествления каких-либо внутренних меток). Однако, как показывает следующий пример, данное предположение оказалось неверным — $\mathcal{R}$-транзитивные сети ширины n и веса $2n-1$ могут быть устроены более сложным образом и допускать «сокращения».

Рассмотрим $\mathcal{Q}$-биективную сеть Σ ширины 4, которая представляется в виде следующего произведения элементарных сетей

$$\Sigma = \Sigma_3^{(2,3)} \cdot \Sigma_4^{(3,4)} \cdot \Sigma_2^{(2,3)} \cdot \Sigma_3^{(3,4)} \cdot \Sigma_1^{(4,1)} \cdot \Sigma_4^{(3,4)} \cdot \Sigma_4^{(4,3)}.$$

Сеть Σ допускает свободную $\mathcal{Q}$-разметку η при произвольных ограничениях $\left(\begin{smallmatrix} v_1 & v_2 & v_3 & v_4 \\ w_1 & w_2 & w_3 & w_4 \end{smallmatrix}\right)$, что наглядно показано на рисунке 9:

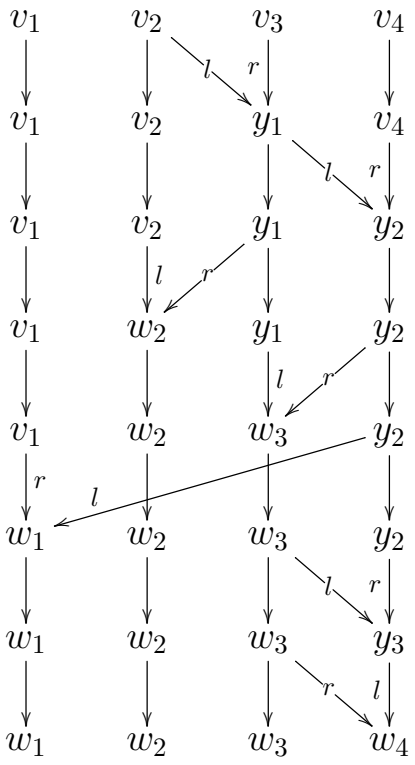

Рис. 9

Правило G, соответствующее указанной разметке η, схематично можно изобразить в виде следующей таблицы:

	v_1	v_2	v_3	v_4	w_3	y_1	y_2	y_3
v_1								
v_2			y_1			w_2		
v_3								
v_4								
w_3							y_3	
y_1				y_2			w_3	
y_2	w_1							
y_3					w_4			

Таб. 7.

Легко видеть, что при отождествлении $v_1 = w_3$ и $w_1 = w_4$ в разметке η и последующем $\mathcal{Q}$-приведении полученной разметки необходимо потребуется отождествление меток y_2 и y_3. При этом правило полученной разметки будет выглядеть следующим образом:

	v_1	v_2	v_3	v_4	y_1	y_2
v_1						y_2
v_2			y_1		w_2	
v_3						
v_4						
y_1				y_2		w_3
y_2	w_1					

Таб. 8.

Однако, нетрудно видеть, что любое дальнейшее отождествление меток в полученных ограничениях, более не вызывает необходимости отождествления внутренних меток y_1 и y_2 между собой и с другими метками. Для большей наглядности укажем вид таблицы правила в крайнем случае при отождествлении $v_1 = v_2 = v_3 = v_4 = w_1 = w_2 = w_3 = w_4$:

	w_1	y_1	y_2
w_1	y_1	w_1	y_2
y_1	y_2		w_1
y_2	w_1		

Таб. 9.

Таким образом, рассмотренная $\mathcal{Q}$-биективная сеть Σ допускает свободную $\mathcal{Q}$-разметку при любых ограничениях, что, согласно утверждению 2.4, равносильно её $\mathcal{Q}$-транзитивности для всех множеств Ω, $|\Omega| \geqslant 11$. Но при этом сеть Σ допускает «сокращения» при некоторых ограничениях.

Выводы по главе

Основные результаты данной главы заключаются в следующем:

1. получены критерии $\mathcal{B}^*$-транзитивности, $\mathcal{Q}$-транзитивности и универсальный критерий $\mathcal{R}$-транзитивности сетей;

2. обосновано интересное с теоретической точки зрения упрощение универсального критерия $\mathcal{R}$-транзитивности;

3. показана возможность эффективной практической реализации для проверки универсального критерия $\mathcal{R}$-транзитивности сетей;

4. сформулированы и строго обоснованы эффективные алгоритмы построения $\mathcal{Q}$-биективных и $\mathcal{B}^*$-биективных сетей, действующих транзитивным образом для всех достаточно больших множеств;

5. получена нетривиальная нижняя оценка веса $\mathcal{R}$-транзитивной сети;

6. построены универсальные конструкции $\mathcal{R}$-биективных сетей небольшого веса, которые могут быть использованы для эффективного построения широких классов $\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры.

Глава 3. k-транзитивные сети

Данная глава диссертации посвящена исследованию k-транзитивности множества блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ при $k \geqslant 2$.

В §3.1 продолжается развитие аппарата разметок — формулируются естественные k-мерные обобщения основных понятий и доказываются k-мерные аналоги основных технических результатов.

В §3.2 с использованием k-мерных инструментов аппарата разметок формулируются и доказываются критерии $k\mathcal{B}^*$-транзитивности, $k\mathcal{Q}$-транзитивности сети и универсальный критерий $k\mathcal{R}$-транзитивности сетей. Кроме того, развитый аппарат разметок позволяет сформулировать и обосновать эффективный с практической точки зрения способ проверки универсального критерия $k\mathcal{R}$-транзитивности.

В §3.3 на языке разметок излагается и обосновывается эффективный алгоритм построения $\mathcal{R}$-биективных сетей, действующих кратно транзитивным образом для всех достаточно больших множеств. Кроме того, в §3.3 определяется универсальная конструкция $\mathcal{R}$-биективных сетей ∇_n ширины $n \in \mathbb{N}$ и небольшого веса $4n-4$, которые являются $k\mathcal{R}$-транзитивными при любом $k \geqslant 2$ для всех достаточно больших множеств. В заключение показывается, что предложенная серия $\mathcal{R}$-биективных сетей ∇_n, $n \in \mathbb{N}$ может быть использована для эффективного построения широких классов $k\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры.

Результаты данной главы опубликованы в [62, 64, 66].

§3.1 k-разметка биективных сетей

Определение 3.1. $\mathcal{R}$-биективную сеть Σ будем называть *$k\mathcal{R}$-транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ является k-транзитивным.

Нетрудно понять, что сама природа множества Ω в данном определении не играет никакой роли, и потому корректно говорить, что $\mathcal{R}$-биективная сеть

Σ является $k\mathcal{R}$-транзитивной для множеств мощности q. По-прежнему, будем полагать, что $\Omega \subset \mathbb{N}$, а для множества $\{1, \ldots, q\}$ будем использовать обозначение Ω_q.

Введенный в §1 и развитый в главе 2 аппарат разметки сетей на самом деле позволяет проверять не только $\mathcal{R}$-транзитивность сети, но и более сложное свойство $k\mathcal{R}$-транзитивности при $k \geqslant 2$. Так, например, из условия $k\mathcal{R}$-транзитивности $\mathcal{R}$-биективной сети Σ для множества Ω следует, что для любых различных наборов

$$(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn}) \in \Omega^n$$

и любых различных наборов

$$(w_{11}, \ldots, w_{1n}), \ldots, (w_{k1}, \ldots, w_{kn}) \in \Omega^n$$

сеть Σ допускает k правильных $\mathcal{R}$-разметок элементами множества Ω с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ соответственно и общим правилом, которое является $\mathcal{R}$-отображением.

Для удобства исследования $k\mathcal{R}$-транзитивности $\mathcal{R}$-биективных сетей сформулируем естественные k-мерные обобщения соответствующих и докажем необходимые основные утверждения.

Поскольку отображение, реализуемое перестановочной сетью, не зависит от выбора операции $F \in \mathcal{B}(\Omega)$, представляется очевидным следующее

Утверждение 3.1. *Пусть Σ — произвольная $k\mathcal{R}$-транзитивная для множества Ω сеть, а Π_1, Π_2 — такие перестановочные сети, для которых существуют корректно определенные произведения $\Pi_1 \cdot \Sigma$ и $\Sigma \cdot \Pi_2$. Тогда сети $\Pi_1 \cdot \Sigma$ и $\Sigma \cdot \Pi_2$ также $k\mathcal{R}$-транзитивны для множества Ω.*

Учитывая результаты теорем 1.2 и 1.5, а также утверждения 3.1, не ограничивая общности, далее будем полагать, что произвольная $\mathcal{Q}$-биективная ($\mathcal{B}^*$-биективная) сеть Σ представляет собой произведение $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ элементарных сетей (1-го типа) с множеством вершин $X_0 \cup X_1 \cup \ldots \cup X_t$ (кратко будем писать $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$).

Определение 3.2. Пусть $\mu_1, \ldots, \mu_k$ — разметки сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Тогда набор $\mu = (\mu_1, \ldots, \mu_k)$ будем называть *k-разметкой* сети Σ; при этом метки разметок $\mu_1, \ldots, \mu_k$ будем называть метками k-разметки μ.

k-разметку $\mu = (\mu_1, \ldots, \mu_k)$ сети Σ будем называть *полной*, если $\mu_1, \ldots, \mu_k$ — полные разметки сети Σ.

С произвольной k-разметкой $\mu = (\mu_1, \ldots, \mu_k)$ сети Σ можно связать отношение $F \subset \mathbb{N}^3$, определённое следующим образом: отношение F содержит тройку (y_l, y_r, y_q) в том и только в том случае, когда для некоторых $s \in \{1, \ldots, t\}$ и $d \in \{1, \ldots, k\}$ выполняются равенства

$$\Sigma_s = \Sigma_j^{(i_1, i_2)} \quad \text{и} \quad (\mu_d(x_{i_1}^{(s-1)}), \mu_d(x_{i_2}^{(s-1)}), \mu_d(x_j^{(s)})) = (y_l, y_r, y_q).$$

Полную k-разметку μ будем называть *правильной*, если связанное с ней отношение F обладает функциональным свойством (1.1). При этом соответствующее частичное отображение F будем называть *минимальным правилом* k-разметки μ.

Правильную k-разметку μ будем называть *$k\mathcal{Q}$-разметкой* (*$k\mathcal{B}^*$-разметкой*), если её минимальное правило является $\mathcal{Q}$-отображением ($\mathcal{B}^*$-отображением).

Определение 3.3. Если для k-разметки $\mu = (\mu_1, \ldots, \mu_k)$ сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ выполняются системы равенств

$$\{\mu_1(x_{i_{j_1}}^{(s_{j_1})}) = v_{j_1} : j_1 \in J_1\}, \ \ldots \ , \{\mu_k(x_{i_{j_k}}^{(s_{j_k})}) = v_{j_k} : j_k \in J_k\}$$

то будем говорить, что μ — разметка сети Σ с условиями

$$\{\mu_1(x_{i_{j_1}}^{(s_{j_1})}) = v_{j_1} : j_1 \in J_1\}, \ \ldots \ , \{\mu_k(x_{i_{j_k}}^{(s_{j_k})}) = v_{j_k} : j_k \in J_k\}.$$

Разметку начальных вершин

$$\mu_1(x_1^{(0)}) = v_{11}, \ldots, \mu_1(x_n^{(0)}) = v_{1n}, \ldots\ldots, \mu_k(x_1^{(0)}) = v_{k1}, \ldots, \mu_k(x_n^{(0)}) = v_{kn}$$

будем называть *начальным условием* k-разметки μ и при этом будем говорить, что μ — *k-разметка с начальным условием* $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$.

Если μ — правильная k-разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$, то произвольное продолжение ее минимального правила естественно называть *правилом*

k-разметки μ. Действительно, если F — некоторое правило k-разметки μ, то данная k-разметка μ удовлетворяет следующим условиям:
для всех $s \in \{1, \dots, t\}$ и $d \in \{1, \dots, k\}$ если $\Sigma_s = \Sigma_j^{(i_1, i_2)}$, то

$$\mu_d(x_j^{(s)}) = F(\mu_d(x_{i_1}^{(s-1)}), \mu_d(x_{i_2}^{(s-1)})) \quad \text{и} \quad \mu(x_m^{(s)}) = \mu(x_m^{(s-1)}),\ m \neq j.$$

Таким образом, правильная k-разметка μ сети Σ однозначно определяется своим начальным условием и некоторым правилом F.

В тех случаях, когда при некоторой разметке начальных вершин

$$\mu_1(x_1^{(0)}) = v_{11}, \dots, \mu_1(x_n^{(0)}) = v_{1n},\ \dots\ , \mu_k(x_1^{(0)}) = v_{k1}, \dots, \mu_k(x_n^{(0)}) = v_{kn}$$

сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ для полного задания правильной k-разметки не хватает области определения частично определённого отображения F, можно продолжить отображение F «свободным» образом и тем самым определить полную k-разметку с правилом F. Рассмотрим подробно два способа построения продолжения. Пусть

$$Y = \{y_{11}, \dots, y_{k1}, y_{12}, \dots, y_{k2}, \dots\dots\} \subset \mathbb{N} \backslash \{v_{11}, \dots, v_{k1}, \dots, v_{1n}, \dots, v_{kn}\}$$

— счётное множество меток, которые не лежат в области значений F и не являются координатами каких-либо наборов из области определения F (при этом возможно, что метки $v_{11}, \dots, v_{k1}, \dots, v_{1n}, \dots, v_{kn}$ также не лежат в области значений F и не являются координатами каких-либо наборов из области определения F).

Последовательное свободное продолжение k-разметки μ заключается в последовательном выполнении следующих действий:

1. используя множество меток $Y_1 = \{y_{11}, y_{12}, \dots\}$, проведём свободное продолжение начальной разметки $\mu_1(x_1^{(0)}) = v_{11}, \dots, \mu_1(x_n^{(0)}) = v_{1n}$ и её правила F относительно сети Σ;

2. используя множество меток $Y_2 = \{y_{21}, y_{22}, \dots\}$, проведём свободное продолжение начальной разметки $\mu_2(x_1^{(0)}) = v_{21}, \dots, \mu_2(x_n^{(0)}) = v_{2n}$ и её правила F_{Σ,μ_1} относительно сети Σ;

...

k. Используя множество меток $Y_k = \{y_{k1}, y_{k2}, \dots\}$, проведём свободное продолжение начальной разметки $\mu_k(x_1^{(0)}) = v_{k1}, \dots, \mu_k(x_n^{(0)}) = v_{kn}$ и её правила $((F_{\Sigma,\mu_1})\dots)_{\Sigma,\mu_{k-1}}$ относительно сети Σ.

Описанную процедуру продолжения k-разметки μ и расширения области определения F будем называть *последовательным свободным продолжением начальной k-разметки*

$$\mu_1(x_1^{(0)}) = v_{11}, \dots, \mu_1(x_n^{(0)}) = v_{1n},\ \dots\ , \mu_k(x_1^{(0)}) = v_{k1}, \dots, \mu_k(x_n^{(0)}) = v_{kn}$$

и отображения F относительно сети Σ. При этом будем говорить, что k-разметка μ получена в результате последовательного свободного продолжения начальной разметки $\mu_1(x_1^{(0)}) = v_{11},\ \dots\dots\ , \mu_k(x_n^{(0)}) = v_{kn}$ и отображения F относительно сети Σ.

Замечание 3.1. При продолжении k-разметки μ сети Σ описанным способом частично определённое $\mathcal{Q}$-отображение ($\mathcal{B}^*$-отображение) F корректным образом продолжается до частично определённого $\mathcal{Q}$-отображения ($\mathcal{B}^*$-отображения) $F_{\Sigma,\mu} = ((F_{\Sigma,\mu_1})\dots)_{\Sigma,\mu_k}$, которое является правилом построенной полной k-разметки μ.

Параллельное свободное продолжение k-разметки заключается в том, что для каждого $s \in \{1, \dots, t\}$ последовательно выполняются следующие действия: если $\Sigma_s = \Sigma_j^{(i_1,i_2)}$, то

0. положим $\mu_d(x_m^{(s)}) = \mu_d(x_m^{(s-1)})$ для всех $d \in \{1, \dots, k\}$ и $m \neq j$;

1. если значение $F\left(\mu_1(x_{i_1}^{(s-1)}), \mu_1(x_{i_2}^{(s-1)})\right)$ определено, то положим $\mu_1(x_j^{(s)}) = F\left(\mu_1(x_{i_1}^{(s-1)}), \mu_1(x_{i_2}^{(s-1)})\right)$; в противном случае положим $\mu_1(x_j^{(s)}) = y_{1s}$ и определим $F\left(\mu_1(x_{i_1}^{(s-1)}), \mu_1(x_{i_2}^{(s-1)})\right) = y_{1s}$;

...

k. если значение $F\left(\mu_k(x_{i_1}^{(s-1)}), \mu_k(x_{i_2}^{(s-1)})\right)$ определено, то положим $\mu_k(x_j^{(s)}) = F\left(\mu_k(x_{i_1}^{(s-1)}), \mu_k(x_{i_2}^{(s-1)})\right)$; в противном случае положим $\mu_k(x_j^{(s)}) = y_{ks}$ и определим $F\left(\mu_k(x_{i_1}^{(s-1)}), \mu_k(x_{i_2}^{(s-1)})\right) = y_{ks}$.

Описанную процедуру продолжения k-разметки μ и расширения области определения F будем называть *параллельным свободным продолжением на-*

чальной k-разметки

$$\mu_1(x_1^{(0)}) = v_{11}, \ldots, \mu_1(x_n^{(0)}) = v_{1n}, \ \ldots \ , \mu_k(x_1^{(0)}) = v_{k1}, \ldots, \mu_k(x_n^{(0)}) = v_{kn}$$

и отображения F относительно сети Σ. При этом будем говорить, что k-разметка μ получена в результате параллельного свободного продолжения начальной разметки $\mu_1(x_1^{(0)}) = v_{11}, \ \ldots\ldots \ , \mu_k(x_n^{(0)}) = v_{kn}$ и отображения F относительно сети Σ.

Замечание 3.2. При продолжении k-разметки μ сети Σ описанным способом частично определённое $\mathcal{Q}$-отображение ($\mathcal{B}^*$-отображение) F корректным образом продолжается до частично определённого $\mathcal{Q}$-отображения ($\mathcal{B}^*$-отображения) $F_{\Sigma,\mu}$, которое является правилом построенной полной k-разметки μ.

Теорема 3.2. *Пусть k-разметки μ' и μ'' получены в результате последовательного и соответственно параллельного свободных продолжений начальной k-разметки*

$$\mu_1(x_1^{(0)}) = v_{11}, \ldots, \mu_1(x_n^{(0)}) = v_{1n}, \ \ldots \ , \mu_k(x_1^{(0)}) = v_{k1}, \ldots, \mu_k(x_n^{(0)}) = v_{kn}$$

и правила F относительно сети Σ. Тогда k-разметки μ' и μ'' отличаются только обратимой заменой меток.

Доказательство. Рассмотрим для простоты понимания сначала случай $k = 2$. Пусть $y_{2j_1}, \ldots, y_{2j_r}$ — все метки вида y_{2*}, которые содержатся в разметке μ_1'', и

$$\mu_1''(x_{i_1}^{(s_1)}) = y_{2j_1}, \ldots, \mu_1''(x_{i_r}^{(s_r)}) = y_{2j_r}$$

— первые появления указанных меток в разметке μ_1''. Тогда нетрудно понять, что в 2-разметке μ'' отсутствуют метки $y_{1s_1}, \ldots, y_{1s_r}$ и обратимая замена меток

$$y_{2j_1} \to y_{1s_1}, \ \ldots \ , y_{2j_r} \to y_{1s_r}$$

переводит 2-разметку μ'' в 2-разметку μ'.

Пусть теперь $k > 2$ и $y_{d_1j_1}, \ldots, y_{d_rj_r}$ — все метки, которые содержатся в k-разметке μ'', и удовлетворяют условию

$$\exists\, d < d_l : \ y_{d_lj_l} \text{ — содержится в разметке } \mu_d''.$$

Для каждого $l \in \{1, \ldots, r\}$ обозначим через d'_l наименьшее d с указанным свойством. Если $\mu''_{d'_l}(x_{i_1}^{(s_1)}) = y_{d_l j_1}$ — первое появления метки $y_{d_l j_l}$ в разметке $\mu''_{d'_l}$, то нетрудно понять, что в k-разметке μ'' отсутствуют метки $y_{d'_1 s_1}, \ldots, y_{d'_r s_r}$ и обратимая замена меток

$$y_{d_1 j_1} \to y_{d'_1 s_1}, \ \ldots \ , y_{d_r j_r} \to y_{d'_r s_r}$$

переводит k-разметку μ'' в k-разметку μ'. □

Замечание 3.3. Вообще говоря, свободное продолжение k-разметки можно определить не только последовательным и параллельным способами, но и любым «промежуточным» способом, использующим произвольную последовательность продолжения компонент k-разметки. В результате получится k-разметка, отличающаяся от последовательного (параллельного) свободного продолжения только обратимым переобозначением меток. Другими словами, главное в свободном продолжении k-разметки — это не порядок продолжения, а его «свобода» в каждый момент.

Пусть $\eta = (\eta_1, \ldots, \eta_k)$ и $\mu = (\mu_1, \ldots, \mu_k)$ — k-разметки сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ и для частичного отображения $\sigma_\mu \colon \mathbb{N} \to \mathbb{N}$ выполняются соотношения

$$\sigma_\mu \circ \eta_1 = \mu_1, \ldots, \sigma_\mu \circ \eta_k = \mu_k.$$

Будем обозначать это условие как $\sigma_\mu \colon \eta \to \mu$.

Определение 3.4. Правильную k-разметку η сети Σ с начальным условием $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ будем называть *свободной*, если для любой правильной k-разметки μ сети Σ начальным условием $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ существует отображение σ_μ, удовлетворяющее условию $\sigma_\mu \colon \eta \to \mu$.

Непосредственно из определения свободной k-разметки следует, что, при условии существования, свободная k-разметка сети Σ с начальным условием $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ определена однозначно с точностью до обратимого переобозначения меток.

Теорема 3.3. *Пусть k-разметка η получена в результате свободного продолжения начальной k-разметки*

$$\eta_1(x_1^{(0)}) = v_{11}, \ldots, \eta_1(x_n^{(0)}) = v_{1n}, \ \ldots \ , \eta_k(x_1^{(0)}) = v_{k1}, \ldots, \eta_k(x_n^{(0)}) = v_{kn}$$

и отображения $G\colon \varnothing \to \mathbb{N}$ *относительно сети* Σ. *Тогда* η *— свободная* k*-разметка сети* Σ *с начальным условием* $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$, *а* $\mathcal{Q}$*-отображение* $G_{\Sigma,\eta}$ *— её минимальное правило.*

Доказательство. Аналогично доказательству теоремы 1.6. □

Замечание 3.4. Поскольку свободная k-разметка сети Σ с начальным условием $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ определена однозначно с точностью до обратимого переобозначения меток, то, не ограничивая общности, будем полагать, что произвольная свободная k-разметка η сети Σ может быть получена при помощи параллельного (последовательного) свободного продолжения начальной k-разметки

$$\eta_1(x_1^{(0)}) = v_{11}, \ldots, \eta_1(x_n^{(0)}) = v_{1n}, \ \ldots \ , \eta_k(x_1^{(0)}) = v_{k1}, \ldots, \eta(x_n^{(0)}) = v_{kn}$$

и отображения $G\colon \varnothing \to \mathbb{N}$ относительно сети Σ.

Теорема 3.4. *Пусть* η *— свободная* k*-разметка сети* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$, μ *— правильная* k*-разметка сети* Σ, *и возможно определить отображение* σ_μ *по правилу:* $\sigma_\mu(\eta_d(x_i^{(0)})) = \mu_d(x_i^{(0)}),\ i \in \{1, \ldots, n\},\ d \in \{1, \ldots, k\}$. *Тогда отображение* σ_μ *допускает продолжение, удовлетворяющее условию* $\sigma_\mu\colon \eta \to \mu$.

Доказательство. Аналогично доказательству теоремы 1.7. □

Следствие 3.1. *В условиях теоремы 3.4 если* G *и* F *— минимальные правила* k*-разметок* η *и* μ *соответственно, то при всех допустимых* $z_i, z_j \in \mathbb{N}$ *выполняется равенство* $\sigma_\mu(G(z_i, z_j)) = F(\sigma_\mu(z_i), \sigma_\mu(z_j))$.

В заключение сформулируем и докажем одно простое утверждение, которое необходимо для лучшего понимания свободной k-разметки.

Утверждение 3.5. *Пусть* $\eta = (\eta_1, \ldots, \eta_k)$ *— свободная* k*-разметка сети* Σ *с начальным условием* $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$. *Тогда каждая из разметок* η_i, $i \in \{1, \ldots, k\}$ *является свободной разметкой сети* Σ *с начальным условием* $(v_{i1}, \ldots, v_{in})$.

Доказательство. Рассмотрим k-разметку $\mu = (\mu_1, \ldots, \mu_k)$ сети Σ, полученную в результате последовательного свободного продолжения начальной разметки

$$\mu_1(x_1^{(0)}) = v_{11}, \ldots, \mu_1(x_n^{(0)}) = v_{1n}, \ \ldots \ , \mu_k(x_1^{(0)}) = v_{k1}, \ldots, \mu_k(x_n^{(0)}) = v_{kn}.$$

и отображения $F\colon \varnothing \to \mathbb{N}$. Согласно определению процедуры последовательного свободного продолжения k-разметки, разметка μ_1 является свободной разметкой сети Σ с начальным условием $(v_{11}, \ldots, v_{1n})$. По определению свободной k-разметки, существует отображение σ_μ, удовлетворяющее условию $\sigma_\mu\colon \eta \to \mu$ и, в частности, отображение σ_μ удовлетворяет условию $\sigma_\mu\colon \eta_1 \to \mu_1$. Поскольку μ_1 — свободная разметка сети Σ с начальным условием $(v_{11}, \ldots, v_{1n})$, то нетрудно понять, что η_1 также является свободной разметкой сети Σ.

Аналогичным образом, с учетом замечания 3.3, доказывается, что разметки $\eta_2, \ldots, \eta_k$ являются свободными разметками сети Σ с начальными условиями $(v_{21}, \ldots, v_{2n}), \ldots, (v_{k1}, \ldots, v_{kn})$ соответственно. □

§3.2 k-транзитивность биективных сетей

Определение 3.5. k-разметку $\mu = (\mu_1, \ldots, \mu_k)$ сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ будем называть *k-разметкой сети Σ с ограничениями* $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$, если $\mu_1, \ldots, \mu_k$ — разметки сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ соответственно. При этом будем говорить, что сеть Σ *допускает* k-разметку μ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$.

Ограничения $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ k-разметки будем называть *невырожденными*, если наборы $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ — попарно различные и $(w_{11}, \ldots, w_{1n}), \ldots, (w_{k1}, \ldots, w_{kn})$ — попарно различные.

Замечание 3.5. Для правильной $k\mathcal{R}$-разметки $\mu = (\mu_1, \ldots, \mu_k)$ сети Σ невырожденность её ограничений $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ равносильна тому, что $\mu_1, \ldots, \mu_k$ — различные $\mathcal{R}$-разметки сети Σ.

Значение введенных понятий для построения $k\mathcal{R}$-транзитивных сетей раскрывается в следующих утверждениях.

Утверждение 3.6. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{B}^*$-биективная сеть ширины n. Тогда для любого множества Ω следующие утверждения эквивалентны:*

1. *сеть Σ является $k\mathcal{B}^*$-транзитивной для множества Ω;*
2. *сеть Σ допускает $k\mathcal{B}^*$-разметку элементами множества Ω при произвольных невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из множества Ω.*

Доказательство. Аналогично доказательству утверждения 2.2. □

Утверждение 3.7. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{Q}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого строго больше чем $k\|\Sigma\|$, следующие утверждения эквивалентны:*

1. *сеть Σ является $k\mathcal{Q}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $k\mathcal{Q}$-разметку элементами множества Ω при произвольных невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из множества Ω.*

Доказательство. Аналогично доказательству утверждения 2.3. □

Сформулированные в утверждениях 3.6 и 3.7 критерии $k\mathcal{R}$-транзитивности сети Σ для множества Ω в терминах существования $k\mathcal{R}$-разметок элементами множества Ω со всеми возможными невырожденными ограничениями из данного множества представляются достаточно трудными для проверки. Однако, при введении дополнительных ограничений на мощность множества Ω имеющиеся критерии $k\mathcal{R}$-транзитивности произвольной сети можно дополнить эквивалентной формулировкой, которая, как будет показано далее, допускает эффективную проверку. В следующем утверждении приводится универсальный критерий $k\mathcal{R}$-транзитивности сети в терминах наличия $k\mathcal{R}$-разметок.

Утверждение 3.8. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $k(t+n)$, следующие утверждения эквивалентны:*

1. *сеть* Σ *является* $k\mathcal{R}$*-транзитивной для множества* Ω*;*

2. *сеть* Σ *допускает* $k\mathcal{R}$*-разметку элементами множества* Ω *при произвольных невырожденных ограничениях* $\left(\begin{smallmatrix} v_{11} & \dots & v_{1n} \\ w_{11} & \dots & w_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} v_{k1} & \dots & v_{kn} \\ w_{k1} & \dots & w_{kn} \end{smallmatrix}\right)$ *из множества* Ω*;*

3. *сеть* Σ *допускает* $k\mathcal{R}$*-разметку при произвольных невырожденных ограничениях* $\left(\begin{smallmatrix} v_{11} & \dots & v_{1n} \\ w_{11} & \dots & w_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} v_{k1} & \dots & v_{kn} \\ w_{k1} & \dots & w_{kn} \end{smallmatrix}\right)$ *из множества* $\mathbb{N}$*.*

Теперь приступим к обоснованию того, что условие 3 из формулировки утверждения 3.8 можно проверять достаточно эффективным образом.

Для практического построения $k\mathcal{R}$-разметки с требуемыми ограничениями мы будем использовать процедуру $\mathcal{R}$-приведения. Во избежание путаницы опишем данную процедуру отдельным образом для случаев $\mathcal{R} = \mathcal{Q}$ и $\mathcal{R} = \mathcal{B}^*$.

Процедура $\mathcal{Q}$-приведения. Пусть $\eta^{(0)}$ — произвольная k-разметка $\mathcal{Q}$-биективной сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Если в отношении G_0, соответствующем k-разметке $\eta^{(0)}$, содержатся две тройки, отличающиеся только в одной координате, например (y_l, y_r, y_q) и $(y_l, y_r, y_{q'})$, то, заменив в k-разметке $\eta^{(0)}$ все метки $y_{q'}$ на y_q, получим k-разметку $\eta^{(1)}$, в которой используется на одну метку меньше, чем в разметке $\eta^{(0)}$. Если в отношении G_1, соответствующем k-разметке $\eta^{(1)}$, присутствуют две тройки, отличающиеся только в одной координате, то повторим описанные выше действия, и так далее.

Таким образом, построим последовательность k-разметок $\eta^{(0)}, \eta^{(1)}, \dots$ сети Σ, в которой каждая следующая k-разметка использует на одну метку меньше, чем предыдущая. Указанная последовательность k-разметок, очевидно, оборвётся на некотором конечном шаге с номером m в том смысле, что в отношении G_m, соответствующем k-разметке $\eta^{(m)}$, не найдётся двух троек, отличающихся только в одной координате. Построенная k-разметка $\eta^{(m)}$, очевидно, будет $k\mathcal{Q}$-разметкой сети Σ, а соответствующее $\mathcal{Q}$-отображение G_m — её минимальным правилом.

Описанную процедуру будем называть *$\mathcal{Q}$-приведением k-разметки* $\eta^{(0)}$. При этом будем говорить, что k-разметка $\eta^{(m)}$ *получена $\mathcal{Q}$-приведением k-разметки* $\eta^{(0)}$.

Процедура $\mathcal{B}^*$-приведения. Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{B}^*$-биективная сеть и $\eta^{(0)}$ — произвольная k-разметка сети Σ. Если в отношении G_0, соответствующем k-разметке $\eta^{(0)}$, содержатся две тройки (y_l, y_r, y_q) и (y_l, y'_r, y_q), отличающиеся только во второй координате, то заменим в k-разметке $\eta^{(0)}$ все метки y'_r на y_r; аналогичным образом, если в отношении G_0 содержатся две тройки (y_l, y_r, y_q) и (y_l, y_r, y'_q), отличающиеся только в третьей координате, то заменим в k-разметке $\eta^{(0)}$ все метки y'_q на y_q. В обоих случаях получим k-разметку $\eta^{(1)}$, в которой используется на одну метку меньше, чем в k-разметке $\eta^{(0)}$. Если в отношении G_1, соответствующем k-разметке $\eta^{(1)}$, присутствуют две тройки, отличающиеся только во второй или в третьей координате, то повторим описанные выше действия, и так далее.

Таким образом, построим последовательность k-разметок $\eta^{(0)}, \eta^{(1)}, \ldots$ сети Σ, в которой каждая следующая k-разметка использует на одну метку меньше, чем предыдущая. Указанная последовательность k-разметок, очевидно, оборвётся на некотором конечном шаге с номером m в том смысле, что в отношении G_m, соответствующем k-разметке $\eta^{(m)}$, не найдётся двух троек, отличающихся только во второй или только в третьей координате. Построенная k-разметка $\eta^{(m)}$, очевидно, будет $k\mathcal{B}^*$-разметкой сети Σ, а соответствующее $\mathcal{B}^*$-отображение G_m — её минимальным правилом.

Описанную процедуру будем называть *$\mathcal{B}^*$-приведением k-разметки $\eta^{(0)}$*. При этом будем говорить, что k-разметка $\eta^{(m)}$ *получена $\mathcal{B}^*$-приведением k-разметки $\eta^{(0)}$*.

Лемма 3.9. *Пусть $\eta^{(0)}$ — произвольная k-разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$, μ — $k\mathcal{R}$-разметка сети Σ, и существует отображение $\sigma_\mu \colon \eta^{(0)} \to \mu$. Тогда для любой k-разметки η, полученной $\mathcal{R}$-приведением k-разметки $\eta^{(0)}$, также выполняется условие $\sigma_\mu \colon \eta \to \mu$.*

Доказательство. Аналогично доказательству леммы 2.5. □

Следствие 3.2. *Пусть η_0 — произвольная k-разметка сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Тогда $k\mathcal{R}$-разметка η, полученная $\mathcal{R}$-приведением k-разметки η_0, определена однозначно с точностью до обратимого переобозначения меток.*

Доказательство. Аналогично доказательству следствия 2.1. □

Напомним, что, согласно утверждению 3.8, необходимым и достаточным условием для $k\mathcal{R}$-транзитивности $\mathcal{R}$-биективной сети Σ над достаточно большим множеством Ω является существование $k\mathcal{R}$-разметок сети Σ при всех возможных ограничениях из $\mathbb{N}$. Следующий результат предоставляет эффективный с теоретической точки зрения способ проверки указанного условия, который в дальнейшем будет доведен до достаточно эффективной с практической точки зрения реализации

Теорема 3.10. *Сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ допускает $k\mathcal{R}$-разметки при всех возможных невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из $\mathbb{N}$ в том и только в том случае, когда сеть Σ допускает $k\mathcal{R}$-разметки при всех возможных невырожденных ограничениях $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ из Ω_{k+1}.*

Доказательство. Необходимость очевидна, докажем достаточность.

Для удобства дальнейшего изложения будем считать, что

$$Y = \mathbb{N}\backslash\{v_{di}, w_{di}, \bar{v}_{di}, \bar{w}_{di} : d \in \{1, \ldots, k\},\ i \in \{1, \ldots, n\}\}.$$

Пусть свободная k-разметка $\eta^{(0)} = (\eta_1^{(0)}, \ldots, \eta_k^{(0)})$ сети Σ получена в результате свободного продолжения начальной k-разметки

$$\eta_1^{(0)}(x_1^{(0)}) = v_{11}, \ldots, \eta_1^{(0)}(x_n^{(0)}) = v_{1n},\ \ldots\ , \eta_k^{(0)}(x_1^{(0)}) = v_{k1}, \ldots, \eta_k^{(0)}(x_n^{(0)}) = v_{kn}$$

с использованием меток $y_{11}, \ldots, y_{k1}, y_{12}, \ldots, y_{k2}, \ldots\ldots$ из множества Y. Заменив в k-разметке $\eta^{(0)}$ метки

$$\eta_1^{(0)}(x_1^{(t)}), \ldots, \eta_1^{(0)}(x_n^{(t)}),\ \ldots\ , \eta_k^{(0)}(x_1^{(t)}), \ldots, \eta_k^{(0)}(x_n^{(t)})$$

на

$$w_{11}, \ldots, w_{1n},\ \ldots\ , w_{k1}, \ldots, w_{kn}$$

соответственно, получим k-разметку $\eta^{(1)}$ сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$. Проведём процедуру $\mathcal{R}$-приведения k-разметки $\eta^{(1)}$ с уточнениями:

- при отождествлении меток v_{di} и y_{sj} будем заменять метку y_{sj} на v_{di};

- при отождествлении меток w_{di} и y_{sj} будем заменять метку y_{sj} на w_{di}.

Пусть $\eta = (\eta_1, \ldots, \eta_k)$ — $k\mathcal{R}$-разметка сети Σ, полученная $\mathcal{R}$-приведением k-разметки $\eta^{(1)}$. Тогда, согласно сделанным уточнениям, все метки

$$\eta_d(x_i^{(0)}),\ \eta_d(x_i^{(t)}), \quad d \in \{1, \ldots, k\}, \quad i \in \{1, \ldots, n\}$$

содержатся в множестве

$$\{v_{di}, w_{di} : d \in \{1, \ldots, k\},\ i \in \{1, \ldots, n\}\},$$

но при этом в ограничениях разметки η могли появиться отождествления следующих типов:

1. $\eta_d(x_i^{(0)}) = v_{sj} \neq v_{di}$;
2. $\eta_d(x_i^{(0)}) = w_{sj} \neq v_{di}$;
3. $\eta_d(x_i^{(t)}) = v_{sj} \neq w_{di}$;
4. $\eta_d(x_i^{(t)}) = w_{sj} \neq w_{di}$.

Методом от противного покажем, что на самом деле $k\mathcal{R}$-разметка η будет иметь ограничения $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$. Для этого нам потребуется следующее вспомогательное утверждение.

Лемма 3.11. *Пусть* $\vec{v}_1 = (v_{11}, \ldots, v_{1n}), \ldots, \vec{v}_k = (v_{k1}, \ldots, v_{kn}) \in \mathbb{N}^n$ — *различные векторы и* $\vec{w}_1 = (w_{11}, \ldots, w_{1n}), \ldots, \vec{w}_k = (w_{k1}, \ldots, w_{kn}) \in \mathbb{N}^n$ — *различные векторы. Тогда существует такое отображение* $\sigma\colon \mathbb{N} \to \Omega_k$, *что*

$$\sigma(\vec{v}_1) = (\sigma(v_{11}), \ldots, \sigma(v_{1n})),\ \ldots\ , \sigma(\vec{v}_k) = (\sigma(v_{k1}), \ldots, \sigma(v_{kn}))\ \text{— различные,}$$

$$\sigma(\vec{w}_1) = (\sigma(w_{11}), \ldots, \sigma(w_{1n}))\,,\ \ldots\ , \sigma(\vec{w}_k) = (\sigma(w_{k1}), \ldots, \sigma(w_{kn}))\ \text{— различные.}$$

Доказательство. Не ограничивая общности, будем полагать, что ни один из элементов множества Ω_k не является координатой какого-либо из векторов $\vec{v}_1, \ldots, \vec{v}_k, \vec{w}_1, \ldots, \vec{w}_k$.

Докажем индукцией по $s \in \{1, \ldots, k\}$ существование отображений $\sigma_s\colon \mathbb{N} \to \Omega_s$, для которых

$$|\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}| \geqslant s \quad \text{и} \quad |\{\sigma_s(\vec{w}_1), \ldots, \sigma_s(\vec{w}_k)\}| \geqslant s.$$

База при $\sigma_1\colon \mathbb{N} \to \{1\}$ очевидна:

$$|\{\sigma_1(\vec{v}_1), \ldots, \sigma_1(\vec{v}_k)\}| = 1 \quad \text{и} \quad |\{\sigma_1(\vec{w}_1), \ldots, \sigma_1(\vec{w}_k)\}| = 1.$$

В предположении, что при $s < k$ построено отображение $\sigma_s\colon \mathbb{N} \to \Omega_s$, для которого

$$|\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}| \geqslant s \quad \text{и} \quad |\{\sigma_s(\vec{w}_1), \ldots, \sigma_s(\vec{w}_k)\}| \geqslant s,$$

докажем существование соответствующего отображения $\sigma_{s+1}\colon \mathbb{N} \to \Omega_{s+1}$. Рассмотрим возможные случаи.

Случай 1. Если $|\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}| > s$ и $|\{\sigma_s(\vec{w}_1), \ldots, \sigma_s(\vec{w}_k)\}| > s$, то $\sigma_{s+1} = \sigma_s$ — искомое отображение.

Случай 2. Если, не ограничивая общности, $|\{\sigma_s(\vec{w}_1), \ldots, \sigma_s(\vec{w}_k)\}| > s$ и $|\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}| = s$, то для удобства будем полагать, что $\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_s)$ — все различные элементы множества $\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}$ и $\sigma_s(\vec{v}_s) = \sigma_s(\vec{v}_{s+1})$. Поскольку $\vec{v}_s \neq \vec{v}_{s+1}$, то $v_{sj} \neq v_{s+1j}$ для некоторого $j \in \{1, \ldots, n\}$ и, полагая

$$\sigma_{s+1}(x) = \begin{cases} s+1, & \text{если } x = v_{s+1j}, \\ \sigma_s(x), & \text{если } x \neq v_{s+1j}, \end{cases}$$

получим, что множество $\{\sigma_{s+1}(\vec{v}_1), \ldots, \sigma_{s+1}(\vec{v}_k)\}$ содержит как минимум $s+1$ различных векторов — $\sigma_{s+1}(\vec{v}_1), \ldots, \sigma_{s+1}(\vec{v}_{s+1})$, и $|\{\sigma_{s+1}(\vec{w}_1), \ldots, \sigma_{s+1}(\vec{w}_k)\}| > s$. Таким образом, σ_{s+1} — искомое.

Случай 3. Если $|\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}| = |\{\sigma_s(\vec{w}_1), \ldots, \sigma_s(\vec{w}_k)\}| = s$ и существует такой $a \in \mathbb{N}$, при котором для отображения

$$\sigma_{s+1}(x) = \begin{cases} s+1, & \text{если } x = a, \\ \sigma_s(x), & \text{если } x \neq a \end{cases}$$

выполняются оба неравенства

$$|\{\sigma_{s+1}(\vec{v}_1), \ldots, \sigma_{s+1}(\vec{v}_k)\}| > |\{\sigma_s(\vec{v}_1), \ldots, \sigma_s(\vec{v}_k)\}| \geqslant s,$$
$$|\{\sigma_{s+1}(\vec{w}_1), \ldots, \sigma_{s+1}(\vec{w}_k)\}| > |\{\sigma_s(\vec{w}_1), \ldots, \sigma_s(\vec{w}_k)\}| \geqslant s,$$

то, очевидно, отображение σ_{s+1} является искомым.

Случай 4. Пусть $|\{\sigma_s(\vec{v}_1),\dots,\sigma_s(\vec{v}_k)\}| = |\{\sigma_s(\vec{w}_1),\dots,\sigma_s(\vec{w}_k)\}| = s$ и при любом $a \in \mathbb{N}$ для отображения

$$\sigma^a_{s+1}(x) = \begin{cases} s+1, & \text{если } x = a; \\ \sigma_s(x), & \text{если } x \neq a, \end{cases}$$

выполняется одно из равенств

$$|\{\sigma^a_{s+1}(\vec{v}_1),\dots,\sigma^a_{s+1}(\vec{v}_k)\}| = |\{\sigma_s(\vec{v}_1),\dots,\sigma_s(\vec{v}_k)\}|,$$
$$|\{\sigma^a_{s+1}(\vec{w}_1),\dots,\sigma^a_{s+1}(\vec{w}_k)\}| = |\{\sigma_s(\vec{w}_1),\dots,\sigma_s(\vec{w}_k)\}|.$$

Тогда, следуя рассуждениям, проведенным в случае 1, легко увидеть, что существуют $a, b \in \mathbb{N}$, для которых выполняются неравенства

$$|\{\sigma^a_{s+1}(\vec{v}_1),\dots,\sigma^a_{s+1}(\vec{v}_k)\}| > |\{\sigma_s(\vec{v}_1),\dots,\sigma_s(\vec{v}_k)\}|,$$
$$|\{\sigma^b_{s+1}(\vec{w}_1),\dots,\sigma^b_{s+1}(\vec{w}_k)\}| > |\{\sigma_s(\vec{w}_1),\dots,\sigma_s(\vec{w}_k)\}|.$$

В таком случае искомым является отображение

$$\sigma_{s+1}(x) = \begin{cases} s+1, & \text{если } x = a \text{ или } x = b; \\ \sigma_s(x), & \text{если } x \neq a, b, \end{cases}$$

для которого выполняются оба неравенства

$$|\{\sigma_{s+1}(\vec{v}_1),\dots,\sigma_{s+1}(\vec{v}_k)\}| > |\{\sigma_s(\vec{v}_1),\dots,\sigma_s(\vec{v}_k)\}| \geqslant s,$$
$$|\{\sigma_{s+1}(\vec{w}_1),\dots,\sigma_{s+1}(\vec{w}_k)\}| > |\{\sigma_s(\vec{w}_1),\dots,\sigma_s(\vec{w}_k)\}| \geqslant s.$$

Утверждение доказано методом математической индукции. □

Рассмотрим, не ограничивая общности, подслучай $\eta_1(x_i^{(0)}) = v_{sj} \neq v_{1i}$, относящийся к первому типу отождествлений. Согласно доказанной леммы 3.11, для любых невырожденных ограничений $\binom{v_{11}\ \dots\ v_{1n}}{w_{11}\ \dots\ w_{1n}}, \dots, \binom{v_{k1}\ \dots\ v_{kn}}{w_{k1}\ \dots\ w_{kn}}$ существует отображение $\sigma_\mu\colon \mathbb{N} \to \Omega_k$, при котором $\begin{pmatrix} \sigma_\mu(v_{11})\ \dots\ \sigma_\mu(v_{1n}) \\ \sigma_\mu(w_{11})\ \dots\ \sigma_\mu(w_{1n}) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_\mu(v_{k1})\ \dots\ \sigma_\mu(v_{kn}) \\ \sigma_\mu(w_{k1})\ \dots\ \sigma_\mu(w_{kn}) \end{pmatrix}$ — невырожденные ограничения из Ω_k. Если при этом $\sigma_\mu(v_{sj}) = \sigma_\mu(v_{1i})$, то переопределим σ_μ таким образом, что $\sigma_\mu(v_{1i}) = k+1$.

По условию теоремы существует $k\mathcal{R}$-разметка μ с ограничениями

$$\begin{pmatrix} \sigma_\mu(v_{11})\ \dots\ \sigma_\mu(v_{1n}) \\ \sigma_\mu(w_{11})\ \dots\ \sigma_\mu(w_{1n}) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_\mu(v_{k1})\ \dots\ \sigma_\mu(v_{kn}) \\ \sigma_\mu(w_{k1})\ \dots\ \sigma_\mu(w_{kn}) \end{pmatrix}$$

из Ω_{k+1} и по теореме 3.4 отображение σ_μ продолжается таким образом, что удовлетворяет условию $\sigma_\mu\colon \eta^{(0)} \to \mu$. Значит $\sigma_\mu\colon \eta^{(1)} \to \mu$ и $k\mathcal{R}$-разметка η, полученная в результате $\mathcal{R}$-приведения разметки $\eta^{(1)}$, согласно лемме 3.9, также удовлетворяет условию $\sigma_\mu\colon \eta \to \mu$ — получили противоречие:

$$\sigma_\mu(\eta_1(x_i^{(0)})) = \sigma_\mu(v_{1i}) = k+1 \neq \sigma_\mu(v_{sj}) = \sigma_\mu(\eta_s(x_j^{(0)})).$$

Отсутствие отождествлений остальных типов устанавливается аналогично. □

Теперь с учетом утверждения 3.8 легко вывести следующие критерии $k\mathcal{R}$-транзитивности сети.

Следствие 3.3. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $k(t+n)$, следующие утверждения эквивалентны:*

1. *сеть Σ является $k\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $k\mathcal{R}$-разметку элементами множества Ω при любых невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $k\mathcal{R}$-разметку элементами множества Ω при любых невырожденных ограничениях $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ из множества $\Omega_{k+1} \subset \Omega$;*
4. *множество преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$ действует k-транзитивным образом на подмножестве $\Omega_{k+1}^n \subset \Omega^n$.*

Для проведения дальнейших исследований в области $k\mathcal{R}$-транзитивности сетей нам потребуется следующий инструмент.

Определение 3.6. $k\mathcal{R}$-разметку η сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ будем называть *свободной $k\mathcal{R}$-разметкой сети Σ с ограничениями*, если для любой $k\mathcal{R}$-разметки μ сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ существует отображение $\sigma_\mu\colon \eta \to \mu$.

Из определения следует, что, при условии существования, свободная $k\mathcal{R}$-разметка сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \dots & v_{1n} \\ w_{11} & \dots & w_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} v_{k1} & \dots & v_{kn} \\ w_{k1} & \dots & w_{kn} \end{smallmatrix}\right)$ определена однозначно с точностью до обратимого переобозначения меток. Также отметим, что свободная $k\mathcal{R}$-разметка сети Σ с ограничениями является «свободной» только в классе $k\mathcal{R}$-разметок с теми же ограничениями, но не в классе всех правильных разметок.

Теорема 3.12. *Пусть $\mathcal{R}$-биективная сеть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ допускает $k\mathcal{R}$-разметку с ограничениями $\left(\begin{smallmatrix} v_{11} & \dots & v_{1n} \\ w_{11} & \dots & w_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} v_{k1} & \dots & v_{kn} \\ w_{k1} & \dots & w_{kn} \end{smallmatrix}\right)$. Тогда существует свободная $k\mathcal{R}$-разметка η сети Σ с указанными ограничениями.*

Если $k\mathcal{R}$-разметка μ сети Σ с ограничениями $\left(\begin{smallmatrix} \bar{v}_{11} & \dots & \bar{v}_{1n} \\ \bar{w}_{11} & \dots & \bar{w}_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} \bar{v}_{k1} & \dots & \bar{v}_{kn} \\ \bar{w}_{k1} & \dots & \bar{w}_{kn} \end{smallmatrix}\right)$ такова, что возможно определить отображение σ_μ:

$$\sigma_\mu(v_{di}) = \bar{v}_{di}, \quad \sigma_\mu(w_{di}) = \bar{w}_{di}, \quad d \in \{1, \dots, k\}, \quad i \in \{1, \dots, n\},$$

то указанное отображение σ_μ допускает продолжение, удовлетворяющее условию $\sigma_\mu \colon \eta \to \mu$.

Доказательство. Для удобства дальнейшего изложения будем считать, что

$$Y = \mathbb{N} \backslash \{v_{di}, w_{di}, \bar{v}_{di}, \bar{w}_{di} : d \in \{1, \dots, k\},\ i \in \{1, \dots, n\}\}.$$

Пусть свободная k-разметка $\eta^{(0)} = (\eta_1^{(0)}, \dots, \eta_k^{(0)})$ сети Σ получена в результате свободного продолжения начальной k-разметки

$$\eta_1^{(0)}(x_1^{(0)}) = v_{11}, \dots, \eta_1^{(0)}(x_n^{(0)}) = v_{1n},\ \dots\ , \eta_k^{(0)}(x_1^{(0)}) = v_{k1}, \dots, \eta_k^{(0)}(x_n^{(0)}) = v_{kn}$$

с использованием меток $y_{11}, \dots, y_{k1}, y_{12}, \dots, y_{k2}, \dots\dots$ из множества Y. Тогда, согласно определению свободной разметки, для любой правильной $k\mathcal{R}$-разметки ϑ с ограничениями $\left(\begin{smallmatrix} v_{11} & \dots & v_{1n} \\ w_{11} & \dots & w_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} v_{k1} & \dots & v_{kn} \\ w_{k1} & \dots & w_{kn} \end{smallmatrix}\right)$ существует отображение σ_ϑ, удовлетворяющее условию $\sigma_\vartheta \colon \eta^{(0)} \to \vartheta$. Заменим в k-разметке $\eta^{(0)}$ метки

$$\eta_1^{(0)}(x_1^{(t)}), \dots, \eta_1^{(0)}(x_n^{(t)}),\ \dots\ , \eta_k^{(0)}(x_1^{(t)}), \dots, \eta_k^{(0)}(x_n^{(t)})$$

на

$$w_{11}, \dots, w_{1n},\ \dots\ , w_{k1}, \dots, w_{kn}$$

соответственно и продолжим отображение σ_ϑ по правилу

$$\sigma_\vartheta(w_{di}) = w_{di}, \quad d \in \{1, \ldots, k\}, \quad i \in \{1, \ldots, n\}.$$

В результате выполнения перечисленных действий получим k-разметку $\eta^{(1)}$ сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ такую, что для любой $k\mathcal{R}$-разметки ϑ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ существует отображение σ_ϑ, удовлетворяющее условию $\sigma_\vartheta \colon \eta^{(1)} \to \vartheta$. Проведём процедуру $\mathcal{R}$-приведения $k\mathcal{R}$-разметки $\eta^{(1)}$ с уточнениями:

- при отождествлении меток v_{di} и y_{sj} будем заменять метку y_{sj} на v_{di};
- при отождествлении меток w_{di} и y_{sj} будем заменять метку y_{sj} на w_{di}.

Пусть $\eta = (\eta_1, \ldots, \eta_k)$ — $k\mathcal{R}$-разметка сети Σ, полученная $\mathcal{R}$-приведением k-разметки $\eta^{(1)}$. Тогда, согласно сделанным уточнениям, все метки

$$\eta_d(x_i^{(0)}),\ \eta_d(x_i^{(t)}), \quad d \in \{1, \ldots, k\}, \quad i \in \{1, \ldots, n\}$$

содержатся в множестве

$$\{v_{di}, w_{di} : d \in \{1, \ldots, k\},\ i \in \{1, \ldots, n\}\}$$

и при этом, согласно лемме 3.9, для любой $k\mathcal{R}$-разметки ϑ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ соответствующее отображение σ_ϑ удовлетворяет условию $\sigma_\vartheta \colon \eta \to \vartheta$. Таким образом, $k\mathcal{R}$-разметка η является свободной $k\mathcal{R}$-разметкой сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$.

Если μ — $k\mathcal{R}$-разметка с ограничениями $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$, при которых возможно определить отображение σ_μ по правилу

$$\sigma_\mu(v_{di}) = \bar{v}_{di}, \quad \sigma_\mu(w_{di}) = \bar{w}_{di}, \quad d \in \{1, \ldots, k\}, \quad i \in \{1, \ldots, n\},$$

то, согласно теореме 3.4, указанное отображение σ_μ продолжается таким образом, что удовлетворяет условию $\sigma_\mu \colon \eta^{(0)} \to \mu$. При замене в k-разметке $\eta^{(0)}$ меток $\eta_1^{(0)}(x_1^{(t)}), \ldots\ldots, \eta_k^{(0)}(x_n^{(t)})$ на $w_{11}, \ldots\ldots, w_{kn}$ соответственно, получается k-разметка $\eta^{(1)}$ сети Σ с ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$, для которой выполняется условие $\sigma_\mu \colon \eta^{(1)} \to \mu$. Согласно лемме 3.9, $k\mathcal{R}$-разметка η, полученная в результате $\mathcal{R}$-приведения разметки $\eta^{(1)}$, также удовлетворяет требуемому условию $\sigma_\mu \colon \eta \to \mu$. $\square$

Следствие 3.4. *В условиях теоремы 3.12, если G и F — минимальные правила k-разметок η и μ соответственно, то при всех допустимых $z_i, z_j \in \mathbb{N}$ выполняется равенство $\sigma_\mu(G(z_i, z_j)) = F(\sigma_\mu(z_i), \sigma_\mu(z_j))$.*

Теорема 3.12 позволяет дополнить ряд критериев $k\mathcal{R}$-транзитивности сети Σ, перечисленных в следствии 3.3, еще одним утверждением, которое, очевидно, допускает достаточно эффективную проверку.

Следствие 3.5. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда для любого множества Ω, мощность которого не менее чем $k(t+n)$, следующие утверждения эквивалентны:*

1. *сеть Σ является $k\mathcal{R}$-транзитивной для множества Ω;*
2. *сеть Σ допускает $k\mathcal{R}$-разметку элементами множества Ω при любых невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из множества Ω;*
3. *сеть Σ допускает $k\mathcal{R}$-разметку элементами множества Ω при любых невырожденных ограничениях $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ из множества $\Omega_{k+1} \subset \Omega$;*
4. *сеть Σ допускает свободную $k\mathcal{R}$-разметку элементами множества $\mathbb{N}$ при любых невырожденных ограничениях $\left(\begin{smallmatrix} \bar{v}_{11} & \ldots & \bar{v}_{1n} \\ \bar{w}_{11} & \ldots & \bar{w}_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} \bar{v}_{k1} & \ldots & \bar{v}_{kn} \\ \bar{w}_{k1} & \ldots & \bar{w}_{kn} \end{smallmatrix}\right)$ из множества Ω_{k+1}.*

Замечание 3.6. Доказательство теоремы 3.12 конструктивно и предоставляет полиномиальный по сложности ($\mathcal{O}(k^3t^3)$) способ построения свободной $k\mathcal{R}$-разметки с требуемыми ограничениями. Таким образом, общую сложность проверки критерия из пункта 4 следствия 3.5 можно оценить величиной $\mathcal{O}(k^{2kn+3} \cdot t^3)$.

В дальнейшем нам потребуются следующее естественное обобщение понятия свободной $k\mathcal{R}$-разметки с ограничениями и соответствующие результаты.

Определение 3.7. Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть. Тогда $k\mathcal{R}$-разметку $\eta = (\eta_1, \ldots, \eta_k)$ сети Σ будем называть *свободной $k\mathcal{R}$-разметкой*

сети Σ *с условиями*

$$\eta_d(x_1^{(0)}) = v_{d1}, \ldots, \eta_d(x_n^{(0)}) = v_{dn}, \quad d \in \{1, \ldots, k\},$$
$$\eta_d(x_{i_1}^{(t)}) = w_{di_1}, \ldots, \eta_d(x_{i_s}^{(t)}) = w_{di_s}, \quad d \in \{1, \ldots, k\},$$

если для любой $k\mathcal{R}$-разметки $\mu = (\mu_1, \ldots, \mu_k)$ сети Σ с аналогичными условиями

$$\mu_d(x_1^{(0)}) = v_{d1}, \ldots, \mu_d(x_n^{(0)}) = v_{dn}, \quad d \in \{1, \ldots, k\},$$
$$\mu_d(x_{i_1}^{(t)}) = w_{di_1}, \ldots, \mu_d(x_{i_s}^{(t)}) = w_{di_s}, \quad d \in \{1, \ldots, k\},$$

существует такое отображение σ_μ, что $\sigma_\mu \colon \eta \to \mu$.

Теорема 3.13. *Если существует* $k\mathcal{R}$*-разметка* $\vartheta = (\vartheta_1, \ldots, \vartheta_k)$ $\mathcal{R}$*-биективной сети* $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ *с условиями*

$$\vartheta_d(x_1^{(0)}) = v_{d1}, \ldots, \vartheta_d(x_n^{(0)}) = v_{dn}, \quad d \in \{1, \ldots, k\},$$
$$\vartheta_d(x_{i_1}^{(t)}) = w_{di_1}, \ldots, \vartheta_d(x_{i_s}^{(t)}) = w_{di_s}, \quad d \in \{1, \ldots, k\},$$

то существует единственная, с точностью до переобозначений, свободная $k\mathcal{R}$*-разметка* $\eta = (\eta_1, \ldots, \eta_k)$ *сети* Σ *с аналогичными условиями*

$$\eta_d(x_1^{(0)}) = v_{d1}, \ldots, \eta_d(x_n^{(0)}) = v_{dn}, \quad d \in \{1, \ldots, k\},$$
$$\eta_d(x_{i_1}^{(t)}) = w_{di_1}, \ldots, \eta_d(x_{i_s}^{(t)}) = w_{di_s}, \quad d \in \{1, \ldots, k\}.$$

Если для $k\mathcal{R}$*-разметки* $\mu = (\mu_1, \ldots, \mu_k)$ *сети* Σ *с условиями*

$$\mu_d(x_1^{(0)}) = \bar{v}_{d1}, \ldots, \mu_d(x_n^{(0)}) = \bar{v}_{dn}, \quad d \in \{1, \ldots, k\},$$
$$\mu_d(x_{i_1}^{(t)}) = \bar{w}_{di_1}, \ldots, \mu_d(x_{i_s}^{(t)}) = \bar{w}_{di_s}, \quad d \in \{1, \ldots, k\}.$$

возможно определить отображение σ_μ*:*

$$\sigma_\mu(v_{di}) = \bar{v}_{di}, \quad \sigma_\mu(w_{di}) = \bar{w}_{di}, \quad d \in \{1, \ldots, k\}, \quad i \in \{1, \ldots, n\},$$

то указанное отображение σ_μ *допускает продолжение, удовлетворяющее условию* $\sigma_\mu \colon \eta \to \mu$.

Следствие 3.6. *В условиях теоремы 3.13, если G и F — минимальные правила $k\mathcal{R}$-разметок η и μ соответственно, то при всех допустимых $z_i, z_j \in \mathbb{N}$ выполняется равенство $\sigma_\mu(G(z_i, z_j)) = F(\sigma_\mu(z_i), \sigma_\mu(z_j))$.*

В частности, если метка $\mu_r(x_i^{(s)})$ не является координатой какого-либо набора из области определения F, то метка $\eta_r(x_i^{(s)})$ не является координатой какого-либо набора из области определения G.

§3.3 Построение k-транзитивных сетей

Не ограничивая общности, всюду далее в этом параграфе будем считать, что произвольная $\mathcal{R}$-биективная сеть Σ задается своим каноническим представлением

$$(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$$

с множеством вершин $X_0 \cup X_{11} \cup \ldots \cup X_{1k_1} \cup \ldots \cup X_{n1} \cup \ldots \cup X_{nk_n}$.

В данном параграфе предлагается универсальный алгоритм модификации канонического представления произвольной $\mathcal{R}$-биективной сети, в результате работы которого получается $\mathcal{R}$-биективная сеть, действующая $k\mathcal{R}$-транзитивным образом для всех достаточно больших множеств. Универсальность предлагаемого алгоритма построения $k\mathcal{R}$-транзитивной сети основана на большом «запасе прочности» по отношению к используемому множеству бинарных операций, который во многом обеспечивается специфическими конструкциями первого и последнего слоев.

Алгоритм 3. (построение $k\mathcal{R}$-транзитивной сети)
Вход: произвольная $\mathcal{R}$-биективная сеть Σ в каноническом представлении

$$\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n}).$$

Не ограничивая общности, будем считать, что 1-й слой имеет вид

$$\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1} = \Sigma_{11} \cdot \ldots \cdot \Sigma_{1l} \cdot \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \ldots \cdot \Sigma_1^{(2,1)},$$

а в противном случае приведем его к такому виду, добавив не более $2(n-1)$ соответствующих элементарных сетей.

Шаг $s \in \{1, \ldots, n-1\}$**.** Пусть первые $s-1$ слоев канонического представления сети Σ уже модифицированы

$$\widehat{\Sigma}_{s-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}),$$

и μ — свободная $\mathcal{R}$-разметка сети $\widehat{\Sigma}_{s-1}$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \mu(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = v.$$

Продолжим $\mathcal{R}$-разметку μ сети $\widehat{\Sigma}_{s-1}$ свободным образом до $\mathcal{R}$-разметки сети

$$\widehat{\Sigma}'_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s})$$

и выберем такую вершину $x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$, $j \in \{s, \ldots, n\}$, у которой метка $\mu(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)})$ не является координатой какого-либо набора из области определения $F_{\widehat{\Sigma}'_s}$ — минимального правила разметки μ сети $\widehat{\Sigma}'_s$.

Если $s \leqslant n-2$ **и** $j = s$**, то** выбираем произвольный $m \in \{s+1, \ldots, n\}$ и модифицируем s-й слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ следующим образом:

$$\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s} = \Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s} \cdot \Sigma_m^{(s,m)} \cdot \Sigma_s^{(m,s)} \cdot \Sigma_m^{(s,m)}.$$

Если $s \leqslant n-2$ **и** $j \neq s$**, то** выбираем произвольный $m \in \{s+1, \ldots, n\}$, $m \neq j$ и модифицируем s-й слой $\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s}$ следующим образом:

$$\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s} = \Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s} \cdot \Sigma_s^{(j,s)} \cdot \Sigma_m^{(s,m)} \cdot \Sigma_s^{(j,s)}.$$

Если $s = n-1$**, то** модифицируем $(n-1)$-й слой $\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}}$ следующим образом:

$$\begin{aligned}&\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}} = \\ =&\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}} \cdot (\Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \Sigma_{n-1}^{(n,n-1)}) \cdot (\Sigma_n^{(n-1,n)} \cdot \ldots \cdot \Sigma_n^{(1,n)}).\end{aligned}$$

Выход: $(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots\ldots \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$ — каноническое представление $\mathcal{R}$-биективной сети $\widehat{\Sigma}$, сложности не более чем $\|\Sigma\| + 6n - 6$.

Теорема 3.14. *Пусть* $\Sigma = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}) \cdot \ldots\ldots \cdot (\Sigma_{n1} \cdot \ldots \cdot \Sigma_{nk_n})$ *— произвольная* $\mathcal{R}$*-биективная сеть ширины* n*. Тогда её модификация* $\widehat{\Sigma}$ *является* $k\mathcal{R}$*-транзитивной для любого множества* Ω*, мощность которого не менее чем* $k\,(\|\Sigma\| + 7n - 6)$*.*

Доказательство. Всюду далее будем полагать, что каждая свободная $k\mathcal{R}$-разметка получена параллельным свободным продолжением соответствующих начальных условий с использованием множеств меток

$$Y_1 = \{y_{11}, y_{12}, \dots\},\ \dots\ , Y_k = \{y_{k1}, y_{k2}, \dots\}.$$

Для доказательства корректности действий, выполняемых на шаге 1, нам потребуется следующий вспомогательный результат.

Лемма 3.15. *Для любой свободной k-разметки $\eta = (\eta_1, \dots, \eta_k)$ сети*

$$\widehat{\Sigma}'_1 = \Sigma_{11} \cdot \ldots \cdot \Sigma_{1l} \cdot \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \ldots \cdot \Sigma_1^{(2,1)}$$

с невырожденными начальными условиями $(v_{11}, \dots, v_{1n}), \dots, (v_{21}, \dots, v_{2n})$ справедливы утверждения:

1. $\eta_1(x_1^{(k_1)}), \dots, \eta_1(x_n^{(k_1)}) \in Y_1,\ \dots\ , \eta_k(x_1^{(k_1)}), \dots, \eta_k(x_n^{(k_1)}) \in Y_k$;
2. *метки $\eta_1(x_1^{(k_1)}), \dots, \eta_k(x_1^{(k_1)})$ (и только они), независимо от условий $(v_{11}, \dots, v_{1n}), \dots, (v_{k1}, \dots, v_{kn})$, не являются координатами какого-либо набора из области определения $G_{\widehat{\Sigma}'_1}$ — минимального правила k-разметки η.*

Доказательство. Введём понятие уровня метки в свободной k-разметке η произвольной сети $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$. Для каждой метки

$$\eta_d(x_i^{(0)}),\ i \in \{1, \dots, n\},\ d \in \{1, \dots, k\}$$

уровень $h(\eta_d(x_i^{(0)}))$ полагаем равным нулю. Если метка z_s удовлетворяет соотношению $G_\Sigma(z_l, z_r) = z_s$ для минимального правила G_Σ k-разметки η сети Σ, то полагаем $h(z_s) = \max\{h(z_l), h(z_r)\}+1$. Такое определение корректно, поскольку минимальное правило G_Σ свободной k-разметки η удовлетворяет условию

$$(G_{\Sigma,\eta}(z_1, z_2) = G_{\Sigma,\eta}(z_3, z_4)) \Longrightarrow ((z_1, z_2) = (z_3, z_4)) \tag{3.1}$$

при всех допустимых $z_1, z_2, z_3, z_4 \in \mathbb{N}$.

Индукцией по длине произведения элементарных сетей $\Sigma_1 \cdot \ldots \cdot \Sigma_t$ нетрудно показать, что для любой вершины $x_i^{(s)}$ сети Σ уровни меток $\eta_1(x_i^{(s)}), \dots, \eta_k(x_i^{(s)})$ совпадают.

Пусть η — свободная k-разметка сети

$$\Sigma_{11} \cdot \ldots \cdot \Sigma_{1l} \cdot \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)},$$

полученная в результате параллельного свободного продолжения начальных невырожденных условий $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ с использованием набора множеств $Y_1 = \{y_{11}, y_{12}, \ldots\}, \ \ldots \ , Y_k = \{y_{k1}, y_{k2}, \ldots\}$. Легко видеть, что в k-разметке η ровно k меток имеют максимальный уровень:

$$\eta_1(x_n^{(l+n-1)}), \ldots, \eta_k(x_n^{(l+n-1)}).$$

Из максимальности уровня следует, что каждая из перечисленных меток не содержится в области определения минимального правила k-разметки η.

Предположим, что $\eta_d(x_n^{(l+n-1)}) \in Y_{d'}$ для некоторых $d \neq d'$. Тогда, согласно построению, метка $\eta_d(x_n^{(l+n-1)})$ впервые появилась в разметке $\eta_{d'}$ и, следовательно, в силу максимальности её уровня, должна совпадать единственно с $\eta_{d'}(x_n^{(l+n-1)})$. Но в таком случае, пользуясь конструктивной особенностью (3.1) свободной k-разметки, нетрудно показать совпадение

$$\eta_d(x_1^{(l)}) = \eta_{d'}(x_1^{(l)}), \ldots, \eta_d(x_n^{(l)}) = \eta_{d'}(x_n^{(l)}),$$

которое противоречит начальным условиям $(v_{d1}, \ldots, v_{dn}) \neq (v_{d'1}, \ldots, v_{d'n})$ при $d \neq d'$. Таким образом, $\eta_1(x_n^{(l+n-1)}) \in Y_1, \ldots, \eta_k(x_n^{(l+n-1)}) \in Y_k$.

По построению каждая из меток $\eta_1(x_n^{(l+n-1)}), \ldots, \eta_k(x_n^{(l+n-1)})$ не является координатой какого-либо набора из области определения минимального правила k-разметки η. Поэтому при продолжении свободной k-разметки η свободным образом (с использованием набора множеств $Y_1, \ldots, Y_k$) до свободной разметки сети

$$\widehat{\Sigma}_1' = \Sigma_{11} \cdot \ldots \cdot \Sigma_{1l} \cdot \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \ldots \cdot \Sigma_1^{(2,1)}$$

будут выполнены следующие условия:

1. $\eta_1(x_1^{(k_1)}), \ldots, \eta_1(x_n^{(k_1)}) \in Y_1, \ \ldots \ , \eta_k(x_1^{(k_1)}), \ldots, \eta_k(x_n^{(k_1)}) \in Y_k$;
2. метки $\eta_1(x_1^{(k_1)}), \ldots, \eta_k(x_1^{(k_1)})$ (и только они), независимо от условий $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$, не являются координатами какого-либо набора из области определения $G_{\widehat{\Sigma}_1'}$ — минимального правила k-разметки η.

Лемма доказана. □

Корректность действий, выполняемых на шаге с номером 1.

Ввиду леммы 3.15, для свободной разметки μ сети $\widehat{\Sigma}'_1 = \Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}$ с начальным условием $(v, \ldots, v)$ метка $\mu(x_1^{(k_1)})$ (и только она) не является координатой какого-либо набора из области определения $F_{\widehat{\Sigma}'_1}$ — минимального правила разметки μ и на шаге 1 произойдет модификация слоя $\widehat{\Sigma}'_1 = \Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1}$ до сети $\widehat{\Sigma}_1 = \Sigma_{11} \cdot \ldots \cdot \Sigma_{1k_1} \cdot \Sigma_m^{(1,m)} \cdot \Sigma_1^{(m,1)} \cdot \Sigma_m^{(1,m)}$. Теперь остается заметить, что свободная k-разметка η сети $\widehat{\Sigma}'_1$ с начальными условиями $(v_{11}, \ldots, v_{1n}), \ldots, (v_{k1}, \ldots, v_{kn})$ свободным образом без отождествлений продолжается до свободной k-разметки η сети $\widehat{\Sigma}_1$ с любыми условиями $\eta_1(x_1^{(\widehat{k}_1)}) = w_{11}, \ldots, \eta_k(x_1^{(\widehat{k}_1)}) = w_{k1}$ и при этом:

1. $\eta_1(x_2^{(\widehat{k}_1)}), \ldots, \eta_1(x_n^{(\widehat{k}_1)}) \in Y_1, \ \ldots \ , \eta_k(x_2^{(\widehat{k}_1)}), \ldots, \eta_k(x_n^{(\widehat{k}_1)}) \in Y_k$;
2. метки $\eta_1(x_m^{(\widehat{k}_1)}), \ldots, \eta_k(x_m^{(\widehat{k}_1)})$, независимо от начальных условий, не являются координатами какого-либо набора из области определения $G_{\widehat{\Sigma}_1}$ — минимального правила k-разметки η сети $\widehat{\Sigma}_1$.

Корректность действий, выполняемых на шаге с номером $2 \leqslant s \leqslant n-2$.

Пусть первые $s-1$ слоёв канонического представления сети Σ уже модифицированы таким образом, что сеть

$$\widehat{\Sigma}_{s-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}})$$

допускает свободную k-разметку $\eta = (\eta_1, \ldots, \eta_k)$ при любых условиях

$$\eta_d(x_1^{(0)}) = v_{d1}, \ldots, \eta_d(x_n^{(0)}) = v_{dn}, \ d \in \{1, \ldots, k\} \tag{3.2}$$

$$\eta_d(x_1^{(\widehat{k}_1)}) = w_{d1}, \ldots, \eta_d(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = w_{ds-1}, \ d \in \{1, \ldots, k\} \tag{3.3}$$

и при этом:

1. $\eta_d(x_s^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}), \ldots, \eta_d(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) \in Y_d, \ d \in \{1, \ldots, k\}$;
2. среди $x_s^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}, \ldots, x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}$ существует вершина $x_m^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}$, для которой каждая из меток $\eta_d(x_m^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})})$, $d \in \{1, \ldots, k\}$, независимо от условий (3.2) и (3.3), не является координатой какого-либо набора из области определения $G_{\widehat{\Sigma}_{s-1}}$ — минимального правила k-разметки η сети $\widehat{\Sigma}_{s-1}$.

Тогда для свободной разметки μ сети $\widehat{\Sigma}_{s-1}$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \mu(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = v$$

метка $\mu(x_m^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})})$ также не содержится в области определения минимального правила $F_{\widehat{\Sigma}_{s-1}}$ и при продолжении разметки μ сети $\widehat{\Sigma}_{s-1}$ свободным образом до разметки сети

$$\widehat{\Sigma}'_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{sk_s})$$

среди вершин $x_s^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}, \ldots, x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$, согласно лемме 2.11, существует такая вершина $x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}$, что метка $\mu(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)})$ не содержится в области определения $F_{\widehat{\Sigma}'_s}$ — минимального правила разметки μ сети $\widehat{\Sigma}'_s$. Поскольку разметка μ по построению является свободной разметкой сети $\widehat{\Sigma}'_s$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \mu(x_{s-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})}) = v,$$

то, согласно следствию 3.6, для свободного продолжения свободной k-разметки η сети $\widehat{\Sigma}'_s$ с условиями (3.2) и (3.3) выполнены следующие условия:

1. $\eta_d(x_s^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}), \ldots, \eta_d(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}) \in Y_d,\ d \in \{1, \ldots, k\}$;
2. метки $\eta_1(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)}), \ldots, \eta_k(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1}+k_s)})$, независимо от условий (3.2) и (3.3), не являются координатами какого-либо набора из области определения $G_{\widehat{\Sigma}'_s}$ — минимального правила k-разметки η сети $\widehat{\Sigma}'_s$.

В каждом из возможных вариантов модификации сети $\widehat{\Sigma}'_s$ свободная k-разметка η сети $\widehat{\Sigma}'_s$ с условиями (3.2) и (3.3) свободным образом без отождествлений продолжается до свободной k-разметки η сети

$$\widehat{\Sigma}_s = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(s-1)1} \cdot \ldots \cdot \Sigma_{(s-1)\widehat{k}_{s-1}}) \cdot (\Sigma_{s1} \cdot \ldots \cdot \Sigma_{s\widehat{k}_s})$$

с любыми условиями $\eta_d(x_s^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) = w_{ds},\ d \in \{1, \ldots, k\}$ и при этом:

1. $\eta_d(x_{s+1}^{(\widehat{k}_1+\ldots+\widehat{k}_s)}), \ldots, \eta_d(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) \in Y_d,\ d \in \{1, \ldots, k\}$;
2. каждая из меток $\eta_d(x_m^{(\widehat{k}_1+\ldots+\widehat{k}_s)}),\ d \in \{1, \ldots, k\}$, независимо от условий $\eta_d(x_s^{(\widehat{k}_1+\ldots+\widehat{k}_s)}) = w_{ds},\ d \in \{1, \ldots, k\}$ не является координатой какого-либо набора из области определения $G_{\widehat{\Sigma}_s}$ — минимального правила k-разметки η сети $\widehat{\Sigma}_s$.

Корректность действий, выполняемых на шаге с номером $n-1$.

Пусть первые $n-2$ слоя канонического представления сети Σ уже модифицированы таким образом, что сеть

$$\widehat{\Sigma}_{n-2} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-2)1} \cdot \ldots \cdot \Sigma_{(n-2)\widehat{k}_{n-2}}),$$

допускает свободную k-разметку $\eta = (\eta_1, \ldots, \eta_k)$ при любых условиях

$$\eta_d(x_1^{(0)}) = v_{d1}, \ldots, \ \eta_d(x_n^{(0)}) = v_{dn}, \ d \in \{1, \ldots, k\}, \tag{3.4}$$

$$\eta_d(x_1^{(\widehat{k}_1)}) = w_{d1}, \ldots, \ \eta_d(x_{n-2}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}) = w_{dn-2}, \ d \in \{1, \ldots, k\} \tag{3.5}$$

и при этом

1. $\eta_d(x_{n-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}), \eta_d(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}) \in Y_d, \ d \in \{1, \ldots, k\}$;
2. среди $x_{n-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}, x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}$ существует вершина $x_m^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}$, для которой каждая из меток $\eta_d(x_m^{(\widehat{k}_1+\ldots+\widehat{k}_{s-1})})$, $d \in \{1, \ldots, k\}$, независимо от условий (3.4) и (3.5), не является координатой какого-либо набора из области определения $G_{\widehat{\Sigma}_{n-2}}$ — минимального правила k-разметки η сети $\widehat{\Sigma}_{n-2}$.

Тогда для свободной разметки μ сети $\widehat{\Sigma}_{n-2}$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \ \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \ \mu(x_{n-2}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}) = v,$$

метка $\mu(x_m^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})})$ также не содержится в области определения минимального правила $F_{\widehat{\Sigma}_{n-2}}$ и при продолжении разметки μ сети $\widehat{\Sigma}_{n-2}$ свободным образом до разметки сети

$$\widehat{\Sigma}'_{n-1} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-2)1} \cdot \ldots \cdot \Sigma_{(n-2)\widehat{k}_{n-2}}) \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)k_{n-1}}),$$

согласно лемме 2.11, среди вершин $x_{n-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1})}, x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1})}$ существует такая вершина $x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1})}$, что метка $\mu(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1})})$ не содержится в области определения минимального правила $F_{\widehat{\Sigma}'_{n-1}}$. Поскольку разметка μ по построению является свободной разметкой сети $\widehat{\Sigma}'_{n-1}$ с условиями

$$\mu(x_1^{(0)}) = v, \ldots, \ \mu(x_n^{(0)}) = v, \quad \mu(x_1^{(\widehat{k}_1)}) = v, \ldots, \ \mu(x_{n-2}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2})}) = v,$$

то, согласно следствию 3.6, для свободного продолжения свободной k-разметки η сети $\widehat{\Sigma}'_{n-1}$ с условиями (3.4) и (3.5) выполнены следующие условия:

1. $\eta_d(x_{n-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-1}+k_{n-1})}), \eta_d(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1})}) \in Y_d,\ d \in \{1,\ldots,k\}$;
2. метки $\eta_d(x_j^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1})}),\ d \in \{1,\ldots,k\}$, независимо от условий (3.4) и (3.5), не являются координатами какого-либо набора из области определения $G_{\widehat{\Sigma}'_{n-1}}$ — минимального правила k-разметки η сети $\widehat{\Sigma}'_{n-1}$.

Остается заметить, что свободная k-разметка η сети $\widehat{\Sigma}'_{n-1}$ с условиями (3.4) и (3.5) свободным образом продолжается до свободной k-разметки η сети

$$\widehat{\Sigma} = (\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-2)1} \cdot \ldots \cdot \Sigma_{(n-2)\widehat{k}_{n-2}}) \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$$

с произвольными условиями $\eta_d(x_{n-1}^{(\widehat{k}_1+\ldots+\widehat{k}_{n-1})}) = w_{dn-1},\ d \in \{1,\ldots,k\}$, а последующая замена всех меток $\eta_1(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-1})}), \ldots, \eta_k(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-1})})$, соответственно, на $w_{1n}, \ldots, w_{kn}$ не может привести к отождествлению меток

$$\eta_1(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1}+2)}) \in Y_1, \ldots, \eta_k(x_n^{(\widehat{k}_1+\ldots+\widehat{k}_{n-2}+k_{n-1}+2)}) \in Y_k,$$

при условии, что $(w_{11}, \ldots, w_{1n}), \ldots, (w_{k1}, \ldots, w_{kn})$ — попарно различны.

Результат работы алгоритма.

Таким образом, в результате работы алгоритма каноническое представление исходной сети Σ модифицируется до канонического представления

$$(\Sigma_{11} \cdot \ldots \cdot \Sigma_{1\widehat{k}_1}) \cdot \ldots \cdot (\Sigma_{(n-1)1} \cdot \ldots \cdot \Sigma_{(n-1)\widehat{k}_{n-1}})$$

новой $\mathcal{R}$-биективной сети $\widehat{\Sigma}$, сложность которой не более чем $\|\Sigma\|+6n-6$. Кроме того, показано, что построенная сеть $\widehat{\Sigma}$ допускает $k\mathcal{R}$-разметку при произвольных невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из $\mathbb{N}$. Поскольку $\|\widehat{\Sigma}\| \leqslant \|\Sigma\| + 6n - 6$, то для проведения $k\mathcal{R}$-разметки сети $\widehat{\Sigma}$ при произвольных невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из $\mathbb{N}$ требуется не более чем $k(\|\Sigma\| + 6n - 6 + n)$ различных меток. Значит, при выборе любого множества Ω мощности не менее чем $k\,(\|\Sigma\| + 7n - 6)$, можно считать, что сеть $\widehat{\Sigma}$ допускает $k\mathcal{R}$-разметку элементами множества Ω при произвольных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из Ω, что, согласно утверждению 3.8, равносильно $k\mathcal{R}$-транзитивности сети $\widehat{\Sigma}$ для множества Ω. $\square$

Следствие 3.7. *Для любого $n \geqslant 2$ существует $\mathcal{R}$-биективная сеть $\widehat{\Sigma}$ ширины n и веса $6n-6$, которая $k\mathcal{R}$-транзитивна для любого множества мощности не менее чем $k(7n-6)$.*

Замечание 3.7. Рассмотренный алгоритм построения $k\mathcal{R}$-транзитивной сети является «жестким» по структуре выполняемых действий, но не по их содержанию — добавляемые на промежуточных шагах элементарные сети можно выбирать различными способами (см. например [62]), что особенно важно при использовании данного алгоритма для построения $k\mathcal{Q}$-транзитивных сетей. Другими словами, предложенный алгоритм стоит рассматривать как общую схему, на основе которой можно сконфигурировать целое семейство алгоритмов построения $k\mathcal{R}$-транзитивных сетей примерно одинаковой «архитектуры», но с различными «оттенками» содержимого.

Рассмотренный алгоритм построения $k\mathcal{R}$-транзитивной сети позволяет создавать $k\mathcal{R}$-транзитивные сети ширины n достаточно малого веса $6n-6$. Более того, использующиеся в данном алгоритме идеи позволяют построить $k\mathcal{R}$-транзитивную сеть ширины еще меньшего веса $4n-4$, которая, в свою очередь, может быть использована для эффективного построения широкого класса $k\mathcal{R}$-транзитивных сетей. Здесь стоит отметить, что произвольная $k\mathcal{R}$-транзитивная сеть не может иметь вес менее $2n-2$ поскольку первый слой ее канонического разложения не может иметь вес менее $n-1$, а последующие $n-1$ слоев, очевидно, не могут быть пустыми. Однако, вопрос о более точной нижней оценке веса произвольной $k\mathcal{R}$-транзитивной сети на данный момент является открытым (до сих пор даже не удалось построить примера $k\mathcal{R}$-транзитивной сети веса менее чем $4n-4$).

Пример 3.1. Рассмотрим $\mathcal{B}^*$-биективную сеть ∇_n ширины n, которая представляется в виде следующего произведения $4n-4$ элементарных сетей:

$$\nabla_n = \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \ldots \cdot \Sigma_1^{(2,1)} \cdot \Sigma_n^{(n-1,n)} \cdot \ldots \cdot \Sigma_2^{(1,2)} \cdot \Sigma_1^{(2,1)} \cdot \ldots \cdot \Sigma_1^{(n,1)}.$$

Покажем, что данная сеть ∇_n допускает свободную $k\mathcal{R}$-разметку при любых невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из $\mathbb{N}$.

Для простоты обоснования рассмотрим случай $k = 2$, изображенный на рисунке 10. При проведении свободного параллельного продолжения начальных условий $(v_{11}, \ldots, v_{1n}) \neq (v_{21}, \ldots, v_{2n})$ возможны варианты:

- если $v_{11} \neq v_{21}$, то $\{y_{12}, \ldots, y_{1n-1}, z_{1n}\} \cap \{y_{22}, \ldots, y_{2n-1}, z_{2n}\} = \varnothing$,
- если $v_{11} = v_{21}$, то $v_{1m} \neq v_{2m}$ для некоторого $m \in \{2, \ldots, n\}$ и
$$\{y_{1m}, \ldots, y_{1n-1}, z_{1n}\} \cap \{y_{2m}, \ldots, y_{2n-1}, z_{2n}\} = \varnothing.$$

Однако в любом случае $z_{1n} \neq z_{2n}$. Теперь, учитывая определение свободного параллельного продолжения, легко видеть, что

$$\{z_{11}, \ldots, z_{1n}\} \cap \{z_{21}, \ldots, z_{2n}\} = \varnothing$$

и, следовательно, при выборе любых условий $w_{12}, \ldots, w_{1n}, w_{22}, \ldots, w_{2n}$ не потребуется никакого отождествления среди меток множества

$$\{z_{11}, \ldots, z_{1n}\} \cup \{z_{21}, \ldots, z_{2n}\}.$$

Далее, при свободном параллельном продолжении имеющейся 2-разметки, получаем, что

$$\{u_{13}, \ldots, u_{1n}\} \cap \{u_{23}, \ldots, u_{2n}\} = \varnothing$$

и остается рассмотреть 2 возможных варианта окончания разметки при невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \left(\begin{smallmatrix} v_{21} & \ldots & v_{2n} \\ w_{21} & \ldots & w_{2n} \end{smallmatrix}\right)$:

- если $w_{11} \neq w_{21}$, то, очевидно, не требуется никакого отождествления среди меток множества
$$\{u_{13}, \ldots, u_{1n}\} \cup \{u_{23}, \ldots, u_{2n}\}.$$
- если $w_{11} = w_{21}, \ldots, w_{1m-1} = w_{2m-1}$ и $w_{1m} \neq w_{2m}$, то легко видеть, что потребуются только лишь следующие отождествления
$$u_{13} = u_{23}, \ldots, u_{1m-1} = u_{2m-1}.$$

Таким образом, рассмотренная сеть ∇_n допускает свободную $2\mathcal{R}$-разметку при любых невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \left(\begin{smallmatrix} v_{21} & \ldots & v_{2n} \\ w_{21} & \ldots & w_{2n} \end{smallmatrix}\right)$ (см. рис. 10).

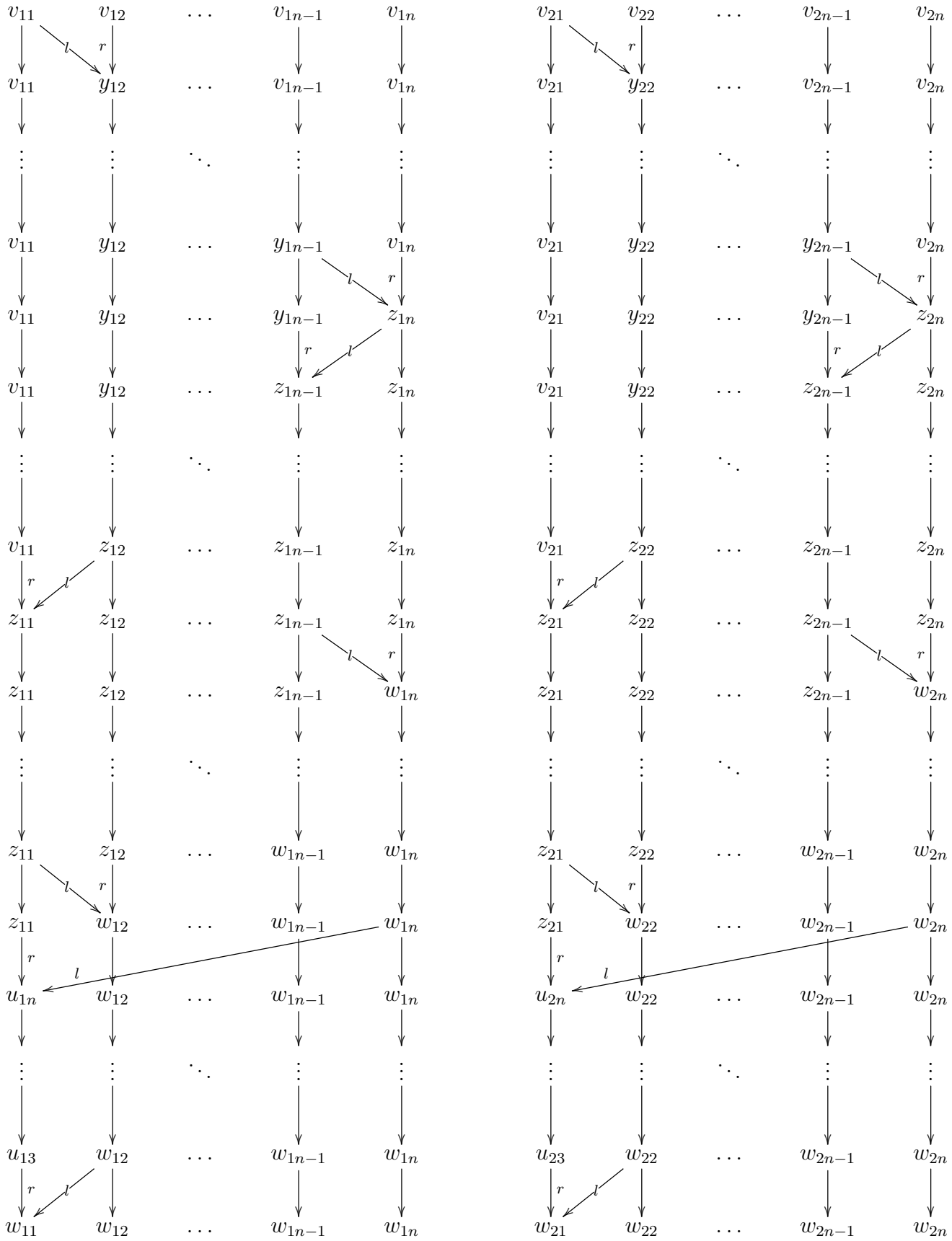
v_{11} v_{12} $\cdots$ v_{1n-1} v_{1n}
v_{21} v_{22} $\cdots$ v_{2n-1} v_{2n}
y_{12} y_{1n-1} y_{22} y_{2n-1}
z_{1n} z_{2n}
z_{12} z_{1n-1} z_{22} z_{2n-1}
z_{11} z_{21}
w_{1n} w_{2n}
w_{12} w_{1n-1} w_{22} w_{2n-1}
u_{1n} u_{2n}
u_{13} u_{23}
w_{11} w_{21}
l r

Рис. 10.

Аналогично доказывается, что сеть ∇_n допускает свободную $k\mathcal{R}$-разметку при любых невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \dots & v_{1n} \\ w_{11} & \dots & w_{1n} \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} v_{k1} & \dots & v_{kn} \\ w_{k1} & \dots & w_{kn} \end{smallmatrix}\right)$ из $\mathbb{N}$.

Поскольку каждая k-разметка сети ∇_n содержит не более $k(5n-4)$ различных меток, то для произвольного множества Ω, мощность которого не менее чем $k(5n-4)$, сеть ∇_n допускает $k\mathcal{R}$-разметку элементами множества Ω при любых невырожденных ограничениях из Ω, что, согласно утверждению 3.8, равносильно $k\mathcal{R}$-транзитивности сети ∇_n для множества Ω.

Архитектура рассмотренной в примере 3.1 сети ∇_n обладает одной особенностью, которая позволяет использовать данную сеть для построения широкого класса $k\mathcal{R}$-транзитивных сетей.

Теорема 3.16. *Пусть $\Sigma = \Sigma_1 \cdot \ldots \cdot \Sigma_t$ — $\mathcal{R}$-биективная сеть ширины n. Тогда произведение $\Sigma \cdot \nabla_n$ является $k\mathcal{R}$-транзитивным для любого множества Ω мощности не менее чем $k(t+5n-4)$.*

Доказательство. Пусть $\eta = (\eta_1, \dots, \eta_k)$ — свободная $k\mathcal{R}$-разметка сети

$$\Sigma' = \Sigma \cdot \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \ldots \cdot \Sigma_1^{(2,1)}$$

с невырожденными начальными условиями $(v_{11}, \dots, v_{1n}), \dots, (v_{k1}, \dots, v_{kn})$. Не ограничивая общности, будем полагать, что разметка η получена параллельным свободным продолжением соответствующих начальных условий с использованием множеств меток

$$Y_1 = \{y_{11}, y_{12}, \dots\},\ \dots\ , Y_k = \{y_{k1}, y_{k2}, \dots\}.$$

Согласно лемме 3.15, для свободной k-разметки η сети Σ' с невырожденными начальными условиями $(v_{11}, \dots, v_{1n}), \dots, (v_{21}, \dots, v_{2n})$ выполняются условия:

1. $\eta_d(x_1^{(t+2n-2)}), \dots, \eta_d(x_n^{(t+2n-2)}) \in Y_d,\ d \in \{1, \dots, k\}$;
2. метки $\eta_d(x_1^{(t+2n-2)}),\ d \in \{1, \dots, k\}$ (и только они), независимо от условий $(v_{11}, \dots, v_{1n}), \dots, (v_{21}, \dots, v_{2n})$, не являются координатами какого-либо набора из области определения $G_{\Sigma'_1}$ — минимального правила k-разметки η.

Ввиду первого условия, при продолжении рассмотренной свободной k-разметки η до k-разметки сети

$$\Sigma \cdot \Sigma_2^{(1,2)} \cdot \ldots \cdot \Sigma_n^{(n-1,n)} \cdot \Sigma_{n-1}^{(n,n-1)} \cdot \ldots \cdot \Sigma_1^{(2,1)} \cdot \Sigma_n^{(n-1,n)} \cdot \ldots \cdot \Sigma_2^{(1,2)},$$

с условиями

$$\eta_d(x_2^{(t+2n-1)}) = w_{d2}, \ldots, \eta_d(x_n^{(t+3n-3)}) = w_{dn},\ d \in \{1, \ldots, k\}$$

не требуется отождествлять никакие внутренние метки.

В завершение, остается продолжить свободным образом k-разметку η до окончания сети $\Sigma \cdot \nabla_n$ и положить $\eta_1(x_1^{(t+4n-4)}) = w_{11}, \ldots, \eta_k(x_1^{(t+4n-4)}) = w_{k1}$ — при этом возможно потребуется отождествление некоторых меток среди

$$\eta_1(x_1^{(t+3n-2)}), \ldots, \eta_1(x_1^{(t+4n-5)}),\ \ldots\ , \eta_1(x_k^{(t+3n-2)}), \ldots, \eta_k(x_1^{(t+4n-5)})$$

(подобно тому, как это было с разметкой сети ∇_n в примере 3.1).

В результате выполнения описанных действий будет построена k-разметка η сети $\Sigma \cdot \nabla_n$ с невырожденными ограничениями $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$, которая, согласно замечанию 3.6, является свободной $k\mathcal{R}$-разметкой сети $\Sigma \cdot \nabla_n$ с указанными невырожденными ограничениями.

Поскольку для проведения произвольной k-разметки сети $\Sigma \cdot \nabla_n$ требуется не более $k(t + 4n - 4 + n)$ различных меток, то для произвольного множества Ω, мощность которого не менее чем $k(t + 5n - 4)$, сеть $\Sigma \cdot \nabla_n$ допускает $k\mathcal{R}$-разметку элементами множества Ω при любых невырожденных ограничениях $\left(\begin{smallmatrix} v_{11} & \ldots & v_{1n} \\ w_{11} & \ldots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \ldots & v_{kn} \\ w_{k1} & \ldots & w_{kn} \end{smallmatrix}\right)$ из Ω, что, согласно утверждению 3.8, равносильно $k\mathcal{R}$-транзитивности сети $\Sigma \cdot \nabla_n$ для множества Ω. □

Следствие 3.8. *При всех натуральных r сеть ∇_n^r — $k\mathcal{R}$-транзитивна для любого множества Ω, мощность которого не менее чем $k(r(4n - 4) + n)$.*

Замечание 3.8. В данной главе с использованием аппарата разметок удалось сформулировать и обосновать несколько эффективных способов построения таких $\mathcal{R}$-биективных сетей Σ, которые являются $k\mathcal{R}$-транзитивными для всякого множества Ω мощности не менее чем $k(\|\Sigma\| + n)$, где n — ширина Σ.

При этом, стоит отметить, что в качестве k-транзитивного класса преобразований, реализуемого сетью Σ, можно использовать не только полный класс $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, но и специальные репрезентативные выборки $\{\Sigma^F : F \in \mathcal{K}\}$, где $\mathcal{K} \subset \mathcal{R}(\Omega)$ и $|\mathcal{K}| \leqslant |\Omega|^{2kn}$, которые также действуют k-транзитивным образом на множестве наборов Ω^n. Поясним как построить подобную выборку.

Если сеть Σ — $k\mathcal{R}$-транзитивна для множества Ω, то она при любых ограничениях $\left(\begin{smallmatrix} v_{11} & \cdots & v_{1n} \\ w_{11} & \cdots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \cdots & v_{kn} \\ w_{k1} & \cdots & w_{kn} \end{smallmatrix}\right)$ из Ω допускает k-разметку элементами Ω, а правило данной k-разметки можно продолжить до некоторой бинарной операции $F \in \mathcal{R}(\Omega)$ со свойством:

$$\Sigma^F(v_{11}, \ldots, v_{1n}) = (w_{11}, \ldots, w_{1n}), \ldots, \Sigma^F(v_{k1}, \ldots, v_{kn}) = (w_{k1}, \ldots, w_{kn}).$$

Таким образом, построив для каждых ограничений $\left(\begin{smallmatrix} v_{11} & \cdots & v_{1n} \\ w_{11} & \cdots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \cdots & v_{kn} \\ w_{k1} & \cdots & w_{kn} \end{smallmatrix}\right)$ из Ω произвольную $k\mathcal{R}$-разметку элементами множества Ω (например, свободную $k\mathcal{R}$-разметку с ограничениями $\left(\begin{smallmatrix} v_{11} & \cdots & v_{1n} \\ w_{11} & \cdots & w_{1n} \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} v_{k1} & \cdots & v_{kn} \\ w_{k1} & \cdots & w_{kn} \end{smallmatrix}\right)$) и продолжив ее минимальное правило до некоторой бинарной операции $F \in \mathcal{R}(\Omega)$, мы определим класс $\mathcal{K} \subset \mathcal{R}(\Omega)$, $|\mathcal{K}| \leqslant |\Omega|^{2kn}$, для которого множество преобразований $\{\Sigma^F : F \in \mathcal{K}\}$ действует k-транзитивным образом на множестве наборов Ω^n.

Выводы по главе

Основные результаты данной главы заключаются в следующем:

1. сформулированы k-мерные обобщения основных понятий аппарата разметок и доказаны k-мерные аналоги основных технических результатов о разметках;

2. показано, что свободная k-разметка определена однозначно независимо от способа построения;

3. получены критерии $k\mathcal{B}^*$-транзитивности, $k\mathcal{Q}$-транзитивности и универсальный критерий $k\mathcal{R}$-транзитивности сетей;

4. обосновано интересное с теоретической точки зрения упрощение универсального критерия $k\mathcal{R}$-транзитивности;

5. показана возможность эффективной практической реализации для проверки универсального критерия $k\mathcal{R}$-биективности сетей;

6. сформулирован и строго обоснован эффективный универсальный алгоритм построения $\mathcal{R}$-биективных сетей, действующих $k\mathcal{R}$-транзитивным образом для всех достаточно больших множеств;

7. построены универсальные конструкции $\mathcal{R}$-биективных сетей небольшого веса, которые могут быть использованы для эффективного построения широких классов $k\mathcal{R}$-транзитивных сетей с требуемыми особенностями архитектуры.

Заключение

Перечислим основные результаты, полученные автором в диссертации.

1. Описано строение $\mathcal{R}$-биективных сетей — бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из множества $\mathcal{R}(\Omega)$.

2. Разработан эффективный метод проверки кратной транзитивности полного класса блочных преобразований $\{\Sigma^F : F \in \mathcal{R}(\Omega)\}$, определяемых произвольной $\mathcal{R}$-биективной сетью Σ.

3. Предложены и строго обоснованы алгоритмы построения $\mathcal{R}$-биективных сетей, для которых соответствующие полные классы блочных преобразований обладают требуемым показателем кратной транзитивности при достаточно большом множестве Ω.

4. Построены практически значимые классы $\mathcal{R}$-биективных сетей с небольшой сложностью, для которых соответствующие классы блочных преобразований обладают требуемым показателем кратной транзитивности, в том числе и при использовании специальных репрезентативных выборок из множества $\mathcal{R}(\Omega)$.

Результаты диссертационного исследования могут найти применение в области синтеза и анализа узлов защиты информации. С одной стороны, полученные в работе результаты позволяют создавать компоненты узлов защиты и переработки информации, которые обеспечивают высокие показатели конфиденциальности. С другой стороны, при исследовании некоторых известных узлов защиты информации для аппроксимации множества преобразований, реализуемых данными узлами, можно использовать предложенную в работе модель классов блочных преобразований — в рамках указанной модели разработанный аппарат разметки позволяет достаточно эффективно выявлять кратную транзитивность.

Благодарности. Автор выражает глубокую благодарность своим научным руководителям: член-корреспонденту Академии криптографии РФ, доктору физико-математических наук, профессору Черемушкину Александру Васильевичу за постановку задачи и обсуждение результатов, кандидату физико-математических наук, старшему научному сотруднику Галатенко Алексею Владимировичу за оказанную поддержку и внимание к работе, а также всем сотрудникам кафедры математической теории интеллектуальных систем Механико-математического факультета МГУ им. М.В. Ломоносова за внимание и доброжелательное отношение.

Литература

[1] **Артамонов, В. А.** Квазигруппы и их приложения / В. А. Артамонов // Чебышевский сб. — 2018. — т. 19. — №2. — С. 111–122.

[2] **Белоусов, В. Д.** Основы теории квазигрупп и луп / В. Д. Белоусов. — Москва: Наука, 1967 — 222 с.

[3] **Галатенко, А. В.** Один подход к построению кратно транзитивного множества блочных преобразований / А. В. Галатенко, А. Е. Панкратьев, С. Б. Родин // Алгебра и логика. — 2018. — т. 57. — №5. — С. 509–521.

[4] **Галатенко, А. В.** О сложности проверки полиномиальной полноты конечных квазигрупп / А. В. Галатенко, А. Е. Панкратьев // Дискрет. матем. — 2018. — т. 30. — №4. — С. 3–11.

[5] **Глухов, М. М.** О применении квазигрупп в криптографии / М. М. Глухов // Прикладная дискретная математика. — 2008. — №2. — P. 28–32.

[6] **Минк, Х.** Перманенты / Х. Минк. — Москва: Мир, 1982 — 211 с.

[7] **Сачков, В. Н.** Комбинаторика неотрицательных матриц / В. Н. Сачков, В. Е. Тараканов. — Москва: ТВП, 2000 — 448 с.

[8] **Abraham, A.** Hash functions based on large quasigroups / A. Abraham, J. Dvorsky, P. Kromer, J. Platos, V. Snasel // In ICCS 2009. — 2009. — P. 521–529.

[9] **Adams, C. M.** Constructing Symmetric Ciphers Using the CAST Design Procedure / C. M. Adams // Designs, Codes, and Cryptography. — 1997. — vol. 12. — №3. — P. 283–316.

[10] **Anderson, L. D.** Thank Evans! / L. D. Anderson, A. J. W. Hilton // Proc. London Math. Soc. — 1983. — №47. — P. 507–522.

[11] **Angelis, L.** All-or-nothing transforms using quasigroups / L. Angelis, G. L. Bleris, S. I. Marnas // In Proceedings of 1st Balkan Conference in Informatics. — 2003. — P. 183–191.

[12] **Baysal, A., Coban, M., Ozen M.** Feistel Like Construction of Involutory Binary Matrices With High Branch Number [Электронный ресурс] / A. Baysal, M. Coban, M. Ozen // Cryptology ePrint Archive. Report 2016/751. — 2016. — Режим доступа: https://eprint.iacr.org/2016/751.pdf

[13] **Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.** The SIMON and SPECK Families of Lightweight Block Ciphers [Электронный ресурс] / R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers // Cryptology ePrint Archive. Report 2013/404. — 2013. — Режим доступа: http://eprint.iacr.org/2013/404.pdf

[14] **Biryukov, A., Perrin, L., Udovenko, A.** Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1 / A. Biryukov, L. Perrin, A. Udovenko // EUROCRYPT 2016 (LNCS). — 2016. — vol. 9665. — №2. — P. 372–402.

[15] **Canteaut, A., Duval, S., Leurent, G.** Construction of lightweight s-boxes using Feistel and MISTY structures (full version) [Электронный ресурс] / A. Canteaut, S. Duval, G. Leurent // Cryptology ePrint Archive. Report 2015/711. — 2016. — Режим доступа: http://eprint.iacr.org/2015/711

[16] **Carter, S.** Universal Class of Hash Function. / S. Carter, M. N. Wegman // J. of Computer and System Sciences — 1979. — №2. — P. 143–154.

[17] **Carter, S.** New Hash Functions and their Use in Authentication and Set Equality. / S. Carter, M. N. Wegman // J. of Computer and System Sciences — 1981. — №22. — P. 265–279.

[18] **Colbourn, C. J.** Handbook of combinatorial designs. 2nd ed. / Edited by Charles J. Colbourn, Jeffrey H. Dinitz. — CRC Press., 2007. — 1011 c.

[19] **Dawson, E.** Quasigrops, isotopism and authentication schemes. / E. Dawson, D. Donovan, A. Offer // The Australasian journal of combinatorics — 1996. — №13. — P. 75–88.

[20] **Denes, J.** Latin Squares. New Developments in the Theory and Applications. / J. Denes, A. D. Keedwell. — Amsterdam: Nord-Holland Publishing Co., 1981. — 545 c.

[21] **Denes, J.** A new Authentication Scheme based in Latin Squares. / J. Denes, A. D. Keedwell // Discrete Mathematics. — 1992. — №106/107. — P. 157–162.

[22] **Dimitrova, V.** On Quasigroup Pseudo Random Sequence Generators / V.Dimitrova, S. Markovski // In Proceedings of the 1st Balkan Conference in Informatics. — 2003. — P. 393–401.

[23] **Dvorsky, J.** Hashovaci funkce zalozena na kvazigrupach / J. Dvorsky, E. Ochodkova, V. Snasel // In Workshop Milkulasska kryptobesidka. — 2000. — P. 105–112.

[24] **Dvorsky, J.** Hash functions based on large quasigroups / J. Dvorsky, E. Ochodkova, V. Snasel // Velokonocni kryptologie. — 2002. — P. 1–8.

[25] **El-Hadedy, M.** High Performance Implementation of a Public Key Block Cipher MQQ for FPGA Platforms [Электронный ресурс]/ M. El-Hadedy, D. Gligoroski, S. J. Knapskog // Cryptology ePrint Archive. Report 2008/339. — 2008. — Режим доступа: http://eprint.iacr.org/

[26] **Evans, T.** Embedding incomplete latin squares / T. Evans // Amer. Math. Monthly. — 1960. — №67. — P. 959–961.

[27] **Fomin, D. B.** New classes of 8-bit permutations based on a butterfly structure / D. B. Fomin // Матем. вопр. криптогр. — 2019. — т. 10. — №2. — С. 169–180.

[28] **Gligoroski, D.** Candidate One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations [Электронный ресурс] / D. Gligoroski // — 2005. — Режим доступа: http://eprint.iacr.org/2005/352.pdf

[29] **Gligoroski, D.** Stream cipher based on quasigroup string transformation in Zp* [Электронный ресурс] / D. Gligoroski // — 2004. — Режим доступа: ArXiv:cs.CR/0403043v2.

[30] **Gligoroski, D.** Edon-R, An infnite family of cryptographic hash functions [Электронный ресурс] / D. Gligoroski, S. Markovski, L. Kocarev // Режим доступа: http://csrc.nist.gov/pki/HashWorkshop/2006/Papers.

[31] **Gligoroski, D.** On the insecurity of interchanged use of OFB and CBC modes of operation [Электронный ресурс] / D. Gligoroski // Cryptology ePrint Archive. Report 2007/385. — 2007. — Режим доступа: http://eprint.iacr.org/

[32] **Gligoroski, D.** A public key block cipher based on multivariate quadratic quasigroups [Электронный ресурс]/ D. Gligoroski, S. Markovski, S. J. Knapskog // Cryptology ePrint Archive. — 2008. — Режим доступа: http://arxiv.org/0808.0247:22 pages.

[33] **Gligoroski, D.** Edon80 [Электронный ресурс] / D. Gligoroski, S. Markovski, L. Kocarev, M. Gusev // eSTREAM, ECRYPT Stream Cipher Project. — 2005. — Режим доступа: http://www.ecrypt.eu.org/stream/edon80p3.html

[34] **Gligoroski, D.** Quasigroup and Hash Functions / S. Gligoroski, S. Markovski, V. Bakeva // Discr. Math. And Appl. Proc. of the 6th ICDMA Bansko. — 2001. — P. 43–50.

[35] **Gligoroski, D.** Quasigroup String Processing: Part1 / D. Gligoroski, S. Markovski, V. Bakeva // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XX. — 1999. — №1–2. — P. 13–28.

[36] **Gligoroski, D.** On infinite Class of strongly Collision Resistant Hash Functions «EDON-F» with Variable Length of Output / S. Gligoroski, S. Markovski, V. Bakeva // Proc. 1st International Conference on Mathematics and Informatics for Industry. — 2003.

[37] **Hassinen, M.** Secure SMS messaging using Quasigroup encryption and Java SMS API / M. Hassinen, S. Markovski // In SPLST'03. — 2003.

[38] **Hassinen, M.** Differential cryptanalysis of the quasigroup cipher. Definition of the encryption method / M. Hassinen, S. Markovski // In Differential cryptanalysis, Petrozavodsk. — 2004.

[39] **Hell, M.** A key recovery attack on Edon80 / M. Hell, T. Johanson // ASIACRYPT'07. — 2007. — С. 568–581.

[40] **Hoahg, V. T., Rogaway, P.** On Generalized Feistel Networks / В. А. Артамонов // Annual Cryptology Conference CRYPTO 2010: Advances in Cryptology (LNCS). — 2010. — vol. 6223. — P. 613–630.

[41] **Koscielny, C.** A method of constructing quasigroup-based stream ciphers / C. Koscienly // Appl. Math. and Comp. Sci. — 1996. — №6. — С. 109–121.

[42] **Koscielny, C.** NLPN Sequences over GF(q) / C. Koscienly // Quasigroups Relat. Syst. — 1997. — №4. — С. 89–102.

[43] **Luby, M., Rackoff, C.** How to Construct Pseudo-random Permutations from Pseudo-random functions / M. Luby, C. Rackoff // SIAM J. Computing. — 1988. — vol. 17. — №2. — P. 373–386..

[44] **Markovski, S.** Quasigroup String Processing: Part2 / S. Markovski, V. Kusacatov // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXI. — 2000. — №1–2. — P. 15–32.

[45] **Markovski, S.** Quasigroup String Processing: Part3 / S. Markovski, V. Kusacatov // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXIII. — 2002. — №1–2. — P. 7–27.

[46] **Markovski, S.** Quasigroup String Processing: Part4 / S. Markovski, V. Bakeva // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XXVII. — 2006. — №1–2. — P. 41–53.

[47] **Menezes, A. J., Oorschot, P. C., Vanstone, S. A.** Handbook of applied cryptography / A. J. Menezes, P. C. Oorschot , S. A. Vanstone. — CRC Press, 1996 — 816 p.

[48] **Naor, M., Reingold, O.** On the construction of pseudo-random permutations: Luby-Rackoff revisited / M. Naor, O. Reingold // Journal of Cryptology. — 1997. — vol. 12. — №1. — P. 29–66.

[49] **Nyberg, K.** Generalized Feistel Networks / K. Nyberg // ASIACRYPT'96. LNCS. — 1996. — vol. 1163. — P. 90–104.

[50] **Ochadkova, E.** Using quasigroups for secure encoding of file system / E. Ochadkova, V. Snasel // In Conference «Security and Protection of information». — 2001. — P. 175–181.

[51] **Shcherbacov, V. A.** Quasigroups in cryptology / V. A. Shcherbacov // Comput. Sci. J. Moldova. — 2009. — №2(50). — P. 193–228.

[52] **Schneier, B.** Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) / B. Schneier // Fast Software Encryption: Cambridge Security Workshop Cambridge (LNCS). — 1994. — vol. 809. — P. 191–204.

[53] **Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N.** Twofish: A 128-bit Block Cipher [Электронный ресурс] / B.Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson // Режим доступа: http://www.counterpane.com/twofish.html

[54] **Shimizu, A., Miyaguchi, S.** Fast Data Encipherment Algorithm FEAL / A. Shimizu, S. Miyaguchi // Advances in Cryptology — EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques. — 1988. — т. 19. — №2. — P. 267–278.

[55] **Smetaniuk, B.** A new construction on latin squares. A proof of the Evans conjecture / B. Smetaniuk // Ars Combinatoria. — 1981. — №11. — P. 155-172.

[56] **Suzaki, T., Minematsu, K.** Improving the Generalized Feistel / T. Suzaki, K. Minematsu // International Workshop on Fast Software Encryption FSE 2010: Fast Software Encryption (LNCS) — 2010. — vol. 6147. — №2. — P. 19–39.

[57] **Takeshi S., Naofumi H., Takafumi A., Akashi S.** High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA / S. Takeshi, H. Naofumi, A. Takafumi, S. Akashi // 2008 IEEE International Symposium on Circuits and Systems. — 2008. — P. 111–122.

[58] **Vojvoda, M.** Cryptanalysis of one hash function based on quasigroup / M. Vojvoda // Tatra Mt. Math. Publ. — 2004. — №29. — С. 173–181.

[59] **Vojvoda, M.** Stream ciphers and hash functions - analysis of some new design approaches: PhD thesis / M. Vojvoda. — Slovak University of Technology, 2004.

[60] **Zheng, Y., Matsumoto, T., Imai, H.** On the construction of block ciphers provably secure and not relying on any unproved hypotheses / Y. Zheng, T. Matsumoto, H. Imai // CRYPTO'89 (LNCS). — 1990. — vol. 435. — P. 461–480.

Публикации автора по теме диссертации

Научные статьи, опубликованные в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в списки Scopus и/или WoS, RSCI

[61] **Чередник, И. В.** Один подход к построению транзитивного множества блочных преобразований / И. В. Чередник // Прикладная дискретная математика. — 2017. — №38. — С. 5–34. (WoS, RSCI, ИФ РИНЦ 0.370)

[62] **Чередник, И. В.** Один подход к построению кратно транзитивного множества блочных преобразований / И. В. Чередник // Прикладная дискретная математика. — 2018. — №42. — С. 18–47. (WoS, RSCI, ИФ РИНЦ 0.507)

[63] **Чередник, И. В.** Об использовании бинарных операций при построении транзитивного множества блочных преобразований / И. В. Чередник // Дискретная математика. — 2019. — т. 31 №3. — С. 93–113.
(WoS, RSCI, ИФ РИНЦ 0.518)

(Пер. на англ. яз.: **Cherednik, I. V.** Using binary operations to construct a transitive set of block transformations / I. V. Cherednik // Discrete Mathematics and Applications. — 2020. — **30: 3**. — P. 375–389.) (Scopus, WoS)

[64] **Чередник, И. В.** Об использовании бинарных операций при построении кратно транзитивного множества блочных преобразований / И. В. Чередник // Дискретная математика. — 2020. — т. 32 №2. — С. 85–111.
(WoS, RSCI, ИФ РИНЦ 0.390)

(Пер. на англ. яз.: **Cherednik, I. V.** On the use of binary operations for the construction of a multiply transitive class of block transformations /
I. V. Cherednik // Discrete Mathematics and Applications. — 2021. — **31: 2**. — P. 91–111.) (Scopus, WoS)

Прочие публикации (по теме диссертации)

[65] **Чередник, И. В.** Об одном подходе к построению транзитивного множества блочных преобразований / И. В. Чередник // Материалы Всероссийской конференции SIBECRYPT'17 — Прикладная дискретная математика. Приложение — 2017. — №10. — С. 27–29.

[66] **Чередник, И. В.** k-транзитивность одного класса блочных преобразований / И. В. Чередник // Материалы Всероссийской конференции SIBECRYPT'18 — Прикладная дискретная математика. Приложение — 2018. — №11. — С. 21–23.