Math-Net.Ru
Общероссийский математический портал

С. В. Полин, Решение уравнений методом последовательного группирования и его оптимизация,
Матем. вопр. криптогр., 2012, том 3, выпуск 1, 97–123

https://www.mathnet.ru/mvk50

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.9.168
25 апреля 2025 г., 01:52:54

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2012 Т. 3 № 1 С. 97–123

УДК 519.16+519.615.5+519.712

Решение уравнений методом последовательного группирования и его оптимизация

С. В. Полин

Академия криптографии Российской Федерации, Москва

Получено 11.X.2010

Построена общая модель класса алгоритмов решения уравнений и систем нелинейных уравнений, состоящих из нескольких последовательных этапов, на каждом из которых проводится группирование неизвестных с последующим опробованием и отсевом группы. Предложен способ выделения в этом классе оптимального алгоритма.

Ключевые слова: нелинейные системы уравнений, метод группирования, представления решеток

Solution of equations by the sequential grouping method and its optimization

S. V. Polin

Academy of Cryptography of Russian Federation, Moscow

Abstract. A general model of a class of algorithms for the solution of equations and systems of nonlinear equations is constructed. These algorithms are performed in several steps consisting in grouping of unknowns, testing and possible elimination of such groups. An approach for choosing the optimal algorithm is suggested.

Key words: systems of nonlinear equations, grouping method, lattice representations

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 1, pp. 97–123 (Russian).

© 2012 С. В. Полин

§ 1. Древовидные алгоритмы перебора

Выберем и фиксируем конечное множество A.

Через $\mathcal{E}(A)$ обозначим решетку всех отношений эквивалентности на множестве A с упорядоченностью по включению. Наименьшим и наибольшим элементами этой решетки являются отношения $\Delta_A = \langle (a,a) \mid a \in A \rangle$ и $\nabla_A = A \times A$. Пересечение и объединение элементов θ, ρ решетки $\mathcal{E}(A)$ будем обозначать через $\theta \cap \rho$ и $\theta \cup \rho$ соответственно. Необходимо подчеркнуть, что пересечение отношений совпадает с их теоретико-множественным пересечением, а объединение в общем случае отличается от их теоретико-множественного объединения. Последний факт, в принципе, мог бы вызвать недоразумения, однако этого не произойдет из-за того, что мы не будем рассматривать объединение отношений эквивалентности в теоретико-множественном смысле.

Пусть $\theta \in \mathcal{E}(A)$. Класс эквивалентности отношения θ, содержащий элемент a, обозначим через $[a]_\theta$. Множество всех классов эквивалентности отношения θ образует фактормножество A/θ.

Рассмотрение классов эквивалентности удобно при теоретических исследованиях, однако при практической реализации алгоритмов их использование сталкивается с определенными проблемами. Например, чтобы записать класс эквивалентности в память вычислительной системы, формально нужно записать в память все элементы класса. Однако обычно либо в память заносится один представитель класса, либо используется какая-нибудь кодировка классов и в память заносится соответствующий код. Аналогично, при реализации тех или иных операций с классами также используется эта кодировка. Поэтому для каждого отношения $\theta \in \mathcal{E}(A)$ мы введем в рассмотрение некоторое множество A_θ, равномощное множеству A/θ, с элементами которого удобно оперировать, и взаимно однозначное отображение $\xi_\theta : A/\theta \to A_\theta$. Также полагаем $\pi_\theta(a) = \xi_\theta([a]_\theta)$. Ясно, что каждое отображение π_θ сюръективно.

В частности, выберем $A_{\Delta_A} = A$, $\xi_{\Delta_A}(\{a\}) = a$. Тогда π_{Δ_A} оказывается тождественным на A отображением 1_A.

Наличие взаимно однозначного отображения ξ_A показывает, что алгебраические свойства множеств отображений из множества A/θ в какое-либо множество B и из множества A_θ в то же множество B одинаковы. В частности, из теоремы о гомоморфизме для множества A/θ вытекает аналогичное утверждение для множества A_θ. Для удобства читателей сформулируем это утверждение. Предварительно напомним, что *ядром* произвольного отображения $g: C \to D$ называется отношение эквивалентности

$$\ker g = \left\langle (c_1, c_2) \in C^2 \;\middle|\; g(c_1) = g(c_2) \right\rangle.$$

Лемма 1.1. *Для любого отношения* $\theta \in \mathcal{E}(A)$ *справедливо равенство* $\ker \pi_\theta = \theta$. *Если* $f: A \to B$ *— такое отображение, что* $\theta \subseteq \ker f$, *то существует единственное отображение* $f': A_\theta \to B$, *для которого выполняется равенство* $f = f' \pi_\theta$.

Пусть $\rho, \theta \in \mathcal{E}(A)$ и $\rho \subseteq \theta$. Тогда из леммы 1.1 вытекает существование сюръективного отображения $\pi_{\theta\rho}: A_\rho \to A_\theta$, для которого выполняется равенство $\pi_{\theta\rho}\pi_\rho = \pi_\theta$, причем этим условием отображение $\pi_{\theta\rho}$ определяется однозначно. Нетрудно проверить, что

$$\pi_{\theta\theta} = 1_{A/\theta}, \quad \pi_{\theta\Delta_A} = \pi_\theta, \quad \pi_{\tau\theta}\pi_{\theta\rho} = \pi_{\tau\rho} \tag{1.1}$$

для всех отношений $\rho, \theta, \tau \in \mathcal{E}(A)$.

Для элемента $d \in A_\theta$ полагаем

$$\mathcal{F}(d, \rho) = \left\langle c \in A_\rho \;\middle|\; \pi_{\theta\rho}(c) = d \right\rangle. \tag{1.2}$$

Все такие множества будем называть *факторами*. Поскольку отображение $\pi_{\theta\rho}$ сюръективно, имеет место разбиение множества A_ρ

$$A_\rho = \coprod_{d \in A_\theta} \mathcal{F}(d, \rho). \tag{1.3}$$

На множестве $\mathcal{E}(A)$ можно ввести структуру ориентированного графа, считая, что пара (θ, ρ) является дугой, ведущей из вершины θ в вершину ρ, тогда и только тогда, когда $\theta \supset \rho$. Выберем и временно фиксируем некоторый подграф $\mathcal{G}$ графа $\mathcal{E}(A)$, содержащий вершины ∇_A и Δ_A.

Напомним, что последовательность $\vec{\theta} = \theta_0, ..., \theta_n$ называется *маршрутом* графа $\mathcal{G}$, ведущим из вершины ∇_A в вершину Δ_A, если $\nabla_A = \theta_0$, $\Delta_A = \theta_n$ и каждая пара (θ_i, θ_{i+1}) является дугой графа. Множество всех маршрутов, ведущих из ∇_A в Δ_A, обозначим через $\mathfrak{M}(\mathcal{G})$.

Отметим, что для каждого маршрута $\vec{\theta} = \theta_0, ..., \theta_n \in \mathfrak{M}(\mathcal{G})$ имеет место цепочка включений

$$\nabla_A = \theta_0 \supset \theta_1 \supset ... \supset \theta_{n-1} \supset \theta_n = \Delta_A.$$

Это позволяет по маршруту $\vec{\theta}$ построить выходящее дерево $\mathcal{D}(\vec{\theta})$ следующим образом.

- Множеством вершин дерева является множество $V(\vec{\theta}) = \coprod_{i=0}^{n} A_{\theta_i}$.
- Если $d \in A_{\theta_i}, c \in A_{\theta_j}$, то пара (d, c) является дугой дерева тогда и только тогда, когда $j = i + 1$ и $c \in \mathcal{F}(d, \theta_{i+1})$.

Предположим, что для каждой дуги (θ, ρ) графа $\mathcal{G}$ и каждого элемента $d \in A_\theta$ существует эффективный алгоритм перебора всех элементов множества $c \in \mathcal{F}(d, \rho)$. Точнее, будем считать, что *построение очередного элемента каждого из этих множеств является элементарной операцией.* Элементы, выбираемые первым и последним, будем называть *начальным и конечным* элементами соответствующего множества. Если элемент c' выбирается непосредственно за элементом c, то будем писать $c' = \mathrm{Next}(c)$.

Подчеркнем, что это требование накладывает ограничение не на граф, а на используемую модель вычислителя. Действительно, если память вычислителя достаточно велика, то элементы каждого из множеств $\mathcal{F}(c, \theta)$ могут быть занесены в определенный сегмент памяти и алгоритм перебора состоит в последовательном считывании элементов из соответствующего сегмента.

Соединим существующие по предположению алгоритмы перебора факторов и алгоритм прохождения дерева $\mathcal{D}(\vec{\theta})$ в глубину [7, гл. 2]. Это дает алгоритм перебора элементов множества A. Алгоритм использует числовую переменную k и переменные $c_0, c_1, ..., c_{n-1}$. Переменная c_i принимает значение в множестве A_{θ_i}, причем если переменной c_{i-1} присвоено значение d, то переменная c_i принимает значение в множестве $\mathcal{F}(c_{i-1}, \theta_i)$.

Алгоритм $\mathfrak{A}\left(\vec{\theta}\right)$:

1. $k := 0, c_0 := o,$ где o — единственный элемент множества A_{∇_A}.
2. Пока $k < n-1,$ выполняем операции:
   переменной c_{k+1} присваиваем значение, равное начальному элементу множества $\mathcal{F}\left(c_k, \theta_{k+1}\right)$;
   $k := k+1;$
   возврат на начало шага.
3. Перебираем и выдаем на выход элементы множества $\mathcal{F}\left(c_{n-1}, \Delta_A\right)$.
4. Пока $k > 0$ и c_k является конечным элементом множества $\mathcal{F}\left(c_{k-1}, \theta_k\right),$ выполняем операцию $k := k-1.$ Если $k = 0,$ то выполнение алгоритма прекращается.
5. Полагаем $c_k := \mathrm{Next}\left(c_k\right).$ Возврат на шаг 2.

Как обычно, пренебрежем управляющими операциями, операциями организации циклов и т. д. В результате трудоемкость алгоритма будет равна суммарной трудоемкости перебора элементов множества A_{∇_A} и элементов всех множеств $\mathcal{F}\left(c_{k-1}, \theta_k\right),$ где $k \in \{1,...,n\},$ $c_{k-1} \in A_{\theta_{k-1}}$. В наших предположениях трудоемкость равна

$$1 + \sum_{k=1}^{n} \bigcup_{c_{k-1} \in A_{\theta_{k-1}}} \left|\mathcal{F}\left(c_{k-1}, \theta_k\right)\right| = \sum_{k=1}^{n} \left|A_{\theta_{k-1}}\right|.$$

Построенный алгоритм будем называть *древовидным.*

§ 2. $\mathcal{L}$ - множества

Выше мы отмечали, что на выбор графа $\mathcal{G}$ можно было бы не накладывать никаких ограничений, однако при их отсутствии получить сколько-нибудь содержательные результаты не представляется возможным. Ограничения можно выбирать различными способами в зависимости от цели исследований. Нижеуказанные ограничения выбраны так, чтобы их можно было использовать в ряде важных для практики случаев.

Пусть $\mathcal{L} \subseteq \mathcal{E}(A)$ — подрешетка решетки $\mathcal{E}(A),$ содержащая отношения Δ_A и ∇_A. Для элементов θ, ρ полагаем $\theta \triangleright \rho$ тогда и только тогда, когда $\theta \supset \rho$ и не существует такого элемента $\tau \in \mathcal{L},$ что $\theta \supset \tau \supset \rho$. Свяжем с подрешеткой граф $\mathcal{G}_{\mathcal{L}},$ взяв в качестве множества его вершин множество

элементов подрешетки $\mathcal{L}$, а в качестве множества дуг — множество таких пар (θ,ρ), что $\theta \triangleright \rho$. Допуская некоторую неточность, вместо «маршруты графа $\mathcal{G}_{\mathcal{L}}$» будем говорить «маршруты решетки $\mathcal{L}$». Соответственно, вместо $\mathfrak{M}(\mathcal{G}_{\mathcal{L}})$ будем писать $\mathfrak{M}(\mathcal{L})$.

Напомним, что подмножество Θ решетки $\mathcal{L}$ называется ее *цепью*, если элементы множества Θ попарно сравнимы. Цепь Θ называется *максимальной*, если не существует цепи Θ', строго содержащей цепь Θ. Ниже нам понадобится связь между маршрутами, принадлежащими множеству $\mathfrak{M}(\mathcal{L})$, и максимальными цепями.

Лемма 2.1. *Пусть* $\vec{\theta} = \theta_0, \theta_1, ..., \theta_n$ *— такая последовательность элементов решетки* $\mathcal{L}$, *что* $\theta_0 \supset \theta_1 \supset ... \supset \theta_n$. *Тогда множество* $\Theta = \{\theta_0, \theta_1, ..., \theta_n\}$ *является цепью. Цепь* Θ *максимальна тогда и только тогда, когда последовательность* $\vec{\theta}$ *принадлежит множеству* $\mathfrak{M}(L)$.

То, что множество Θ является цепью, очевидно. Допустим, что эта цепь не максимальна. Тогда существует такой элемент $\rho \in \mathcal{L} \setminus \Theta$, что множество $\Theta \cup \{\rho\}$ также является цепью. Последнее эквивалентно тому, что элемент ρ сравним со всеми элементами из множества Θ. Ясно, что если $\theta_i \supset \rho$, то $\theta_j \supset \rho$ для всех номеров $j < i$. Отсюда следует, что имеет место один из трех случаев.

1. $\theta_i \supset \rho$ для всех номеров i.
2. $\theta_i \subset \rho$ для всех номеров i.
3. Существует такой номер i, что $\theta_i \supset \rho \supset \theta_{i+1}$.

Если имеет место случай 1, то $\rho \supset \theta_0$ и $\theta_0 \neq \nabla_A$. Так же замечаем, что $\theta_n \neq \Delta_A$ в случае 2. Наконец, случай 3 означает, что $\theta_i \not\triangleright \theta_{i+1}$. В любом случае $\vec{\theta} \notin \mathfrak{M}(L)$.

Обратно, допустим, что $\vec{\theta} \notin \mathfrak{M}(L)$. Опять возможны три случая.

1. $\theta_0 \neq \nabla_A$.
2. $\theta_n \neq \Delta_A$.
3. Существуют такой номер i и такой элемент $\rho \in \mathcal{L}$, что $\theta_i \supset \rho \supset \theta_{i+1}$.

В случае 1 множество $\{\Delta_A\} \cup \Theta$ является цепью, строго содержащей цепь Θ. В случае 2 такой цепью является множество $\{\Delta_A\} \cup \Theta$, а в случае 3 — множество $\{\rho\} \cup \Theta$. ■

В дальнейшем мы будем рассматривать только графы вида $\mathcal{G}_{\mathcal{L}}$. Более того, на решетку $\mathcal{L}$ также будут наложены ограничения.

В терминах монографии [4] вложение $\mathcal{L} \to \mathcal{E}(A)$ определяет *представление* решетки $\mathcal{L}$. В той же монографии проведена классификация представлений и выделены наиболее простые представления типа 1. Рассматриваемое нами представление $\mathcal{L} \to \mathcal{E}(A)$ имеет тип 1 тогда и только тогда, когда элементы решетки $\mathcal{L}$ попарно перестановочны. В случае выполнения этого свойства будем называть решетку $\mathcal{L}$ *перестановочной*. Приведем примеры таких решеток.

Решетка конгруэнций Ω-групп[1]. Предположим, что на множестве A задана структура Ω-группы $\mathbf{A} = \langle A; \Omega, + \rangle$, т. е. на нем задана групповая, не обязательно коммутативная, операция «+» и некоторое множество Ω операций, каждая из которых удовлетворяет равенству $0...0\omega = 0$. Каждая конгруэнция θ Ω-группы **A** определяется подходящим *идеалом* I_θ следующим образом: $\big((a,b) \in \theta\big) \Leftrightarrow \big(a - b \in I_\theta\big)$. Каждый идеал является нормальным делителем группы $\langle A; + \rangle$.

Рассмотрим две конгруэнции θ, ρ и такие элементы a, c, что $(a,c) \in \theta\rho$. Пусть b — такой элемент, что $(a,b) \in \theta$ и $(b,c) \in \rho$. Это означает, что $a = x + b,\ b = y + c$ для подходящих элементов $x \in I_\theta$, $y \in I_\rho$. Полагаем $z = x + y - x,\ d = a + z$. Так как идеал I_ρ является нормальным идеалом, то $z \in I_\rho$ и $(a,d) \in I_\rho$. Далее имеем

$$d + x = a + (x + y - x) + x = (a + x) + y = b + y = c$$

и $(d,c) \in I_\theta$. Таким образом, $(a,c) \in \rho\theta$ и $\theta\rho \subseteq \rho\theta$. Обратное включение доказывается аналогично.

Частным случаем Ω-групп являются часто встречающиеся на практике векторные пространства. Для векторных пространств задача перебора элементов фактора $\mathcal{F}(d,\rho)$ эквивалентна решению линейного уравнения

[1] Определения Ω-групп и связанных с ними понятий содержатся в монографии [6].

$\pi_{\theta\rho}(x) = d$. Как известно, для решения последней существует эффективный алгоритм.

Решетка конгруэнций прямого произведения. Предположим, что множество A разлагается в прямое произведение $\prod_{i=1}^{m} A_i$. Тогда каждый элемент множества A можно отождествить с вектором $\mathbf{a} = (a_1, a_2, ..., a_m)$, где координата a_j принадлежит множеству A_j. Для каждого подмножества $J \subseteq \{1, 2, ..., m\}$ определим отношение θ_J, положив $(\mathbf{a}, \mathbf{b}) \in \theta_J$ тогда и только тогда, когда $a_j = b_j$ для всех $j \in J$. Все отношения указанного вида будем называть *конгруэнциями прямого произведения* $\prod_{i=1}^{m} A_i$.

Очевидно, что $\theta_J \cap \theta_I = \theta_{J \cup I}$.

Пусть $(\mathbf{a}, \mathbf{b}) \in \theta_J$, $(\mathbf{b}, \mathbf{c}) \in \theta_I$. Тогда для каждого номера $j \in J \cap I$ имеем $a_j = b_j = c_j$, т. е. $(\mathbf{a}, \mathbf{c}) \in \theta_{J \cap I}$, откуда следует, что $\theta_J \theta_I \subseteq \theta_{J \cap I}$. Обратно, пусть $(\mathbf{a}, \mathbf{c}) \in \theta_{J \cap I}$. Полагаем

$$b_j = \begin{cases} a_j, & j \in J; \\ c_j, & j \notin J. \end{cases}$$

Непосредственно из определения следует, что $(\mathbf{a}, \mathbf{b}) \in \theta_J$. Если $j \in I$, то либо $j \in J \cap I$ и $b_j = a_j = c_j$, либо $j \notin J \cap I$ и $b_j = c_j$. Таким образом, $(\mathbf{a}, \mathbf{c}) \in \theta_J \cap \theta_I$, откуда следует $\theta_J \theta_I \supseteq \theta_{J \cap I}$, т. е. $\theta_J \theta_I = \theta_{J \cap I}$.

Симметричным образом показываем, что $\theta_I \theta_J = \theta_{J \cap I}$, откуда следует равенство $\theta_I \theta_J = \theta_J \theta_I$. Кроме того, из доказанного равенства вытекает (см. [5]), что $\theta_I \cup \theta_J = \theta_{J \cap I}$. Таким образом, множество отношений эквивалентности рассматриваемого вида образует перестановочную подрешетку решетки $\mathcal{E}(A)$.

Нетрудно видеть, что для существования в рассматриваемом случае эффективных алгоритмов перебора факторов необходимо и достаточно существование эффективных алгоритмов перебора компонент A_i, что обычно выполняется.

Как правило, в практических задачах мы имеем дело с объектами, описанными в приведенных примерах. Поэтому мы могли бы в дальнейших рассмотрениях считать, что решетка $\mathcal{L}$ относится к одному из этих двух

видов, однако между данными решетками имеются различия, которые вынуждали бы нас проводить некоторые доказательства для каждой решетки в отдельности. Чтобы избежать этого, будем считать, что нами выбрана некоторая перестановочная подрешетка $\mathcal{L}$, обладающая дополнительным свойством *однородности*: для любых таких отношений $\theta,\rho\in\mathcal{L}$, что $\theta\supset\rho$, все факторы $\mathcal{F}(d,\rho)$ $(d\in A_\theta)$ равномощны. Ясно, что эта общая мощность $\left|\mathcal{F}(d,\rho)\right|$ равна величине $[\theta:\rho]\overset{df}{=}\dfrac{|A_\rho|}{|A_\theta|}$. То, что обе интересующие нас решетки однородны, легко проверяется.

Множество A, на котором задана перестановочная однородная решетка $\mathcal{L}$ отношений эквивалентности, будем называть $\mathcal{L}$ *-множеством*.

В заключение настоящего раздела приведем два свойства перестановочных решеток, которые мы будем использовать ниже.

Лемма 2.2. *Любая перестановочная подрешетка* $\mathcal{L}\subseteq\mathcal{E}(A)$ *модулярна.*

Утверждение вытекает из теоремы Йенсена [4, с. 258–259]. ■

Чтобы сформулировать следующее утверждение, нам потребуется провести некоторые построения.

Рассмотрим произвольные отношения $\theta,\rho\in\mathcal{E}(A)$. Определенные нами отображения $\pi_{\theta\cup\rho\,\theta}:A_\theta\to A_{\theta\cup\rho}$, $\pi_{\theta\cup\rho\,\rho}:A_\rho\to A_{\theta\cup\rho}$ позволяют построить *расслоенное произведение*

$$A_\theta\times_{A_{\theta\cup\rho}}A_\rho=\left\langle(c,d)\in A_\theta\times A_\rho\;\middle|\;\pi_{\theta\cup\rho\,\theta}(c)=\pi_{\theta\cup\rho\,\rho}(d)\right\rangle.$$

Определим отображение $\varphi_{\theta\rho}:A_{\theta\cap\rho}\to A_\theta\times A_\rho$, положив

$$\varphi_{\theta\rho}(b)=\left(\pi_{\theta\,\theta\cap\rho}(b),\pi_{\rho\,\theta\cap\rho}(b)\right).$$

Из равенств (1.1) следует, что для любого элемента $b\in A_{\theta\cap\rho}$ пара $\varphi_{\theta\rho}(b)$ принадлежит множеству $A_\theta\times_{A_{\theta\cup\rho}}A_\rho$. Таким образом, $\varphi_{\theta\rho}$ является отображением $\varphi_{\theta\rho}:A_{\theta\cap\rho}\to A_\theta\times_{A_{\theta\cup\rho}}A_\rho$.

Лемма 2.3. *Для любых отношений* $\theta,\rho\in\mathcal{E}(A)$ *отображение* $\varphi_{\theta\rho}$ *инъективно. Если отношения* θ,ρ *перестановочны, то отображение* $\varphi_{\theta\rho}$ *является взаимно однозначным*.[1]

[1] Верно и обратное утверждение, но мы не будем его доказывать, поскольку оно не используется в дальнейшем.

Рассмотрим такие элементы $b_1, b_2 \in A_{\theta\cap\rho}$, что $\varphi_{\theta\rho}(b_1) = \varphi_{\theta\rho}(b_2)$. Существуют такие элементы $b_1', b_2' \in A$, что

$$\pi_{\theta\cap\rho}(b_i') = b_i. \tag{2.1}$$

Опять из равенств (1.1) следует

$$\begin{aligned}&\left(\pi_\theta(b_1'), \pi_\rho(b_1')\right) = \left(\pi_{\theta\,\theta\cap\rho}(b_1), \pi_{\rho\,\theta\cap\rho}(b_1)\right) = \\ &= \left(\pi_{\theta\,\theta\cap\rho}(b_2), \pi_{\rho\,\theta\cap\rho}(b_2)\right) = \left(\pi_\theta(b_2'), \pi_\rho(b_2')\right).\end{aligned}$$

Равенство $\pi_\theta(b_1') = \pi_\theta(b_2')$ означает, что $(b_1', b_2') \in \theta$. Также получаем, что $(b_1', b_2') \in \rho$. Поэтому $(b_1', b_2') \in \theta \cap \rho$. Отсюда и из равенства (2.1) следует $b_1 = b_2$.

Таким образом, отображение $\varphi_{\theta\rho}$ инъективно.

Теперь будем считать отношения θ, ρ перестановочными. Поскольку рассматриваемое отображение инъективно, нам нужно только доказать, что оно сюръективно.

Пусть $(c, d) \in A_\theta \times_{A_{\theta\cup\rho}} A_\rho$. Пусть c', d' — такие элементы, что $c = \pi_\theta(c')$, $d = \pi_\rho(d')$. Из равенств (1.1) и определений расслоенного произведения следует

$$\pi_{\theta\cup\rho}(c') = \pi_{\theta\cup\rho\,\theta}\left(\pi_\theta(c')\right) = \pi_{\theta\cup\rho\,\rho}\left(\pi_\rho(d')\right) = \pi_{\theta\cup\rho}(d').$$

Таким образом, $(c', d') \in \theta \cup \rho$.

Так как отношения θ, ρ перестановочны, то выполняется равенство $\theta \cup \rho = \theta\rho$ (см. [5, с. 20]). Следовательно, существует такой элемент $b' \in A$, что $(c', b') \in \theta, (b', d') \in \rho$. Полагаем $b = \pi_{\theta\cap\rho}(b')$. Теперь, используя равенства (1.1), имеем

$$\pi_{\theta\,\theta\cap\rho}(b) = \pi_\theta(b') = \pi_\theta(c') = c,$$

$$\pi_{\rho\,\theta\cap\rho}(b) = \pi_\rho(b') = \pi_\rho(d') = d.$$

Окончательно получаем, что $\varphi_{\theta\rho}(b) = (c, d)$ и отображение сюръективно. ■

Следствие 2.1. *Для любых элементов θ, ρ однородной перестановочной решетки $\mathcal{L}$ выполняется равенство* $[\theta : \theta\cap\rho] = [\theta\cup\rho : \rho]$.

Из леммы 2.3 следует

$$\begin{gathered}\left|A_{\theta\cap\rho}\right|=\left|A_\theta\times_{A_{\theta\cup\rho}}A_\rho\right|=\sum_{d\in A_{\theta\cup\rho}}\left|\mathcal{F}(d,\theta)\times\mathcal{F}(d,\rho)\right|= \\ =\left|A_{\theta\cup\rho}\right|\frac{\left|A_\theta\right|}{\left|A_{\theta\cup\rho}\right|}\frac{\left|A_\rho\right|}{\left|A_{\theta\cup\rho}\right|}=\frac{\left|A_\theta\right|\left|A_\rho\right|}{\left|A_{\theta\cup\rho}\right|}, \\ [\theta:\theta\cap\rho]=\frac{\left|A_\theta\right|}{\left|A_{\theta\cap\rho}\right|}=\frac{\left|A_\theta\right|\left|A_{\theta\cup\rho}\right|}{\left|A_\theta\right|\left|A_\rho\right|}=\frac{\left|A_{\theta\cup\rho}\right|}{\left|A_\rho\right|}=[\theta\cup\rho:\rho].\end{gathered} \tag{2.2}$$

■

§ 3. Метод последовательного группирования

Следующие определения, связанные с уравнениями и системами уравнений являются модификацией определений, введенных Г. В. Балакиным (см. [2]).

Для произвольных множеств Y, Z через Z^Y будем обозначать множество всех отображений из множества Y в множество Z.

Пусть A, B — конечные множества. Тогда каждую пару $(f,b)\in B^A\times B$ будем называть *уравнением*. Его обычно записывают в виде формулы

$$f(x)=b, \tag{3.1}$$

где x — переменная со значением в A. Будем называть ее неизвестной переменной или, короче, *неизвестным*. Множество A будем называть *областью значений неизвестной переменной*. Функция f называется левой частью уравнения (3.1). Как обычно, будем предполагать, что существует эффективный алгоритм, вычисляющий значение функции f на каждом элементе множества A.

Соответственно, *системой уравнений* называется множество, состоящее из нескольких уравнений $(f_1,b_1),...,(f_m,b_m)$ с общей областью значений неизвестных переменных. Другими словами, отображения $f_1,...,f_m$ имеют общую область определения A. При этом их области значений $B_1,...,B_m$ могут быть различными.

Формально система уравнений является более общим понятием, чем понятие уравнения, однако рассмотрение системы $(f_1,b_1),...,(f_m,b_m)$ эквивалентно рассмотрению уравнения

$$\left(\left(\bigtimes_{i=1}^{m}\right)f_i,(b_1,...,b_m)\right), \tag{3.2}$$

где

$$\left(\left(\times\right)_{i=1}^{m} f_i \right)(a) = \left(f_1(a), \ldots, f_m(a) \right).$$

Поэтому в дальнейших рассмотрениях мы будем в основном говорить об уравнениях, а не о системах уравнений.

Множество всех решений уравнения (f, b), т. е. множество таких элементов $a \in A$, что $f(a) = b$, будем обозначать через $\mathrm{Sol}(f, b)$, а число различных решений — через $\xi(f, b)$. Будем говорить, что некоторый алгоритм *решает* рассматриваемое уравнение, если он последовательно строит все элементы множества $\mathrm{Sol}(f, b)$.

Для решения уравнения (3.1) применим метод *лобовой атаки* [9, гл. 7], состоящий в последовательном переборе элементов множества A с помощью одного из описанных выше алгоритмов и подстановки их в уравнение. В соответствии с результатами § 1 его трудоемкость равна $t|A|$. Величина t зависит от параметров использованных деревьев. Для большинства практических случаев t мало отличается от 1, и в качестве трудоемкости метода лобовой атаки можно принять величину $|A|$. Таким образом, трудоемкость построения одного решения равна $\dfrac{|A|}{\xi(f, b)}$.

Для сокращения трудоемкости можно использовать метод *ветвей и границ* [7, с. 140]. Укажем условия, при которых это возможно.

Во-первых, предположим, что для каждого отношения $\theta \in \mathcal{L}$ найдется такое эффективно вычислимое отображение $\iota_\theta : A_\theta \to A$, что $\pi_\theta \iota_\theta = 1_{A_\theta}$. Отметим, что это требование заведомо выполнено, если в качестве A_θ взято множество представителей классов эквивалентности.

Во-вторых, будем считать, что множество B является $\mathcal{M}$-множеством для некоторой перестановочной однородной подрешетки $\mathcal{M} \subseteq \mathcal{E}(B)$, содержащей элементы Δ_B и ∇_B. В частности, для уравнений вида (3.2), соответствующих системам уравнений, область значений правой части является прямым произведением $\prod_{i=1}^{m} B_i$, и в качестве $\mathcal{M}$ естественно рассмотреть решетку конгруэнций этого произведения.

Проведем для этой решетки $\mathcal{M}$ такие же построения, которые были выше проведены для множества A и отношений эквивалентности на множе-

стве A. В результате получим множества $\langle B_\alpha \,|\, \alpha \in \mathcal{M} \rangle$ и отображения $\sigma_\alpha : B \to B_\alpha$, $\sigma_{\alpha\beta} : B_\beta \to B_\alpha$ при $\beta \subseteq \alpha$. Потребуем, чтобы каждое отображение σ_α могло быть эффективно вычислено.

Отображение $\upsilon : \mathcal{M} \to \mathcal{L}$ называется *нижним гомоморфизмом*, если $\upsilon(\nabla_B) = \nabla_A$ и $\upsilon(\alpha \cap \beta) = \upsilon(\alpha) \cap \upsilon(\beta)$ при всех $\alpha, \beta \in \mathcal{M}$. Двойственным образом определяется понятие *верхнего гомоморфизма* $\tau : \mathcal{L} \to \mathcal{M}$.

Лемма 3.1. *Для любого нижнего гомоморфизма* $\upsilon : \mathcal{M} \to \mathcal{L}$ *найдется единственный верхний гомоморфизм* $\tau : \mathcal{L} \to \mathcal{M}$, *удовлетворяющий условию*

$$\big(\theta \subseteq \upsilon(\alpha)\big) \Leftrightarrow \big(\tau(\theta) \subseteq \alpha\big). \tag{3.3}$$

Для произвольного элемента $\theta \in \mathcal{L}$ имеем $\theta \subseteq \nabla_A = \upsilon(\nabla_B)$. Поэтому множество $\mathrm{T}(\theta) = \big\langle \alpha \in \mathcal{M} \,\big|\, \theta \subseteq \upsilon(\alpha) \big\rangle$ не пусто. Если $\alpha \in \mathrm{T}(\theta)$, $\beta \in \mathcal{M}$ и $\alpha \subseteq \beta$, то

$$\theta \subseteq \upsilon(\alpha) = \upsilon(\alpha \cap \beta) = \upsilon(\alpha) \cap \upsilon(\beta) \subseteq \upsilon(\beta)$$

и $\beta \in \mathrm{T}(\theta)$. Если $\alpha, \beta \in \mathrm{T}(\theta)$, то

$$\theta \subseteq \upsilon(\alpha) \cap \upsilon(\beta) = \upsilon(\alpha \cap \beta)$$

и $\alpha \cap \beta \in \mathrm{T}(\theta)$. Таким образом, множество $\mathrm{T}(\theta)$ является фильтром. Поскольку решетка $\mathcal{M}$ конечна, каждый фильтр является главным. Пусть $\tau(\theta)$ — элемент, порождающий фильтр $\mathrm{T}(\theta)$. Теперь выполнение условия (3.3) вытекает непосредственно из построений.

Так как элемент Δ_A является наименьшим элементом решетки $\mathcal{L}$, то неравенство $\Delta_A \subseteq \upsilon(\alpha)$ выполняется для всех $\alpha \in \mathcal{M}$. Поэтому $\mathrm{T}(\Delta_A) = \mathcal{M}$ и $\tau(\Delta_A) = \Delta_B$.

Пусть $\theta, \rho \in \mathcal{L}$. Тогда

$$\big(\theta \cup \rho \subseteq \upsilon(\alpha)\big) \Leftrightarrow \big(\big(\theta \subseteq \upsilon(\alpha)\big) \& \big(\rho \subseteq \upsilon(\alpha)\big)\big).$$

Поэтому $\mathrm{T}(\theta \cup \rho) = \mathrm{T}(\theta) \cap \mathrm{T}(\rho)$ и $\tau(\theta \cup \rho) = \tau(\theta) \cup \tau(\rho)$.

Допустим, что существует другое отображение τ', удовлетворяющее условию леммы. Тогда имеем

$$\big(\tau(\theta) \subseteq \tau(\theta)\big) \Rightarrow \big(\theta \subseteq \rho(\tau(\theta))\big) \Rightarrow \big(\tau'(\theta) \subseteq \tau(\theta)\big).$$

Обратное неравенство доказывается симметричным образом. ■

Выберем и фиксируем произвольный нижний гомоморфизм $\upsilon : \mathcal{M} \to \mathcal{L}$ и верхний гомоморфизм $\tau : \mathcal{L} \to \mathcal{M}$, удовлетворяющий условию (3.3). Полагаем

$$\mathfrak{H}(\upsilon) = \left\langle (\theta, \alpha) \in \mathcal{L} \times \mathcal{M} \;\middle|\; \theta \subseteq \upsilon(\alpha) \right\rangle.$$

Через $\mathfrak{F}(A, B; \upsilon)$ обозначим множество таких отображений $g : A \to B$, что для каждого элемента $\alpha \in \mathcal{M}$ справедливо включение

$$\ker(\sigma_\alpha g) \supseteq \upsilon(\alpha). \tag{3.4}$$

Теорема 3.1. *Пусть* $g \in \mathfrak{F}(A, B; \upsilon)$. *Тогда для каждой пары* $(\theta, \alpha) \in \mathfrak{H}(\upsilon)$ *существует единственное отображение* $g_\alpha^\theta : A_\theta \to B_\alpha$, *для которого выполняется равенство* $\sigma_\alpha g = g_\alpha^\theta \pi_\theta$. *Если пара* (ρ, β) *также принадлежит множеству* $\mathfrak{H}(\upsilon)$ *и* $\theta \subseteq \rho, \alpha \subseteq \beta$, *то* $\sigma_{\beta\alpha} g_\alpha^\theta = g_\beta^\rho \pi_{\rho\theta}$.

Единственность легко следует из того, что отображение π_θ сюръективно.

Рассмотрим произвольный элемент $a \in A$. Имеем

$$\pi_\theta \left(\imath_\theta \pi_\theta (a) \right) = \pi_\theta \imath_\theta \left(\pi_\theta (a) \right) = \pi_\theta (a).$$

Таким образом,

$$\left(a, \imath_\theta \pi_\theta (a) \right) \in \theta.$$

Из определений следует, что

$$\ker(\sigma_\alpha g) \supseteq \upsilon(\alpha) \supseteq \theta.$$

Поэтому

$$\sigma_\alpha g (a) = \sigma_\alpha g \left(\imath_\theta \pi_\theta (a) \right) = \left(\sigma_\alpha g \imath_\theta \right) \left(\pi_\theta (a) \right)$$

и отображение $g_\alpha^\theta = \sigma_\alpha g \imath_\theta$ удовлетворяет требуемому равенству.

Подчеркнем, что при сделанных предположениях из эффективной вычислимости отображения g вытекает эффективная вычислимость всех отображений g_α^θ.

Далее, воспользовавшись равенствами (1.1) и аналогичными равенствами для отображений $\sigma_{\beta\alpha}$, получим

$$\sigma_{\beta\alpha} g_\alpha^\theta \pi_\theta = \sigma_{\beta\alpha} \sigma_\alpha g = \sigma_\beta g = g_\beta^\rho \pi_\rho = g_\beta^\rho \pi_{\rho\theta} \pi_\theta.$$

Так как отображение π_θ сюръективно, то левую и правую части последнего равенства можно сократить на него, что и дает нужное равенство. ■

Отображение $g^\theta_{\tau(\theta)}$ будем обозначать через g^θ, а пару $\left(g^\theta, \sigma_{\tau(\theta)}(b)\right)$ — через $(g,b)^\theta$.

Следствие 3.1. *Пусть* $f \in \mathfrak{F}(A,B;\upsilon)$ *и элемент* $a \in A$ *является решением уравнения* (3.1)*. Тогда элемент* $\pi_\theta(a)$ *является решением уравнения*

$$f^\theta(y) = \sigma_{\tau(\theta)}(b).$$

Утверждение очевидным образом вытекает из теоремы 3.1. ■

Рассмотрим один из маршрутов $\vec{\theta} = \theta_0, \theta_1, ..., \theta_n \in \mathfrak{M}(\mathcal{L})$. Введем в алгоритм $\mathfrak{A}_{\mathcal{D}(\vec{\theta})}$ дополнительный критерий *допустимости* вершины, основанный на следствии 3.1. В результате получаем алгоритм $\mathfrak{B}_{\mathcal{D}(\vec{\theta})}$ решения уравнения (3.1):

1. $k := 0, c_0 := o$, где o — единственный элемент множества A_{∇_A}.
2. Пока $k < n-1$, выполняем операции:
   Переменной c_{k+1} присваиваем значение, равное начальному элементу множества $\mathcal{F}(c_k, \theta_{k+1})$;
   Пока c_{k+1} не является конечным элементом множества $\mathcal{F}(c_k, \theta_{k+1})$ и $f^{\theta_{k+1}}(c_{k+1}) \neq \sigma_{\tau(\theta_{k+1})}(b)$, выполняем операцию $c_{k+1} := \mathrm{Next}(c_{k+1})$;
   Если $f^{\theta_{k+1}}(c_{k+1}) = \sigma_{\tau(\theta_{k+1})}(b)$, то $k := k+1$ и возврат на начало шага 2. В противном случае переход к шагу 4.
3. Перебираем элементы множества $\mathcal{F}(c_{n-1}, \Delta_A)$. Каждый опробованный элемент подставляется в исходное уравнение. Элементы, ему удовлетворяющие, поступают на выход.
4. Пока $k > 0$ и c_k не является конечным элементом множества $\mathcal{F}(c_{k-1}, \theta_k)$, выполняем операцию $k := k-1$. Если $k = 0$, то выполнение алгоритма прекращается.
5. Полагаем $c_k := \mathrm{Next}(c_k)$. Возврат на шаг 2.

Пусть $i \in \{0,1,...,n-1\}$. Из описания алгоритма следует, что для каждого элемента $c \in A_{\theta_i}$, удовлетворяющего равенству

$$f^{\theta_i}(c) = \sigma_{\tau(\theta_i)}(b),$$

проводится перебор элементов множества $\mathcal{F}(c, \theta_{i+1})$. В силу однородности решетки $\mathcal{L}$ мощность этого множества равна $[\theta_i : \theta_{i+1}]$. Таким образом, переборная трудоемкость описанного алгоритма решения уравнения (3.1) равна

$$T\left((f,b);\vec{\theta}\right) = \sum_{i=0}^{n-1} \xi\left((f,b)^{\theta_i}\right)[\theta_i : \theta_{i+1}].$$

Пусть $\mathbb{U}(\upsilon) = \mathfrak{F}(A,B;\upsilon) \times B$. Множество $\mathbb{U}(\upsilon)$, как и любое конечное множество, можно рассматривать как измеримое пространство, любое подмножество которого измеримо.

Распределением вероятностей на множестве $\mathbb{U}(\upsilon)$ называется любая заданная на нем неотрицательная функция p, удовлетворяющая условию

$$\sum_{(f,b)\in\mathbb{U}} p(f,b) = 1 \tag{3.5}$$

(см. [3, с. 14]). Каждая такая функция определяет на множестве $\mathbb{U}(\upsilon)$ вероятностную меру **P**, для которой $\mathbf{P}(F) = \sum_{(f,b)\in F} p(f,b)$, что превращает множество $\mathbb{U}(\upsilon)$ в вероятностное пространство $\langle \mathbb{U}; p \rangle$ элементарных событий. Так же, как в работе [2], событие (f,b) означает, что было выбрано соответствующее уравнение.

Из того, что каждое подмножество множества $\mathbb{U}(\upsilon)$ измеримо, легко выводится, что каждое отображение $\chi : \mathbb{U}(\upsilon) \to E$ в измеримое множество E измеримо. Поэтому в соответствии с определением [8, с. 221] каждое такое отображение $\chi : \mathbb{U}(\upsilon) \to E$ является *случайным элементом со значением в множестве E*, или *E-элементом*. В частности, тождественное отображение $1_{\mathbb{U}(\upsilon)} : \mathbb{U}(\upsilon) \to \mathbb{U}(\upsilon)$ является *случайным уравнением* $\mathbf{\Phi}_p$ *со значением в множестве* $\mathbb{U}(\upsilon)$, а ограничения проекций $B^A \times B \to B^A$ и $B^A \times B \to B$ на множество $\mathbb{U}$ являются соответственно *случайной функцией* φ_p и *случайной правой частью* ω_p. Кроме того, любая вещественная

функция G, определенная на множестве $\mathbb{U}(\upsilon)$, становится случайной величиной $G(\Phi_p)$.

В частности, определены случайные величины $T(\Phi_p;\vec{\theta})$ и $\xi(\Phi_p^\theta)$. Математическое ожидание первой из них

$$\mathbf{E}T(\Phi_p;\vec{\theta}) = \sum_{i=0}^{n-1} [\theta_i : \theta_{i+1}]\, \mathbf{E}\xi(\Phi_p^{\theta_i}) \tag{3.6}$$

является средней трудоемкостью алгоритма, и именно ее следует использовать в качестве оценки эффективности алгоритма при заданных вероятностях выбора уравнений.

Выбор функции p зависит от конкретных условий задачи. Часто рассматриваются функции p, для которых

$$p(f,b) = q(f)\frac{1}{|B|}. \tag{3.7}$$

Соответствующее случайное уравнение Φ_p называется случайным уравнением с *независимой равномерно распределенной правой частью*.

Лемма 3.2. *Пусть* Φ_p *— случайное уравнение с независимой равномерно распределенной правой частью со значениями в множестве* $\mathbb{U}(\upsilon)$. *Тогда* $\mathbf{E}\xi(\Phi_p^\theta) = \dfrac{|A_\theta|}{|B_{\tau(\theta)}|}$ *для любого отношения* $\theta \in \mathcal{L}$.

Пусть функция p имеет вид (3.7).

Для каждого элемента $c \in A_\theta$ полагаем

$$\zeta_c(f,b) = \begin{cases} 1, & f^\theta(c) = \sigma_{\tau(\theta)}(b); \\ 0, & f^\theta(c) \neq \sigma_{\tau(\theta)}(b). \end{cases}$$

Другими словами, ζ_c есть индикатор события: «элемент c является решением уравнения Φ_p^θ». Нетрудно видеть, что

$$\xi\left((f,b)^\theta\right) = \sum_{c\in A_\theta} \zeta_c(f,b),$$

откуда следует

$$\mathbf{E}\xi(\Phi_p^\theta) = \sum_{c\in A_\theta} \mathbf{E}\zeta_c(\Phi_p). \tag{3.8}$$

Замечаем, что для любого отображения $f : A \to B$ справедливо равенство

$$\left\langle b \in B \,\middle|\, f^{\theta}(c) = \sigma_{\tau(\theta)}(b) \right\rangle = \mathcal{F}\left(\sigma_{\tau(\theta)}(b), \Delta_B\right).$$

Поэтому

$$\sum_{b \in B} \zeta_c(f,b) = \left| \left\langle b \in B \,\middle|\, f^{\theta}(c) = \sigma_{\tau(\theta)}(b) \right\rangle \right| = \left| \mathcal{F}\left(\sigma_{\tau(\theta)}(b), \Delta_B\right) \right| = \frac{|B|}{\left|B_{\tau(\theta)}\right|},$$

$$\mathbf{E}\zeta_c(\Phi_p) = \sum_{(f,b)} \zeta_c(f,b)\, p(f,b) = \sum_{(f,b)} \zeta_c(f,b)\, q(f) \frac{1}{|B|} =$$

$$= \sum_{f} q(f) \frac{1}{|B|} \sum_{b} \zeta_c(f,b) = \sum_{f} q(f) \frac{1}{|B|} \frac{|B|}{\left|B_{\tau(\theta)}\right|} = \frac{1}{\left|B_{\tau(\theta)}\right|}.$$

Отсюда и из равенства (3.8) вытекает нужное нам утверждение. ■

Теорема 3.2. *Пусть* Φ_p *— случайное уравнение с независимой равномерно распределенной правой частью со значениями в множестве* $\mathbb{U}(\upsilon)$, $\vec{\theta} = \theta_0, \theta_1, \ldots, \theta_n \in \mathfrak{M}(\mathcal{L})$. *Тогда средняя переборная трудоемкость алгоритма* $\mathfrak{B}_{\mathcal{D}(\vec{\theta})}$ *равна*

$$\mathbf{E}T\left(\Phi_p; \vec{\theta}\right) = \sum_{i=0}^{n-1} [\theta_i : \theta_{i+1}] \frac{\left|A_{\theta_i}\right|}{\left|B_{\tau(\theta_i)}\right|}.$$

■

§ 4. Оптимизация маршрута

Маршрут $\vec{\theta}$, на котором достигается минимум величины (3.6), назовем *оптимальным* для случайного уравнения Φ_p. Естественно, возникает задача построения хотя бы одного оптимального маршрута. Данная задача является классической для теории графов, и для ее решения предложено несколько алгоритмов. Выделим среди них алгоритмы Форда–Беллмана и Дейкстры [1, гл. 10], определяющие оптимальный маршрут за $O\left(N^3\right)$ и $O\left(N^2\right)$ операций соответственно. В нашем случае N равно мощности решетки $\mathcal{L}$.

В настоящем разделе мы покажем, что в наших условиях существует возможность указать одну или несколько «опорных» точек, через которые

заведомо проходит один из оптимальных маршрутов. Это сводит построение оптимального маршрута к построению оптимальных маршрутов между опорными точками.

В дальнейшем множество $\{1,2,...,k\}$ будем обозначать через $\mathcal{I}_k$.

Как обычно, для произвольного подмножества $\Theta \subseteq \mathcal{L}$ и произвольного элемента $\rho \in \mathcal{L}$ через $\Theta \cup \rho$ и $\Theta \cap \rho$ обозначаем множества $\langle \sigma \in \mathcal{L} \mid \exists \theta \in \Theta : \sigma = \theta \cup \rho \rangle$ и $\langle \sigma \in \mathcal{L} \mid \exists \theta \in \Theta : \sigma = \theta \cap \rho \rangle$ соответственно. Полагаем $\Theta \circ \rho = (\Theta \cup \rho) \cup (\Theta \cap \rho)$.

Лемма 4.1. *Пусть Θ — максимальная цепь решетки $\mathcal{L}$. Тогда для любого элемента $\rho \in \mathcal{L}$ множество $\Theta \circ \rho$ также является максимальной цепью.*

Пусть $\Theta = \{\theta_0, \theta_1, ..., \theta_n\}$ и $\theta_0 \supset \theta_1 \supset ... \supset \theta_n$. Отметим, что $\theta_0 = \nabla_A$, $\theta_n = \Delta_A$. В противном случае цепь Θ можно было бы увеличить, добавив к ней один из элементов ∇_A, Δ_A.

Ясно, что для каждого номера $i \in \mathcal{I}_n$ справедливы включения

$$\theta_{i-1} \cup \rho \supseteq \theta_i \cup \rho, \tag{4.1}$$

$$\theta_{i-1} \cap \rho \supseteq \theta_i \cap \rho. \tag{4.2}$$

Из включений (4.1) следует, что множество $\Theta \cup \rho$ является цепью, а из включений вида (4.2) следует, что цепью является множество $\Theta \cap \rho$. Кроме того, для любых номеров i, j имеем $\theta_i \cup \rho \supseteq \rho \supseteq \theta_j \cap \rho$. Отсюда легко следует, что множество $\Theta \circ \rho$ является цепью, и нам нужно доказать ее максимальность.

Пусть $j_1, ..., j_m$ — возрастающая последовательность, составленная из всех номеров $i \in \mathcal{I}_n$, для которых включение (4.1) строгое. Дополним эту последовательность числом $j_0 = 0$. Для номеров $i \in \{0,1,...,m\}$ полагаем $\sigma_i = \theta_i \cup \rho$. Из построений следует, что для любого номера $k \in \mathcal{I}_m$ справедлива формула

$$\sigma_{k-1} = \theta_{j_{k-1}} \cup \rho = \theta_{j_{k-1}+1} \cup \rho = ... = \theta_{j_k - 1} \cup \rho \supset \theta_{j_k} \cup \rho = \sigma_k. \tag{4.3}$$

Кроме того,

$$\sigma_m = \theta_{j_m} \cup \rho = \theta_{j_m+1} \cup \rho = ... = \theta_n \cup \rho = \rho. \tag{4.4}$$

Из этих формул следует, что элементы $\sigma_0, \sigma_1, ..., \sigma_m$ различны и $\Theta \cup \rho = \{\sigma_0, \sigma_1, ..., \sigma_m\}$.

Пусть теперь $t_1,...,t_l$ — возрастающая последовательность, составленная из всех номеров $i \in \mathcal{I}_n$, для которых строгим является включение (4.2). Дополним ее элементом $t_0 = 0$. Для каждого номера $i \in \mathcal{I}_l$ полагаем

$$\sigma_{m+i} = \theta_{t_i} \cap \rho. \tag{4.5}$$

Из формулы (4.4) следует, что

$$\sigma_m = \rho = \nabla_A \cap \rho = \theta_{t_0} \cap \rho.$$

Поэтому равенство (4.5) выполняется и при $i = 0$. Теперь так же, как выше, показываем, что для любого номера $k \in \mathcal{I}_l$ справедлива формула

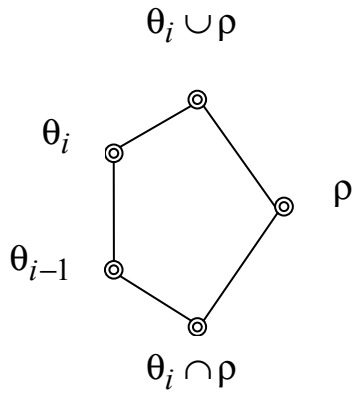
$$\begin{aligned} \sigma_{m+k-1} &= \theta_{j_{m+k-1}} \cap \rho = \theta_{j_{m+k-1}+1} \cap \rho = ... = \\ &= \theta_{j_{m+k}-1} \cap \rho \supset \theta_{j_{m+k}} \cap \rho = \sigma_{m+k} \end{aligned} \tag{4.6}$$

и что $\Theta \cap \rho = \{\sigma_m, \sigma_{m+1}, ..., \sigma_{m+l}\}$.

Таким образом, $\Theta \circ \rho = \{\sigma_0, \sigma_1, ..., \sigma_{m+l}\}$.

Поскольку решетка $\mathcal{L}$ модулярна, к ней применима теорема Жорда–Гёльдера, которая утверждает, что все максимальные цепи решетки $\mathcal{L}$ имеют одинаковую мощность. Поэтому $m + l \le n$, причем равенство имеет место тогда и только тогда, когда цепь $\Theta \circ \rho$ максимальна.

Допустим, что существует такой номер $i \in \mathcal{I}_n$, что оба включения (4.1) и (4.2) являются равенствами. Тогда решетка $\mathcal{L}$ содержит в качестве подрешетки изображенный на рисунке пентагон, что противоречит ее модулярности.



Поэтому для каждого номера i хотя бы одно из включений оказывается строгим. Другими словами, каждый номер $i \in \mathcal{I}_n$ принадлежит хотя бы одному из множеств $J = \{j_1,...,j_m\}$, $T = \{t_1,...,t_l\}$. Поэтому $m + l \geq n$, причем равенство имеет место тогда и только тогда, когда

$$J \cup T = \mathcal{I}_n, \quad J \cap T = \varnothing. \tag{4.7}$$

Таким образом $m + l = n$, откуда следуют максимальность интересующей нас цепи и справедливость равенств (4.7). ■

Рассмотрим произвольный маршрут $\vec{\theta} = \theta_0, \theta_1, ..., \theta_n$, принадлежащий множеству $\mathfrak{M}(\mathcal{L})$, и элемент $\rho \in \mathcal{L}$. В силу леммы 2.1 множество $\Theta = \{\theta_0, \theta_1, ..., \theta_n\}$ является максимальной цепью. Поэтому множество $\Theta \circ \rho$ также является максимальной цепью. Опять применив лемму 2.1, получаем, что последовательность $\sigma_0, \sigma_1, ..., \sigma_n$, построенная при доказательстве леммы 4.1, является маршрутом, принадлежащим множеству $\mathfrak{M}(\mathcal{L})$. Этот маршрут будем обозначать через $\vec{\theta} \circ \rho$.

Следствие 4.1. *Пусть* $\vec{\theta} = \theta_0, \theta_1, ..., \theta_n$, $\vec{\sigma} = \sigma_0, \sigma_1, ..., \sigma_n$ *— маршруты, принадлежащие множеству* $\mathfrak{M}(\mathcal{L})$ *и* $\vec{\sigma} = \vec{\theta} \circ \rho$. *Тогда*

1. *Маршрут* $\vec{\sigma}$ *проходит через точку* ρ.

2. *Если* $\theta_k \supseteq \rho \supseteq \theta_r$, *то* $(\theta_0,...,\theta_k) = (\sigma_0,...,\sigma_k)$, $(\theta_r,...,\theta_n) = (\sigma_r,...,\sigma_n)$.

3. *Существует такая перестановка* ψ *множества* $\mathcal{I}_n$, *что для каждого номера* $i \in \mathcal{I}_n$ *выполняется одно из следующих условий:*

$$\left(\sigma_{\psi(i)-1} = \theta_{i-1} \cup \rho\right) \& \left(\sigma_{\psi(i)} = \theta_i \cup \rho\right), \tag{4.8}$$

$$\left(\sigma_{\psi(i)-1} = \theta_{i-1} \cap \rho\right) \& \left(\sigma_{\psi(i)} = \theta_i \cap \rho\right). \tag{4.9}$$

Будем использовать объекты, построенные при доказательстве леммы 4.1.

Первое утверждение вытекает из формулы (4.4), которая показывает, что $\sigma_m = \rho$.

Допустим, что $\theta_k \supseteq \rho$. Тогда для всех номеров $i \in \mathcal{I}_k$ имеем $\theta_{i-1} \cup \rho = \theta_{i-1} \supset \theta_i = \theta_i \cup \rho$. Таким образом, из построений леммы 4.1 следует, что $j_i = i$ и $\sigma_i = \theta_i \cup \rho = \theta_i$. Равенство $\sigma_0 = \theta_0$ вытекает из определения множества $\mathfrak{M}(\mathcal{L})$.

Второе из равенств п. 2 доказывается аналогично.

Из равенства (4.7) следует, что в строке $(j_1,...,j_m,t_1,...,t_l)$ по одному разу встречаются все элементы множества $\mathcal{I}_n$, что позволяет использовать ее в качестве нижней строки перестановки ψ. Теперь утверждение п.3 вытекает из равенств (4.3) и (4.6). ■

Пусть d — функция, определенная на множестве $\mathcal{L}$. Для произвольной подрешетки $\mathcal{K} \subseteq \mathcal{L}$, не обязательно содержащей элементы Δ_A, ∇_A, положим

$$D_d(\mathcal{K}) = \min_{\theta \in \mathcal{K}} d(\theta), \quad \mathfrak{D}_d(\mathcal{K}) = \langle \theta \in \mathcal{K} \mid d(\theta) = D_d(\mathcal{K}) \rangle.$$

В частности, функции $D_d, \mathfrak{D}_d$ определены на всех решетках вида

$$\mathcal{L}_{\rho\sigma} = \langle \theta \in \mathcal{L} \mid \rho \subseteq \theta \subseteq \sigma \rangle.$$

Для сокращения обозначений вместо $D_d(\mathcal{L}_{\rho\sigma}), \mathfrak{D}_d(\mathcal{L}_{\rho\sigma})$ будем писать $D_d(\rho,\sigma)$ и $\mathfrak{D}_d(\rho,\sigma)$ соответственно.

Функцию d, определенную на множестве $\mathcal{L}$, назовем *субаддитивной*, если для всех элементов $\theta, \rho \in \mathcal{L}$ выполняется неравенство

$$d(\theta \cup \rho) + d(\theta \cap \rho) \le d(\theta) + d(\rho). \tag{4.10}$$

Следующее утверждение дает важный для нас пример субаддитивной функции.

Лемма 4.2. *Пусть Φ_p — случайное уравнение с независимой равномерно распределенной правой частью со значениями в множестве $\mathbb{U}(\upsilon)$. Тогда функция d, определенная равенством*

$$d(\theta) = \ln \mathbf{E}\xi\left(\Phi_p^\theta\right),$$

является субаддитивной.

Из леммы 3.2 следует

$$d(\theta) = \ln \mathbf{E}\xi\left(\Phi_p^\theta\right) = \ln \frac{|A_\theta|}{\left|B_{\tau(\theta)}\right|} = \ln |A_\theta| - \ln \left|B_{\tau(\theta)}\right|.$$

Отсюда, из равенства (2.2), его аналога для решетки $\mathcal{M}$ отношений на множестве B и равенства $\tau(\theta\cup\rho)=\tau(\theta)\cup\tau(\rho)$ получаем

$$d(\theta\cap\rho)=\ln\left|A_{\theta\cap\rho}\right|-\ln\left|B_{\tau(\theta\cap\rho)}\right|=\ln\left|A_{\theta\cap\rho}\right|-\ln\left|B_{\tau(\theta)\cap\tau(\rho)}\right|+\ln\frac{\left|B_{\tau(\theta)\cap\tau(\rho)}\right|}{\left|B_{\tau(\theta\cap\rho)}\right|}=$$

$$=\ln\frac{\left|A_\theta\right|\left|A_\rho\right|}{\left|A_{\theta\cup\rho}\right|}-\ln\frac{\left|B_{\tau(\theta)}\right|\left|B_{\tau(\rho)}\right|}{\left|B_{\tau(\theta)\cup\tau(\rho)}\right|}+\ln\frac{\left|B_{\tau(\theta)\cap\tau(\rho)}\right|}{\left|B_{\tau(\theta\cap\rho)}\right|}=$$

$$=\cdots d(\theta)+d(\rho)-d(\theta\cup\rho)+\ln\frac{\left|B_{\tau(\theta)\cap\tau(\rho)}\right|}{\left|B_{\tau(\theta\cap\rho)}\right|}.$$

Так как отображение τ монотонно, то $\tau(\theta)\cap\tau(\rho)\supseteq\tau(\theta\cap\rho)$ и

$$\left|B_{\tau(\theta)\cap\tau(\rho)}\right|\le\left|B_{\tau(\theta\cap\rho)}\right|.$$

Поэтому $d(\theta\cap\rho)\le d(\theta)+d(\rho)-d(\theta\cup\rho)$, откуда и следует субаддитивность рассматриваемой функции. ■

В дальнейших рассмотрениях выберем и временно фиксируем субаддитивную функцию d.

Лемма 4.3. *Для любой подрешетки $\mathcal{K}\subseteq\mathcal{L}$ множество $\mathfrak{D}_d(\mathcal{K})$ является подрешеткой.*

Пусть $\theta,\rho\in\mathfrak{D}_d(\mathcal{K})$. Допустим, что $\theta\cup\rho\notin\mathfrak{D}_d(\mathcal{K})$. Так как $\theta\cup\rho\in\mathcal{K}$, то из сделанного предположения и определений вытекает неравенство

$$d(\theta\cup\rho)>D_d(\mathcal{K}).$$

Из тех же соображений следует неравенство

$$d(\theta\cap\rho)\ge D_d(\mathcal{K}).$$

Получаем

$$d(\theta\cup\rho)+d(\theta\cap\rho)>2D_d(\mathcal{K})=d(\theta)+d(\rho),$$

что противоречит неравенству (4.10).

Случай $\theta\cap\rho\notin\mathfrak{D}_d(\mathcal{K})$ рассматривается так же. ■

Лемма 4.4. *Пусть* Φ_p *— такое случайное уравнение со значением в множестве* $\mathbb{U}(\upsilon)$, *что* $\mathbf{E}\xi\left(\Phi_p^{\theta}\right)=h\left(d\left(\theta\right)\right)$, *где* h *— монотонно возрастающая функция. Пусть также* $\vec{\theta}=\theta_0,\theta_1,...,\theta_n$ *— маршрут, принадлежащий множеству* $\mathfrak{M}(\mathcal{L})$, $\rho\in\mathfrak{D}_d\left(\theta_r,\theta_k\right)$ *и* $\vec{\sigma}=\vec{\theta}\circ\rho$. *Тогда* $\mathbf{E}T\left(\Phi_p;\vec{\theta}\right)\geq\mathbf{E}T\left(\Phi_p;\vec{\sigma}\right)$.

Пусть $\vec{\sigma}=\sigma_0,\sigma_1,...,\sigma_n$, ψ — перестановка, удовлетворяющая п.3 следствия 4.1.

Произвольно выберем номер $i\in\mathcal{I}_n$. Предположим, что для выбранного номера выполняется условие (4.8), т. е.

$$\left(\sigma_{\psi(i)-1}=\theta_{i-1}\cup\rho\right)\&\left(\sigma_{\psi(i)}=\theta_i\cup\rho\right).$$

Тогда

$$\theta_{i-1}\cup\sigma_{\psi(i)}=\theta_{i-1}\cup\left(\theta_i\cup\rho\right)=\theta_{i-1}\cup\rho=\sigma_{\psi(i)-1}.$$

Так как при сделанном предположении $\left(\theta_{i-1}\cup\rho\right)\neq\left(\theta_i\cup\rho\right)$, а из включений (4.1) и (4.2) только одно является строгим (см. доказательство леммы 4.1), то $\left(\theta_{i-1}\cap\rho\right)=\left(\theta_i\cap\rho\right)$. Отсюда и из модулярности решетки $\mathcal{L}$ следует

$$\theta_{i-1}\cap\sigma_{\psi(i)}=\theta_{i-1}\cap\left(\theta_i\cup\rho\right)=\theta_i\cup\left(\theta_{i-1}\cap\rho\right)=\theta_i\cup\left(\theta_i\cap\rho\right)=\theta_i.$$

Воспользовавшись следствием 2.1, получим

$$\left[\theta_{i-1}:\theta_i\right]=\left[\theta_{i-1}:\theta_i\cap\sigma_{\psi(i)}\right]=\left[\theta_{i-1}\cup\sigma_{\psi(i)}:\sigma_{\psi(i)}\right]=\left[\sigma_{\psi(i)-1}:\sigma_{\psi(i)}\right].$$

Аналогично показываем, что $\left[\theta_{i-1}:\theta_i\right]=\left[\sigma_{\psi(i)-1}:\sigma_{\psi(i)}\right]$, и в случае, когда для выбранного номера выполняется условие (4.9).

Теперь, используя взаимную однозначность отображения ψ, получаем

$$\mathbf{E}T\left(\Phi_p;\vec{\sigma}\right)=\sum_{i=1}^{n}\left[\sigma_{i-1}:\sigma_i\right]\mathbf{E}\xi\left(\Phi_p^{\sigma_{i-1}}\right)=$$

$$=\sum_{i=1}^{n}\left[\sigma_{\psi(i)-1}:\sigma_{\psi(i)}\right]\mathbf{E}\xi\left(\Phi_p^{\sigma_{\psi(i)-1}}\right)=\sum_{i=1}^{n}\left[\theta_{i-1}:\theta_i\right]\mathbf{E}\xi\left(\Phi_p^{\sigma_{\psi(i)-1}}\right).$$

Отсюда следует, что

$$\mathbf{E}T\left(\Phi_p;\vec{\theta}\right)-\mathbf{E}T\left(\Phi_p;\vec{\sigma}\right)=\sum_{i=1}^{n}[\theta_{i-1}:\theta_i]\left\{\mathbf{E}\xi\left(\Phi_p^{\theta_{i-1}}\right)-\mathbf{E}\xi\left(\Phi_p^{\sigma_{\psi(i)-1}}\right)\right\}=$$

$$=\sum_{i=1}^{n}[\theta_{i-1}:\theta_i]\left\{h\left(d\left(\theta_{i-1}\right)\right)-h\left(d\left(\sigma_{\psi(i)-1}\right)\right)\right\}. \tag{4.11}$$

Продолжим рассмотрение выбранного номера i. Он удовлетворяет одному из трех условий.

A. $r\le i-1\le k$. Тогда $\theta_r\subseteq\theta_{i-1}\subseteq\theta_k$, т. е. $\theta_{i-1}\in\mathcal{L}_{\theta_r\theta_k}$. По определению $\mathfrak{D}_d\left(\theta_r,\theta_k\right)\subseteq\mathcal{L}_{\theta_r\theta_k}$. Поэтому из предположений леммы вытекает включение $\rho\in\mathcal{L}_{\theta_r\theta_k}$. Из включения $\rho\in\mathfrak{D}_d\left(\theta_r,\theta_k\right)$ следует неравенство

$$d\left(\rho\right)=\min_{\delta\in\mathcal{L}_{\theta_r\theta_k}}d\left(\delta\right)\le d\left(\theta_{i-1}\cap\rho\right).$$

Теперь из определения субаддитивной функции следует

$$d\left(\theta_{i-1}\right)-d\left(\sigma_{\psi(i)-1}\right)=d\left(\theta_{i-1}\right)-d\left(\theta_{i-1}\cup\rho\right)\ge$$

$$\ge\left\{d\left(\theta_{i-1}\right)-d\left(\theta_{i-1}\cup\rho\right)\right\}+\left\{d\left(\rho\right)-d\left(\theta_{i-1}\cap\rho\right)\right\}\ge 0.$$

B. $i-1<r$. Тогда $\theta_{i-1}\subset\theta_r$. Как мы видели в предыдущем пункте, $\rho\in\mathcal{L}_{\theta_r\theta_k}$, т. е. $\theta_r\subseteq\rho$. Поэтому $\sigma_{\psi(i)-1}=\theta_{i-1}\cup\rho=\theta_{i-1}$ и $d\left(\sigma_{\psi(i)-1}\right)=d\left(\theta_{i-1}\right)$.

C. $k<i-1$. Так же, как выше, имеем $\rho\supseteq\theta_k\supset\theta_{i-1}\supset\theta_i$. Отсюда следует $\rho=\theta_{i-1}\cup\rho=\theta_i\cup\rho$. Это противоречит условию (4.8), что показывает невозможность данного случая.

Таким образом, выполняется неравенство $d\left(\theta_{i-1}\right)\ge d\left(\sigma_{\psi(i)-1}\right)$. Аналогичные рассмотрения показывают, что последнее неравенство выполняется и в том случае, когда для номера i выполняется условие (4.9). Таким образом, неравенство $d\left(\theta_{i-1}\right)\ge d\left(\sigma_{\psi(i)-1}\right)$ выполняется для всех номеров $i\in\mathcal{I}_n$. Из этих неравенств и равенства (4.11) следует доказываемое утверждение. ■

Теорема 4.1. *Пусть* Φ_p *— случайное* $\mathbb{U}(\upsilon)$*-уравнение с независимой равномерно распределенной правой частью,* $d\left(\theta\right)=\ln\mathbf{E}\xi\left(\Phi_p^{\theta}\right)$. *Тогда для любой цепи* $\rho_1\supset\ldots\supset\rho_m$ *множества* $\mathfrak{D}_d\left(\mathcal{L}\right)$ *существует оптимальный для случайного уравнения* Φ_p *маршрут, содержащий все точки* $\rho_1,\ldots,\rho_m$.

В силу леммы 4.2 функция d субаддитивна. Кроме того, $\ln \mathbf{E}\xi\left(\Phi_p^{\theta}\right)=e^{d(\theta)}$. Поэтому случайное уравнение Φ_p удовлетворяет предположениям леммы 4.4.

Для удобства изложения введем в рассмотрение элемент $\rho_0 = \nabla_A$.

Пусть $\overrightarrow{\theta^0}$ — произвольный оптимальный маршрут. Если уже определен некоторый маршрут $\overrightarrow{\theta^l}$ и $l < m$, то в качестве маршрута $\overrightarrow{\theta^{l+1}}$ возьмем маршрут $\overrightarrow{\theta^l} \circ \rho_{l+1}$.

Методом математической индукции докажем, что *маршрут* $\overrightarrow{\theta^l}$ *оптимален и содержит все точки* $\rho_0, \rho_1, ..., \rho_l$.

Для $l = 0$ утверждение очевидно.

Пусть утверждение верно для числа $l-1$ и $\overrightarrow{\theta^{l-1}} = \theta_0^{l-1}, \theta_1^{l-1}, ..., \theta_n^{l-1}$. По предположению индукции существуют такие числа $k_0, ..., k_{l-1}$, что $\rho_j = \theta_{k_j}^{l-1}$ при всех $j \in \{0,1,...,l-1\}$. Так как элемент θ_i^{l-1} уменьшается с ростом номера i, то $k_0 \le k_1 \le ... \le k_{l-1}$. Кроме того,

$$\theta_{k_{l-1}} = \rho_{l-1} \supseteq \rho_l \supseteq \Delta_A = \theta_n. \tag{4.12}$$

В этих условиях применимо следствие 4.1, которое показывает, что точки $\rho_0, \rho_1, ..., \rho_l$ принадлежат маршруту $\overrightarrow{\theta^l}$.

Далее имеем

$$d(\rho_l) = \min_{\sigma \in \mathcal{L}} d(\sigma) \le \min_{\sigma \in \mathcal{L}_{\theta_{k_{l-1}}\theta_n}} d(\sigma) = \mathfrak{D}_d\left(\theta_{k_{l-1}}, \theta_n\right).$$

Отсюда и из неравенств (4.12) следует, что $\rho_l \in \mathfrak{D}_d\left(\theta_{k_{l-1}}, \theta_n\right)$. Применив лемму 4.4, получаем $\mathbf{E}T\left(\Phi_p; \overrightarrow{\theta^{l-1}}\right) \ge \mathbf{E}T\left(\Phi_p; \overrightarrow{\theta^l}\right)$. Теперь из оптимальности маршрута $\overrightarrow{\theta^{l-1}}$ вытекает оптимальность маршрута $\overrightarrow{\theta^l}$.

Ясно, что маршрут $\overrightarrow{\theta^m}$ удовлетворяет всем требованиям теоремы. ■

Список литературы

1. *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: Графы, матроиды, алгоритмы. — Ижевск: НИЦ «РХД», 2001.
2. *Балакин Г. В.* Введение в теорию случайных уравнений // В сб.: Труды по дискретной математике. Т. 1. — 1997. — С. 1-18.
3. *Боровков А. А.* Теория вероятностей. — М.: «Эдиториал УРСС», 1999.

4. *Гретцер Г.* Общая теория решеток. — М.: «Мир», 1982.
5. *Курош А. Г.* Лекции по общей алгебре. — М.: «Наука», 1973.
6. *Плоткин Б. И.* Группы автоморфизмов алгебраических систем. — М.: «Наука», 1966.
7. *Рейнгольд Э., Нивергельт Ю., Део Н.* Комбинаторные алгоритмы. Теория и практика. — М.: «Мир», 1980.
8. *Ширяев А. Н.* Вероятность-1. — М.: МЦНМО, 2004.
9. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: «Триумф», 2002.