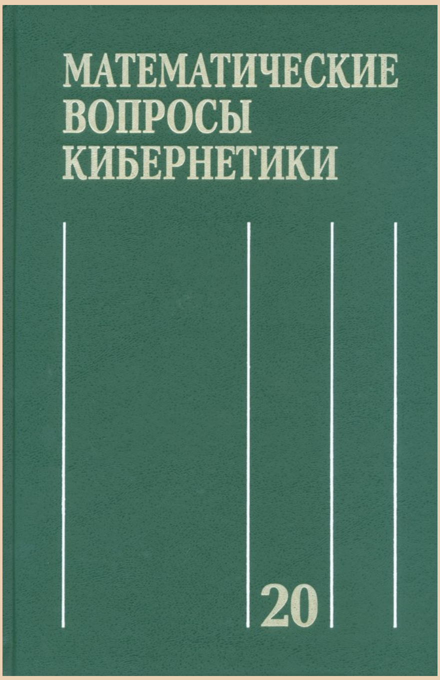


Х. Сайверт,
И. С. Сергеев, С. Юкна

Инверсные входы в арифметических и тропических схемах

ИНВЕРСНЫЕ ВХОДЫ В АРИФМЕТИЧЕСКИХ И ТРОПИЧЕСКИХ СХЕМАХ

Х. САЙВЕРТ, И. С. СЕРГЕЕВ, С. ЮКНА

(ФРАНКФУРТ-НА-МАЙНЕ; МОСКВА; ВИЛЬНЮС / ФРАНКФУРТ-НА-МАЙНЕ)

§ 1. Введение

Одной из наиболее общих задач теории синтеза является исследование влияния эффекта изменения вычислительных возможностей модели на сложность вычисления функции. К этому направлению относится и настоящая работа. Мы изучаем вопрос: может ли вычисление функции арифметической схемой быть существенно ускорено, если разрешить использовать обратные к переменным $x_1, \ldots, x_n$ величины в качестве входов.

В булевых вычислениях роль обратной к x величины играет отрицание $\overline{x}$. Как известно, в любой булевой $(\vee, \wedge, \neg)$-схеме отрицания можно «опустить» на уровень входов ценой увеличения сложности не более чем вдвое. Поэтому результат А. А. Разборова [3] означает, что входы-отрицания позволяют понизить сложность монотонных булевых $(\vee, \wedge)$-схем сверхполиномиально. Позднее Е. Тардош [20] показала, что выигрыш может быть даже экспоненциальным.

Напомним, что *сложность* схемы определяется как число функциональных элементов в ней, а сложность функции — как минимальная сложность реализующей ее схемы. Для удобства, операции, из которых строится схема, мы будем отражать в названии: например, $(+, \cdot)$-схемы — это схемы над базисом $\{+, \cdot\}$.

Мы изучаем эффект добавления инверсных входов в арифметические $(+, \cdot)$-схемы, а также в тропические $(\min, +)$- и $(\max, +)$-схемы. Базовые монотонные версии этих схем в качестве входов используют переменные $x_1, \ldots, x_n$ и произвольные неотрицательные вещественные константы. В случае арифметических схем можно рассмотреть два вида инверсий входов: аддитивные $-x_1, \ldots, -x_n$ и мультипликативные $1/x_1, \ldots, 1/x_n$. Мы обозначаем соответствующие модели как $(+, \cdot, -x_i)$- и $(+, \cdot, 1/x_i)$-схемы. В $(+, \cdot, -)$-схемах разрешается операция вычитания.

Сложность реализации функции $(+, \cdot, -)$- и $(+, \cdot, -x_i)$-схемами практически одна и та же: вычитания всегда могут быть опущены на уровень входов по правилам $-(x+y) = (-x)+(-y)$ и $-x \cdot y = (-x) \cdot y$. Поэтому из результа-

DOI: 10.20948/mvk-2022-61

та Л. Вэльянта [21] следует, что отношение сложностей*) $(+,\cdot)/(+,\cdot,-x_i)$ может быть экспоненциальным. Иначе говоря, аддитивно инверсные входы $-x_i$ позволяют понизить сложность монотонного вычисления (некоторых функций) экспоненциально.

Ф. Штрассен [19] показал, что при доступной операции вычитания $(-)$ деление $(/)$ не может существенно понизить сложность схемы: если многочлен P степени d вычисляется $(+,\cdot,/,-)$-схемой сложности s, то его можно также вычислить $(+,\cdot,-)$-схемой сложности $\mathcal{O}(sd\log d)$. Таким образом, мультипликативные инверсии входов $1/x_1,\ldots,1/x_n$ оказываются малополезными в *немонотонных* вычислениях.

Но может ли операция деления $(/)$ существенно ускорить *монотонные* $(+,\cdot)$-вычисления? Вопрос нетривиален, поскольку метод Штрассена опирается на возможность представления выражения $1/f$ в виде ряда $1/(1-(1-f))=\sum\limits_{i\geqslant 0}(1-f)^i$, который вычисляется при помощи вычитаний. И действительно, аналог результата Штрассена не выполняется для монотонных арифметических схем: здесь деление может экспоненциально понизить сложность.

Экспоненциальное отношение $(+,\cdot)/(+,\cdot,/)$ сложности схем без вычитаний достигается на *многочлене остовных деревьев* (многочлене Кирхгофа) $\kappa_n(x)=\sum\limits_T\prod\limits_{e\in T}x_e$, где суммирование выполняется по всем остовным деревьям полного неориентированного графа K_n на n вершинах. С. Юкна и Х. Сайверт [14] показали, что монотонная арифметическая сложность многочлена κ_n не меньше $2^{\Omega(\sqrt{n})}$. Для ориентированной версии многочлена κ_n (когда K_n — полный ориентированный граф и суммирование выполняется по ориентированным остовным деревьям) нижняя оценка сложности $2^{\Omega(n)}$ была ранее доказана М. Джеррумом и М. Шниром [13]. С другой стороны, С. Фомин, Д. Григорьев и Г. Кошевой [10] недавно показали, что оба многочлена κ_n и его ориентированная версия могут быть вычислены $(+,\cdot,/)$-схемами сложности $\mathcal{O}(n^3)$.

Верхняя оценка $\mathcal{O}(n^3)$ справедлива и в том случае, когда в $(+,\cdot,/)$-схеме разрешается использовать только один элемент деления в самом конце. Действительно, все операции деления можно поднять к выходу схемы по правилам $(x/y)+z=(x+yz)/y$, $(x/y)z=(xz)/y$ и $(x/y)/z=x/(yz)$. Поэтому отношение сложностей $(+,\cdot)/(+,\cdot,/)$ может быть экспоненциально даже если в схеме допускается только один элемент деления (на выходе).

В настоящей работе мы подходим к вопросу с другой стороны: что получается, когда деления разрешены только на входах схемы? Имеют ли $(+,\cdot,1/x_i)$-схемы, т. е. монотонные арифметические схемы с инверсными входами $1/x_1,\ldots,1/x_n$, преимущество перед теми же монотонными схемами без инверсных входов? То, что инверсные входы приводят к экономии сложности, видно на примере многочлена x^{31}. Он может быть вычислен как $x^{32}\cdot(1/x)$ со сложностью 6, однако 7 элементов необходимы любой схеме без инверсных входов, как следует, например, из [1, §4.6.3]. Поэтому правильно поставить вопрос: могут ли $(+,\cdot,1/x_i)$-схемы быть *существенно* проще $(+,\cdot)$-схем?

*) Т. е. сложность реализации одной и той же функции схемами одного типа относительно сложности реализации той же функции схемами другого типа.

Наш ответ отрицательный: отношение $(+,\cdot)/(+,\cdot,1/x_i)$ всегда не более чем квадратично (теорема 1): если многочлен P от n переменных вычисляется $(+,\cdot,1/x_i)$-схемой сложности s, то P можно также реализовать $(+,\cdot)$-схемой сложности $\mathcal{O}(ns^2)$.

Мы также интересуемся влиянием наличия инверсных входов на сложность тропических $(\min,+)$- и $(\max,+)$-схем. Наш интерес вызван тем, что тропические схемы моделируют базовые алгоритмы динамического программирования. Входами тропической схемы являются переменные $x_1,\ldots,x_n$ и неотрицательные вещественные константы; элементы реализуют операции сложения $(+)$ и либо $\min$, либо $\max$. Операция деления x/y в арифметических вычислениях соответствует операции вычитания $x-y$ в тропических. Тропическими версиями арифметических $(+,\cdot,1/x_i)$-схем являются $(\min,+,-x_i)$- и $(\max,+,-x_i)$-схемы.

В тропическом полукольце*) $(\mathbb{R}_+,\min,+)$ многочлену остовных деревьев κ_n соответствует проблема поиска остовного дерева минимального веса MST_n: в полном графе K_n каждому ребру e приписан неотрицательный вес x_e, требуется найти минимальный вес $\sum\limits_{e\in T} x_e$ остовного дерева T в K_n. Как показано в [15], решение этой проблемы требует $(\min,+)$-схем размера $2^{\Omega(\sqrt{n})}$. С другой стороны, поскольку тропические схемы не слабее монотонных арифметических схем, верхняя оценка $\mathcal{O}(n^3)$ [10] сложности многочлена κ_n распространяется на тропические $(\min,+)$-схемы, реализующие MST_n; то же справедливо для $(\max,+)$-схем, вычисляющих $(\max,+)$-версию задачи MST_n. Поэтому отношения сложностей $(\min,+)/(\min,+,-)$ и $(\max,+)/(\max,+,-)$ могут быть экспоненциальными.

Вновь поставим вопрос: как отражается на сложности тропических схем доступ к инверсиям входов? Мы покажем (теорема 2), что отношение $(\min,+)/(\min,+,-x_i)$ всегда не более чем квадратично. В случае тропических $(\max,+,-x_i)$-схем задача оказывается труднее, но все же мы можем доказать (теорема 3), что отношение $(\max,+)/(\max,+,-x_i)$ не более чем квадратично для схем, решающих *однородные* задачи максимизации. Обобщение теоремы 1 на тропические схемы нетривиально, поскольку последние, вообще говоря, сильнее, чем монотонные арифметические схемы. Например, задача поиска кратчайшего пути в графе решается $(\min,+)$-схемой полиномиальной сложности (алгоритм динамического программирования Беллмана — Форда — Мура), но монотонная арифметическая сложность соответствующего многочлена экспоненциальна [13].

§ 2. Результаты

Арифметические схемы. Наш первый результат (теорема 1) показывает, что $(+,\cdot)/(+,\cdot,1/x_i)$ отношение не может быть более чем квадратично. Это значит, что инверсные входы не позволяют существенно понизить сложность монотонных арифметических схем.

Теорема 1. *Если многочлен P от n переменных реализуется $(+,\cdot,1/x_i)$-схемой сложности s, то он также может быть вычислен $(+,\cdot)$-схемой сложности $\mathcal{O}(ns^2)$.*

*) Здесь и далее $\mathbb{R}_+$ обозначает множество всех неотрицательных вещественных чисел.

Из теоремы 1 вытекает следствие, представляющее самостоятельный интерес. Оно относится к монотонной арифметической сложности вычисления «дополняющих» многочленов. Для произвольного подмножества $S \subseteq [n] = \{1, \ldots, n\}$ определим мультилинейный одночлен $X_S = \prod_{i \in S} x_i$. *Дополнением* мультилинейного многочлена $P(x) = \sum_{S \in \mathcal{F}} X_S$ назовем (также мультилинейный) многочлен

$$\text{co-}P(x) := \sum_{S \in \mathcal{F}} \prod_{i \notin S} x_i.$$

Может ли сложность вычисления многочленов P и co-P $(+, \cdot)$-схемами отличаться существенно? Из теоремы 1 следует отрицательный ответ на этот вопрос.

Следствие 1. *Если мультилинейный многочлен P от n переменных реализуется $(+, \cdot)$-схемой сложности s, то его дополнение* co-P *можно вычислить $(+, \cdot)$-схемой сложности $\mathcal{O}(ns^2 + n^3)$.*

Доказательство. Рассмотрим $(+, \cdot)$-схему сложности s, реализующую многочлен $P(x_1, \ldots, x_n) = \sum_{S \in \mathcal{F}} X_S$. Если в нее вместо входов переменных x_i подставить инверсные входы $1/x_i$, то полученная $(+, \cdot, 1/x_i)$-схема сложности s будет вычислять многочлен Лорана*) $P(1/x_1, \ldots, 1/x_n)$. Заметим, что

$$\text{co-}P(x) = \sum_{S \in \mathcal{F}} \prod_{i \notin S} x_i = \prod_{i=1}^{n} x_i \cdot \sum_{S \in \mathcal{F}} \prod_{i \in S} \frac{1}{x_i} = \prod_{i=1}^{n} x_i \cdot P(1/x_1, \ldots, 1/x_n).$$

Таким образом, многочлен co-P реализуется $(+, \cdot, 1/x_i)$-схемой сложности $t = s + n$. Тогда, согласно теореме 1, многочлен co-P можно вычислить $(+, \cdot)$-схемой сложности $\mathcal{O}(nt^2) = \mathcal{O}(ns^2 + n^3)$.

Тропические схемы. Многие алгоритмы динамического программирования являются «чистыми» в том смысле, что они строятся на рекурсивных соотношениях, использующих только операции $(\min, +)$ или $(\max, +)$. К чистым алгоритмам относятся популярные алгоритмы Беллмана — Форда — Мура [5, 11, 16] и Роя — Флойда — Уоршелла [9, 18, 22] поиска кратчайшего пути в графе**), алгоритм Беллмана — Хелда — Карпа [6, 12] решения задачи коммивояжера и алгоритм Дрейфуса — Вагнера — Левина [2, 7] построения дерева Штейнера.

Тропические $(\min, +)$- и $(\max, +)$-*схемы* — это естественная модель для реализации чистых алгоритмов динамического программирования. Такие схемы состоят из двухвходовых $(\min, +)$ или $(\max, +)$ операций. Входами являются переменные***) $x_1, \ldots, x_n$ и любые неотрицательные константы. Иначе говоря, в тропических схемах роль арифметического умножения $(\cdot)$ играет операция сложения $(+)$, а роль арифметического сложения —

*) В многочленах Лорана допускаются отрицательные степени переменных.

**) Первый алгоритм вычисляет кратчайший путь между двумя заданными вершинами, второй — кратчайшие пути между всеми парами вершин.

***) В терминах динамического программирования набор входов переменных тропической схемы также называется *весовым вектором*.

операции min или max. Тропические $(\min,+,-x_i)$- и $(\max,+,-x_i)$-схемы дополнительно используют инверсные входы $-x_1,\ldots,-x_n$.

Тропические $(\min,+)$-схемы вычисляют тропические многочлены $P(x)=\min\limits_{a\in A}\langle a,x\rangle+c_a$, где*) $A\subseteq\mathbb{N}^n$ — конечное множество векторов (показателей степеней мономов в арифметическом случае), $c_a\in\mathbb{R}_+$ — неотрицательные коэффициенты, а $\langle a,x\rangle=a_1x_1+\cdots+a_nx_n$ — скалярное произведение векторов a и x. Аналогично определяются $(\max,+)$-многочлены. Тропические $(\min,+,-x_i)$- и $(\max,+,-x_i)$-схемы вычисляют тропические многочлены Лорана: в этом случае $A\subseteq\mathbb{Z}^n$, т. е. некоторые переменные x_i могут иметь отрицательные показатели степени a_i.

Тропическая схема Φ *вычисляет* тропический многочлен P, если при любом (весовом векторе) $x\in\mathbb{R}_+^n$ выход схемы принимает значение $P(x)$. Два тропических многочлена P и Q от n переменных будем называть *эквивалентными*, если для всех $x\in\mathbb{R}_+^n$ выполнено $P(x)=Q(x)$.

Замечание 1. (Почему неотрицательные входы?) Имеется две причины ограничить рассмотрение неотрицательными наборами входов $x_1,\ldots,x_n\in\mathbb{R}_+$. Во-первых, известные алгоритмы динамического программирования, как правило, эффективны только на неотрицательных входах и не предназначены для работы в ситуациях, когда допускаются отрицательные. Во-вторых, возможности тропических схем при решении оптимизационных задач с любыми наборами входов примерно такие же, как у монотонных арифметических схем (см. [13, след. 2.7]), т. е. переход к модели тропических схем дает мало нового. С другой стороны, если допускаются только неотрицательные входы, то тропические схемы могут быть экспоненциально сильнее монотонных арифметических. Например, задача поиска кратчайшего пути решается полиномиальной $(\min,+)$-схемой методом Беллмана — Форда — Мура, а соответствующий монотонный (арифметический) многочлен имеет экспоненциальную монотонную сложность [13, §4.4].

Следующая теорема является тропическим аналогом теоремы 1 для случая минимизации.

Теорема 2. *Если тропический* $(\min,+)$*-многочлен* $P(x_1,\ldots,x_n)$ *реализуется* $(\min,+,-x_i)$*-схемой сложности* s*, то его также можно вычислить* $(\min,+)$*-схемой сложности* $\mathcal{O}(ns^2)$.

Вопрос с тропическими $(\max,+,-x_i)$-схемами (решающими задачи *максимизации*) оказывается не столь ясным. В этом случае мы можем получить аналог теоремы 2 только для *однородных* многочленов $P(x)=\max\limits_{a\in A}\langle a,x\rangle+c_a$, т. е. таких, что $a_1+\cdots+a_n=m$ при некотором $m\in\mathbb{N}$ для всех $a\in A$.

Теорема 3. *Если однородный* $(\max,+)$*-многочлен* $P(x_1,\ldots,x_n)$ *реализуется* $(\max,+,-x_i)$*-схемой сложности* s*, то он также может быть вычислен* $(\max,+)$*-схемой сложности* $\mathcal{O}(ns^2)$.

По аналогии с арифметическим случаем можно определить *дополнение* тропического многочлена $P(x)=\min\limits_{S\in\mathcal{F}}\sum\limits_{i\in S}x_i$ как

$$\text{co-}P(x)=\min_{S\in\mathcal{F}}\sum_{i\notin S}x_i.$$

---

*) Здесь и далее $\mathbb{N}$ — множество неотрицательных целых чисел.

Но при этом тропический аналог следствия 1 не имеет места: сложность тропических многочленов P и со-P может отличаться экспоненциально. Например, пусть $\mathscr{F}$ — семейство подмножеств ребер полного двудольного $n\times n$ графа $K_{n,n}$, состоящее из всех $n!$ дополнений совершенных паросочетаний и из всех n^2 отдельных ребер. Тогда $(\min,+)$-многочлен $P(x)=\min\limits_{S\in\mathscr{F}}\sum\limits_{e\in S}x_e$ можно вычислить тривиальной $(\min,+)$-схемой размера n^2 (которая просто возвращает минимальный из весов ребер). С другой стороны, дополнительный многочлен со-$P(x)=\min\limits_{S\in\mathscr{F}}\sum\limits_{e\notin S}x_e$ эквивалентен тропическому перманенту $\mathrm{Per}_n(x)=\min\limits_{M}\sum\limits_{e\in M}x_e$, где минимум вычисляется по всем совершенным паросочетаниям M в $K_{n,n}$ (минимум в со-P обязательно достигается на некотором паросочетании $\overline{S}$). Осталось вспомнить, что многочлен Per_n имеет сложность $2^{\Omega(n)}$ при реализации $(\min,+)$-схемами [13].

Ситуация, однако, меняется, когда вместо дополняющих тропических многочленов мы рассматриваем *двойственные* к ним, в которых операции min и max меняются местами.

Следствие 2. *Если многочлен* $P(x)=\max\limits_{a\in A}\langle a,x\rangle$, *где* $A\subseteq\{0,1\}^n$, *реализуется* $(\max,+)$-*схемой сложности* s, *то двойственный многочлен* $P^*(x)=\min\limits_{a\in A}\langle\vec{1}-a,x\rangle$ *может быть вычислен* $(\min,+,-x_i)$-*схемой сложности* $n+s$, *а также* $(\min,+)$-*схемой сложности* $\mathscr{O}(ns^2+n^3)$.

Доказательство. Рассмотрим $(\max,+)$-схему Φ сложности s, вычисляющую многочлен P, и преобразуем ее в $(\min,+,-x_i)$-схему, заменяя каждый элемент max на элемент min, а каждый вход переменной x_i на инверсный вход $-x_i$. Полученная $(\min,+,-x_i)$-схема Φ' имеет ту же сложность и вычисляет многочлен Лорана $Q(x)=\min\limits_{a\in A}\langle a,-x\rangle=\min\limits_{a\in A}\langle -a,x\rangle$. Тогда многочлен $P^*(x)=\min\limits_{a\in A}\langle\vec{1}-a,x\rangle=\langle\vec{1},x\rangle+Q(x)$ реализуется $(\min,+,-x_i)$-схемой сложности $n+s$. Как следует из теоремы 2, многочлен P^* можно также вычислить $(\min,+)$-схемой сложности $\mathscr{O}(ns^2+n^3)$.

Для двойственных к $(\min,+)$-многочленам аналогичное рассуждение, но с использованием теоремы 3 вместо теоремы 2, приводит к несколько более слабому результату.

Следствие 3. *Если многочлен* $P(x)=\min\limits_{a\in A}\langle a,x\rangle$, *где* $A\subseteq\{0,1\}^n$, *реализуется* $(\min,+)$-*схемой сложности* s, *то двойственный многочлен* $P^*(x)=\max\limits_{a\in A}\langle\vec{1}-a,x\rangle$ *может быть вычислен* $(\max,+,-x_i)$-*схемой сложности* $n+s$. *Если многочлен P однородный, то многочлен P^* также можно вычислить* $(\max,+)$-*схемой сложности* $\mathscr{O}(ns^2+n^3)$.

Если говорить о схемах, которым доступны обе операции min и max, то несложно показать (см. предложение 1 ниже), что возможности $(\min,+,\max,-x_i)$-схем примерно такие же, как у тропических $(\min,+,-)$-схем. Как следствие того, что отношение $(\min,+)/(\min,+,-)$ может быть экспоненциальным [10], сложность $(\min,+)$-схемы можно экспоненциально понизить, разрешив операции max и инверсные входы $-x_i$. На самом деле, уже отношение сложностей $(\min,+)/(\min,+,\max)$ может быть экспоненциальным. Действительно, задача построения минимального остовного дерева MST_n решается $(\min,+,\max)$-схемой сложности $\mathscr{O}(n^3)$ [15], но любая $(\min,+)$-схема для этой проблемы имеет сложность $2^{\Omega(\sqrt{n})}$ [14]. С учетом теоремы 2 это означает, что даже отношение $(\min,+,-x_i)/(\min,+,\max)$ может быть экспоненциальным.

Следствие 4. *Задача* MST_n *решается* $(\min,+,\max)$*-схемой сложности* $\mathscr{O}(n^3)$*, но любая* $(\min,+,-x_i)$*-схема для этой задачи имеет сложность* $2^{\Omega(\sqrt{n})}$.

Наши результаты о сравнении нескольких моделей арифметических $(+,\cdot,/)$- и тропических $(\min,+,-)$-схем отражены в форме диаграммы на рис. 1. В тропическом полукольце $(\mathbb{R}_+,\min,+)$ роль сложения играет операция $\min(x,y)$, роль умножения — сложение $x+y$ и роль деления — вычитание $x-y$. Операция max связана с базовыми операциями $(\min,+)$ соотношением $\min(x,y)+\max(x,y)=x+y$. Поэтому в арифметическом полукольце $(\mathbb{R}_+,+,\cdot)$ аналогом операции max является операция *гармонической суммы* (половина от гармонического среднего):

$$x \oplus y := \frac{1}{\frac{1}{x}+\frac{1}{y}} = \frac{x\cdot y}{x+y}\,. \tag{1}$$

Заметим, что $(x+y)\cdot(x\oplus y)=x\cdot y$ и $(x+y)^{-1}=x^{-1}\oplus y^{-1}$. Это арифметические версии тропических тождеств $\min(x,y)+\max(x,y)=x+y$ и $-\min(x,y)=\max(-x,-y)$. В частности, тропическим $(\min,+,\max)$-схемам соответствуют арифметические $(+,\cdot,\oplus)$-схемы.

Отношение «$\approx$» на рис. 1 означает следующее.

Предложение 1. *Сложность в моделях* $(+,\cdot,/)$*-схем и* $(+,\cdot,\oplus,1/x_i)$*-схем совпадает с точностью до постоянного множителя. То же верно для моделей* $(\min,+,-)$*- и* $(\min,+,\max,-x_i)$*-схем.*

Подчеркнем, что в модели $(\min,+,\max,-x_i)$-схем разрешается использовать отрицательные константы в качестве входов.

Доказательство. Рассуждение проводится единообразно для обоих — арифметического и тропического — случаев. В первом случае $x_i^{-1}=1/x_i$, а во втором $x_i^{-1}=-x_i$ и $x\oplus y=\max(x,y)$. Доказательство в одну сторону тривиально: $(+,\cdot,\oplus,{x_i}^{-1})$-схемы моделируются $(+,\cdot,/)$-схемами не более чем втрое большей сложности ввиду (1).

Теперь рассмотрим произвольную $(+,\cdot,/)$-схему Φ сложности s. Продублируем все вычисления в ней вычислением обратных величин. Это значит, что для каждого входа переменной x_i предусмотрим вход x_i^{-1} в новой схеме Φ', а для входа константы c — дополнительный вход c^{-1}. Каждому элементу $g(a,b)$ схемы Φ соответствует пара элементов схемы Φ', функционирующих по правилам:

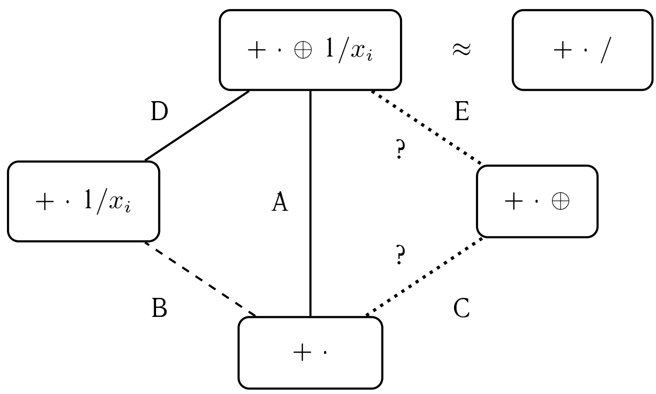
— если $g=a\cdot b$ в Φ, то $g=a\cdot b$ и $g^{-1}=a^{-1}\cdot b^{-1}$ в Φ';

— если $g=a+b$ в Φ, то $g=a+b$ и $g^{-1}=a^{-1}\oplus b^{-1}$ в Φ';

— если $g=a/b$ в Φ, то $g=a\cdot b^{-1}$ и $g^{-1}=a^{-1}\cdot b$ в Φ'.

По построению схема Φ' содержит только элементы из $\{+,\cdot,\oplus\}$, имеет сложность $2s$ и вычисляет ту же функцию.

Таким образом, поскольку отношение сложностей $(+,\cdot)/(+,\cdot,/)$ может быть экспоненциальным, инверсные входы $1/x_1,\ldots,1/x_n$ *вместе* с операцией гармонической суммы $x\oplus y$ позволяют снизить сложность монотонных



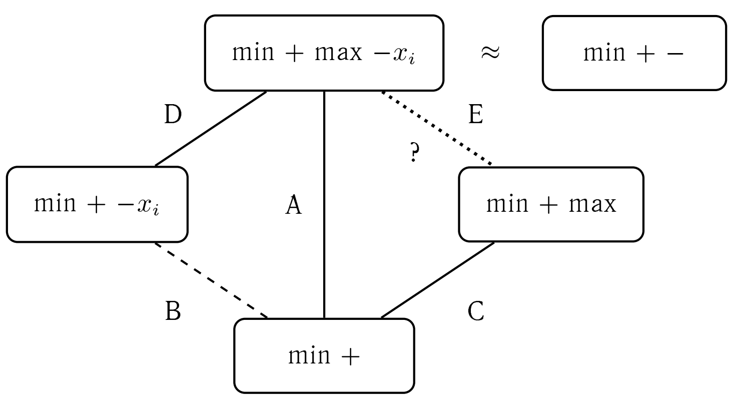


Рис. 1. Базовые подклассы арифметических $(+,\cdot,/)$-схем и тропических $(\min,+,-)$-схем. Здесь $x\oplus y=(x^{-1}+y^{-1})^{-1}$ означает операцию гармонической суммы; ее тропический $(\min,+)$-аналог — операция $\max(x,y)$. Отношение $\approx$ означает, что сложность схем в соответствующих моделях совпадает по порядку (предложение 1). То, что отношение (A) может быть экспоненциальным как в арифметическом, так и в тропическом случаях, следует из нижних оценок [13, 15] и верхних оценок [10] сложности одних и тех же многочленов. Возможность экспоненциальной величины отношения (C) для тропических схем доказана в [14]. Основной результат настоящей работы состоит в том, что отношение (B) безусловно не более чем квадратично для арифметических и тропических $(\min,+)$-схем (теоремы 1, 2), то же верно для $(\max,+)$-схем, вычисляющих однородные многочлены (теорема 3). Вместе с (A) это означает, что отношение (D) может быть экспоненциальным в обеих, арифметической и тропической моделях. Вопросы о величине отношения (E) в обеих моделях и о величине отношения (C) в арифметической модели остаются открытыми.

арифметических схем экспоненциально. Теорема 1 показывает, что наличие элементов $\oplus$ необходимо для подобного ускорения. Естественно возникает вопрос о роли инверсных входов: может ли их наличие вести к существенному снижению сложности $(+,\cdot,\oplus)$-схем, иначе говоря, может ли отношение $(+,\cdot,\oplus)/(+,\cdot,\oplus,1/x_i)$ быть велико?

Такая же ситуация с тропическими $(\min,+)$-схемами (где роль операции $x\oplus y$ играет $\max(x,y)$). Согласно следствию 4, отношение $(\min,+,-x_i)/(\min,+,\max)$ может быть экспоненциально. Это значит, что расширение модели $(\min,+)$-схем путем включения операции $\max$ приводит к более сильной модели, чем добавление инверсных входов $-x_i$. Вопрос в том, могут ли вообще инверсные входы быть полезными для $(\min,+,\max)$-схем. В § 8 эти вопросы обсуждаются подробнее.

§ 3. Предварительные понятия

Арифметические $(+,\cdot)$- и тропические $(\min,+)$- и $(\max,+)$-схемы выполняют вычисления в соответствующих полукольцах. Для единообразия рассуждений пусть $(\mathbb{R}_+,+,\cdot)$ обозначает любое из этих полуколец.

Многочлены. *Многочлен n* переменных над полукольцом $(\mathbb{R}_+,+,\cdot)$ определяется как выражение $P(x)=\sum\limits_{a\in A}c_aX^a$, где $A\subseteq\mathbb{N}^n$ — некоторое конечное множество, $X^a=\prod\limits_{i=1}^{n}x_i^{a_i}$ — *мономы*, c_aX^a — *одночлены*, и $c_a>0$ — *коэффициенты* многочлена P. *Степенью* монома X^a называется сумма $a_1+\dots+a_n$ компонент вектора a, а *степенью* многочлена — максимальная из степеней его мономов. В *многочленах Лорана* допускаются отрицательные экспоненты: в этом случае $A\subseteq\mathbb{Z}^n$. Чтобы подчеркнуть тот факт, что некоторый многочлен Лорана P является на самом деле обычным многочленом (без отрицательных показателей степени), мы иногда будем называть P *нелорановым* многочленом. Таким образом, термины «многочлен» и «нелоранов многочлен» эквивалентны.

В тропических полукольцах мономы X^a превращаются в линейные формы $\langle a,x\rangle=a_1x_1+\dots+a_nx_n$, а одночлены — в аффинные формы $\langle a,x\rangle+c_a=a_1x_1+\dots+a_nx_n+c_a$. Роль «показателей степени» a_i играют коэффициенты этих форм. Таким образом, в полукольце $(\mathbb{R}_+,\min,+)$ многочлен Лорана — это выражение вида $P(x)=\min\limits_{a\in A}\langle a,x\rangle+c_a$. Аналогично определяются многочлены Лорана в полукольце $(\mathbb{R}_+,\max,+)$.

Многочлены, порождаемые схемами. Под *$(+,\cdot,x_i^{-1})$-схемой* мы понимаем схему, использующую операции полукольца $+$ и $\cdot$. Ее входами являются переменные $x_1,\dots,x_n$, инверсии переменных $x_1^{-1},\dots,x_n^{-1}$ и любые *неотрицательные* константы $c\in\mathbb{R}_+$.

Естественным образом каждая $(+,\cdot,x_i^{-1})$-схема *порождает* (т. е. вычисляет синтаксически) определенный многочлен Лорана: при выполнении сложения $(+)$ два порождаемых многочлена складываются, при элементе умножения $(\cdot)$ порождается сумма всех попарных произведений членов двух многочленов на входах. Более точно, порождаемые входами x_i, x_i^{-1} или $c\in\mathbb{R}$

многочлены Лорана полагаются равными x_i, x_i^{-1} и c соответственно. Если $P(x)=\sum_{a\in A} c_aX^a$ и $Q(x)=\sum_{b\in B} c_bX^b$ — многочлены Лорана, порождаемые на входах элемента g, то на выходе элемента порождается многочлен

$$P+Q=\sum_{a\in A} c_aX^a+\sum_{b\in B} c_bX^b,\quad \text{если } g=+,$$

$$P\cdot Q=\sum_{a\in A}\sum_{b\in B} c_ac_bX^{a+b},\quad \text{если } g=\cdot.$$

В частности, в случае тропических $(\min,+,-x_i)$-схем многочлены (Лорана) на входах элемента имеют вид $P(x)=\min_{a\in A}\langle a,x\rangle+c_a$ и $Q(x)=\min_{b\in B}\langle b,x\rangle+c_b$, где $A,B\subseteq\mathbb{Z}^n$ и $c_a,c_b\in\mathbb{R}_+$. Многочлен, порождаемый на выходе элемента, — это либо $\min\{P,Q\}$, либо $P+Q=\min_{a\in A}\min_{b\in B}\langle a+b,x\rangle+c_a+c_b$.

Вычисление и порождение. Напомним, что два многочлена Лорана P и Q от n переменных называются *эквивалентными*, если $P(x)=Q(x)$ для всех $x\in\mathbb{R}_+^n$. Арифметическая или тропическая схема Φ (с инверсными входами или без) *вычисляет* многочлен Лорана P, если многочлен, порождаемый схемой Φ, эквивалентен P.

Хорошо известно (и легко показать, используя, например, вариант фундаментальной теоремы алгебры для многочленов нескольких переменных), что если два многочлена Лорана эквивалентны, то они совпадают как формальные выражения, т. е. содержат одни и те же мономы с одними и теми же ненулевыми коэффициентами при них (см. § 5). Поэтому если арифметическая $(+,\cdot,1/x_i)$-схема вычисляет некоторый многочлен, то она также и порождает его.

Этого нельзя сказать про тропические схемы: разные тропические многочлены (Лорана) могут быть эквивалентны. Например, для любого $(\min,+)$-многочлена P все многочлены $\min\{x,x+P\}$ эквивалентны многочлену x. Джеррум и Шнир [13, след. A3] построили следующую структурную характеризацию всех эквивалентных тропических многочленов Лорана, используя вариант леммы Фаркаша из работы К. Фана [8, теор. 4]. Скажем, что вектор u *лежит выше* вектора v, если $u\geqslant v$, и u *лежит ниже* v, если $u\leqslant v$. Результат [13] состоит в том, что два тропических многочлена Лорана $P(x)=\min_{a\in A}\langle a,x\rangle+c_a$ и $Q(x)=\min_{b\in B}\langle b,x\rangle+c_b$ эквивалентны тогда и только тогда, когда каждый вектор (a,c_a) лежит выше некоторой выпуклой комбинации векторов (b,c_b), и каждый вектор (b,c_b) лежит выше некоторой выпуклой комбинации векторов (a,c_a). Ввиду тождества $\max(x,y)=-\min(-x,-y)$ то же верно для $(\max,+)$-многочленов, если везде «лежит выше» заменить на «лежит ниже».

Так, многочлены Лорана $P=\max\{2x,2y\}$ и $Q=\max\{2x,x+y-z,2y\}$ эквивалентны в силу $(1,1,-1)\leqslant\frac{1}{2}(2,0,0)+\frac{1}{2}(0,2,0)$. Переменная z имеет отрицательный «показатель степени» в Q, так что многочлен Q в принципе не может быть порожден $(\max,+)$-схемой. Пример на рис. 2 показывает, что даже *минимальные* $(\max,+,-x_i)$-схемы, вычисляющие нелорановы $(\max,+)$-многочлены, могут порождать многочлены с отрицательными показателями.

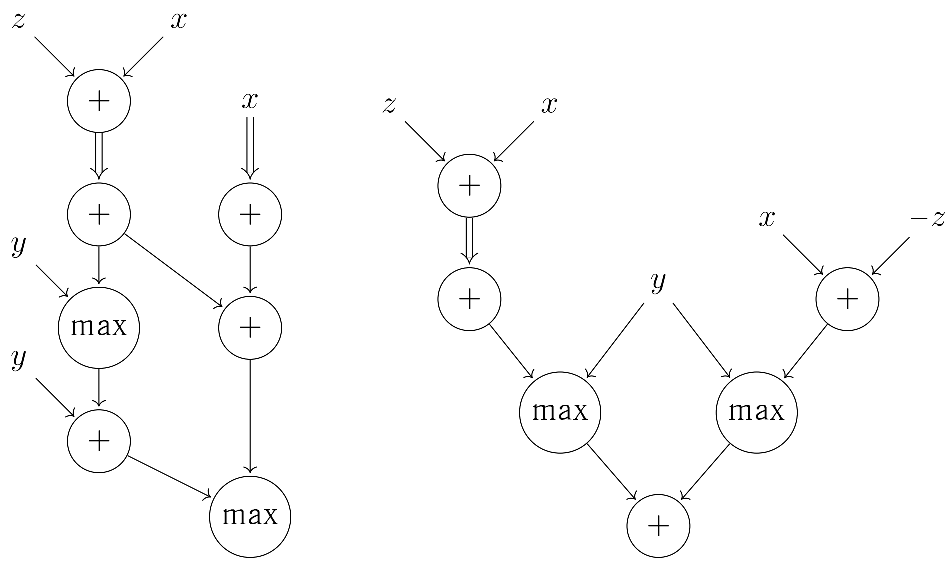


Рис. 2. Слева: минимальная $(\max, +)$-схема, вычисляющая тропический многочлен $P(x, y, z) = \max\{2x+y+2z, 2y, 3x+z\}$ со сложностью 7. Двойная стрелка $\Downarrow$ означает пару параллельных ребер. Справа: минимальная $(\max, +, -x_i)$-схема, вычисляющая тот же многочлен со сложностью 6. Можно проверить, что любая $(\max, +, -x_i)$-схема, вычисляющая P со сложностью 6, порождает многочлен с отрицательными показателями степени. В частности, изображенная справа схема порождает многочлен Лорана $Q = \max\{2x+y+2z, 2y, 3x+z, x+y-z\}$, содержащий избыточный член $x + y - z$.

Делители многочленов. Моном $X^b = \prod_{i=1}^{n} x_i^{b_i}$, $b \in \mathbb{N}^n$, называется *делителем* (нелоранова) многочлена $P = \sum_{a \in A} c_a X^a$, $A \subseteq \mathbb{N}^n$, если он делит все мономы многочлена P, т. е. если все векторы $a - b$, где $a \in A$, — неотрицательны. Моном X^b, для которого $b_i = \min\{a_i \colon a \in A\}$, называется *наибольшим делителем* P. Таким образом, наибольший делитель многочлена P — это моном максимально возможной степени $b_1 + \dots + b_n$, который делит все мономы P. *Базой* многочлена P назовем многочлен

$$[P] := P/M = \sum_{a \in A} c_a X^{a-b},$$

где $M = X^b$ — наибольший делитель P. Например, если $P = x_i$, то $M = x_i$ и $[P] = 1$ (мультипликативная единица). Если $P = c \in \mathbb{R}_+$, то $M = 1$ и $[P] = c$. В тропическом полукольце мультипликативной единицей является 0. Поэтому база тропического $(\max, +)$-многочлена $P = \max_{a \in A} \langle a, x \rangle + c_a$ имеет вид $[P] := P - M = \max_{a \in A} \langle a - b, x \rangle + c_a$.

§ 4. Устранение инверсных входов

В этом разделе мы доказываем, что инверсные входы $x_1{}^{-1}, \dots, x_n{}^{-1}$ можно практически безболезненно устранить из $(+, \cdot, x_i{}^{-1})$-схемы, если *порождаемый* ею многочлен Лорана не содержит отрицательных степеней (лемма 3). Напомним, что под $(+,\cdot,{x_i}^{-1})$-схемами можно понимать как арифметические $(+,\cdot,1/x_i)$-, так и тропические $(\min,+,-x_i)$- или $(\max,+,-x_i)$-схемы.

Следующая лемма показывает, что многочлены Лорана, порождаемые $(+,\cdot,{x_i}^{-1})$-схемами, имеют специальный вид отношения многочлена P и монома M, где P и M можно вычислить $(+,\cdot)$-схемой ненамного большего размера.

Лемма 1. *Пусть* Φ — $(+,\cdot,{x_i}^{-1})$*-схема сложности* s. *Тогда многочлен Лорана* Q, *порождаемый схемой* Φ, *имеет вид* $Q=P/M$, *где многочлен* P *и моном* M *могут быть вычислены одной* $(+,\cdot)$*-схемой сложности не более* $4s$.

Здесь P/M означает $P\cdot M^{-1}$; скажем, в тропическом случае P/M — это тропический многочлен (Лорана) вида $P-M$.

Доказательство. Наша цель состоит в построении преобразования $(+,\cdot,{x_i}^{-1})$-схемы Φ в $(+,\cdot)$-схему Φ' сложности не выше $4s$, порождающую пару многочленов (P,M), где $Q=P/M$. Построение схемы Φ' выполним поэлементно, просматривая схему Φ от входов к выходам. Далее 1 означает мультипликативную единицу соответствующего полукольца, т. е. константу 1 в арифметическом случае и константу 0 — в тропическом.

Входам x_i, x_i^{-1} и $c\in\mathbb{R}_+$ сопоставляются пары (P,M) вида $(x_i,1)$, $(1,x_i)$ и $(c,1)$ соответственно. Теперь предположим, что для многочленов Лорана Q_1 и Q_2 на входах некоторого элемента вычислены требуемые представления $Q_1=P_1/M_1$ и $Q_2=P_2/M_2$. Многочлен Лорана, порождаемый на выходе этого элемента, также вычислим в форме $Q=P/M$. В случае элемента умножения*) $Q=Q_1\cdot Q_2=(P_1/M_1)\cdot(P_2/M_2)=P_1P_2/M_1M_2$, поэтому положим $P=P_1P_2$ и $M=M_1M_2$. Таким образом, вместо одного элемента умножения схемы Φ мы используем два элемента умножения в схеме Φ'. В случае элемента сложения $Q=Q_1+Q_2=(P_1/M_1)+(P_2/M_2)=(P_1M_2+P_2M_1)/M_1M_2$, поэтому можно положить $P=P_1M_2+P_2M_1$ и $M=M_1M_2$. Таким образом, вместо элемента сложения мы используем один элемент сложения и три элемента умножения. Следовательно, построенная в итоге $(+,\cdot)$-схема Φ' содержит максимум вчетверо больше элементов, чем исходная $(+,\cdot,{x_i}^{-1})$-схема Φ, что и требовалось.

Лемма 1 без увеличения порядка сложности позволяет устранить инверсные входы $x_1^{-1},\ldots,x_n^{-1}$ из $(+,\cdot,x_i^{-1})$-схемы ценой одной дополнительной операции «деления на моном». Наша ближайшая цель — устранить и эту операцию. Если Q — нелоранов многочлен, то моном M из выражения $Q=P/M$ должен делить все мономы многочлена P. Следующая лемма утверждает, что ценой квадратичного увеличения сложности от последнего деления можно избавиться в случае, когда M — наибольший делитель многочлена P: тогда $Q=[P]$, где $[P]$ — база многочлена P.

Доказываемая далее лемма 2 справедлива для любого полукольца S со свойством:

(∗) если P_1 и P_2 — многочлены над S, то любой делитель многочлена P_1+P_2 одновременно является делителем каждого из многочленов P_1 и P_2.

*) Как обычно, далее иногда мы будем опускать знак умножения $\cdot$ и писать xy вместо $x\cdot y$.

Немонотонные полукольца, в которых определено вычитание $(-)$, этим свойством не обладают. Скажем, x делит многочлен $P = P_1 + P_2$, где $P_1 = x + y$ и $P_2 = x - y$, но не делит ни один из многочленов P_1, P_2. Однако свойством $(*)$ обладает рассматриваемое нами обобщенное полукольцо $(\mathbb{R}_+, +, \cdot)$ как в арифметической, так и в тропической версиях.

Лемма 2. *Если многочлен P от n переменных порождается $(+, \cdot)$-схемой сложности s, то его база $[P]$ порождается $(+, \cdot)$-схемой сложности $\mathcal{O}(ns^2)$.*

Доказательство. Рассмотрим $(+, \cdot)$-схему Φ сложности s, порождающую многочлен P. Назовем моном $X^a = \prod_{i=1}^{n} x_i^{a_i}$ *простым*, если $0 \leqslant a_i \leqslant 2^s$ для всех $i = 1, \ldots, n$. Поскольку элементы умножения — двухвходовые, каждый делитель многочлена, порождаемого на выходе любого элемента схемы Φ, — простой. Под *расширенной* $(+, \cdot)$-схемой будем понимать $(+, \cdot)$-схему, входами которой могут быть любые простые мономы.

Следующее утверждение сводит задачу порождения базы $[P]$ к задаче порождения простых мономов.

Утверждение. *Многочлен $[P]$ может быть порожден расширенной $(+, \cdot)$-схемой сложности не более $3s$.*

Доказательство. Мы опишем преобразование $(+, \cdot)$-схемы Φ, порождающей многочлен P, в расширенную $(+, \cdot)$-схему Φ' сложности не выше $3s$, порождающую $[P]$. Будем строить схему Φ', просматривая поэлементно схему Φ в направлении от входов к выходам. Для входов x_i и $c \in \mathbb{R}_+$ схемы Φ полагаем $[x_i] = 1$ и $[c] = c$.

Теперь рассмотрим произвольный элемент схемы Φ, на выходе которого из многочленов P_1 и P_2 порождается многочлен P. Предположим, что уже построена часть схемы Φ', порождающая базы $[P_1] = P_1/M_1$ и $[P_2] = P_2/M_2$, где M_1 и M_2 — наибольшие делители многочленов P_1 и P_2. Если $P = P_1 \cdot P_2$, то $M = M_1 \cdot M_2$ — наибольший делитель P. Поэтому мы вычисляем $[P]$ по правилу $[P] = P/M = (P_1/M_1) \cdot (P_2/M_2) = [P_1] \cdot [P_2]$. Если $P = P_1 + P_2$ и M — наибольший делитель P, то вычисляем $[P]$ как

$$[P] = [P_1 + P_2] = \frac{P_1 + P_2}{M} = \frac{M_1 \cdot [P_1] + M_2 \cdot [P_2]}{M} = M_1' \cdot [P_1] + M_2' \cdot [P_2],$$

где $M_1' = M_1/M$ и $M_2' = M_2/M$. Условие $(*)$ гарантирует, что M делит оба монома M_1 и M_2. Следовательно, M_1' и M_2' — простые мономы, которые можно использовать в качестве входов.

Построенная таким образом $(+, \cdot)$−схема Φ' содержит не более $3s$ элементов и порождает многочлен $[P]$.

Расширенная схема из утверждения использует до $2s$ простых мономов в качестве входов. Индивидуальные степени переменных в этих мономах не превосходят 2^s. Эти дополнительные входы можно устранить ценой квадратичного увеличения сложности схемы.

Действительно, все степени $x_i^2, x_i^{2^2}, \ldots, x_i^{2^s}$ одной переменной x_i вычисляются за s умножений. После этого любая степень x_i^d, $d \leqslant 2^s$, может быть порождена при помощи s дополнительных умножений (следуя двоичной записи числа d). Теперь любой простой моном на входе расширенной схемы можно породить при помощи $2ns$ элементов умножения. Так получается (обычная) $(+,\cdot)$-схема сложности не выше $2ns\cdot 2s+3s=\mathcal{O}(ns^2)$, порождающая многочлен $[P]$, что и требовалось.

Доказательство теорем 1, 2, 3 опирается на простое следствие из лемм 1, 2 о сложности схем, порождающих нелорановы многочлены.

Лемма 3. *Если нелоранов многочлен n переменных порождается $(+,\cdot,x_i{}^{-1})$-схемой сложности s, то он может быть порожден $(+,\cdot)$-схемой сложности $\mathcal{O}(ns^2)$.*

Доказательство. Пусть Q — нелоранов многочлен n переменных, порождаемый $(+,\cdot,x_i{}^{-1})$-схемой Φ сложности s. Лемма 1 гарантирует существование $(+,\cdot)$-схемы Φ' сложности не выше $4s$, порождающей многочлен P и моном M, такие что $P=Q\cdot M$. Пусть X^a — наибольший делитель многочлена Q. В силу $[P]=[Q\cdot M]=[Q]$ получаем $Q=[Q]\cdot X^a=[P]\cdot X^a$. Согласно лемме 2, многочлен $[P]$ порождается $(+,\cdot)$-схемой сложности $\mathcal{O}(ns^2)$.

С другой стороны, поскольку многочлен P может быть порожден $(+,\cdot)$-схемой Φ' сложности $4s$, степень любой переменной в P не превосходит 2^{4s}. Так как X^a делит все мономы P, ни одна из компонент вектора a также не превосходит 2^{4s}. При помощи последовательных удвоений моном X^a можно вычислить $(+,\cdot)$-схемой сложности $\mathcal{O}(ns)$. В итоге мы получаем требуемую $(+,\cdot)$-схему сложности $\mathcal{O}(ns^2)$, порождающую многочлен Q.

Замечание 2. Даже если схема порождает многочлен Лорана Q с отрицательными показателями, все равно выполняется $Q=[P]\cdot X^a$ для некоторого лоранова монома X^a, где a_i — минимум (возможно, отрицательный) показателей степени переменной x_i в Q. Но тогда лоранов моном X^a, вообще говоря, не может порождаться $(+,\cdot)$-схемой. Именно поэтому лемма требует, чтобы Q был нелорановым многочленом.

§ 5. Доказательство теоремы 1: арифметические схемы

Пусть монотонная арифметическая $(+,\cdot,1/x_i)$-схема Φ сложности s вычисляет многочлен P от n переменных. Покажем, что многочлен P также можно вычислить монотонной $(+,\cdot)$-схемой сложности $\mathcal{O}(ns^2)$. Обозначим через Q многочлен Лорана, порождаемый схемой Φ. Поскольку Φ вычисляет P, для всех $x\in\mathbb{R}_+^n$ выполняется $P(x)=Q(x)$. Ввиду леммы 3, достаточно показать, что $Q=P$, т. е. что на самом деле схема Φ порождает непосредственно многочлен P.

Хорошо известно, что если многочлен F степени d от одной переменной обращается в ноль на множестве $S\subseteq\mathbb{R}$ мощности $|S|\geqslant d+1$, то $F=0$ тождественно. Простой индукцией по числу переменных этот факт распространяется на случай многочленов нескольких переменных (см., например, [4, лемма 2.1]): если $F\in\mathbb{R}[x_1,\ldots,x_n]$ — ненулевой многочлен степени d, то для любого множества $S\subseteq\mathbb{R}$ мощности $|S|\geqslant d+1$, многочлен F принимает ненулевое значение хотя бы в одной точке $x\in S^n$.

Выберем моном M достаточно большой степени так, что многочлен MQ не имеет отрицательных степеней. Рассмотрим многочлен $F=MP-MQ$. Предположим, что $Q\neq P$. Тогда F — ненулевой многочлен ограниченной степени d, который, следовательно, не может принимать только нулевые значение на любом множестве $S\subseteq\mathbb{R}_+$ мощности $|S|\geqslant d+1$. Поэтому $F(x)\neq 0$, а значит, $P(x)\neq Q(x)$, при некотором $x\in\mathbb{R}_+^n$. Противоречие. Теорема 1 доказана.

§ 6. Доказательство теоремы 2: минимизация

Пусть $P(x_1, \ldots, x_n) = \min_{a \in A} \langle a, x\rangle + c_a$ — тропический $(\min, +)$-многочлен (таким образом, $A \subseteq \mathbb{N}^n$ и $c_a \in \mathbb{R}_+$), который реализуется $(\min, +, -x_i)$-схемой Φ сложности s. Покажем, что P также можно вычислить $(\min, +)$-схемой сложности $\mathcal{O}(ns^2)$.

Пусть схема Φ порождает некоторый тропический многочлен Лорана $Q(x) = \min_{b \in B} \langle b, x\rangle + c_b$, где $B \subseteq \mathbb{Z}^n$ и $c_b \in \mathbb{R}_+$ для всех $b \in B$, причем $Q(x) = P(x)$ при любом $x \in \mathbb{R}^n_+$. Чтобы применять лемму 3, достаточно доказать, что Q не содержит отрицательных «показателей», т. е. что $B \subseteq \mathbb{N}^n$. Это вытекает из общей характеризации эквивалентных тропических многочленов Лорана, полученной в [13] (см. § 3): для любого вектора $b \in B$ существует выпуклая комбинация c векторов из A такая, что $b \geqslant c$; поскольку вектор c неотрицательный, то вектор b также неотрицательный. Однако в случае минимизации включение $B \subseteq \mathbb{N}^n$ можно показать непосредственно.

Предположим, что при некотором $b \in B$ и i выполнено $b_i < 0$, т. е. $b_i \leqslant -1$. Положим $K = 1 + c_b$, где c_b — коэффициент при тропическом одночлене $\langle b, x\rangle + c_b$ многочлена Q. Определим весовой вектор $x \in \{0, K\}^n$ условиями $x_i := K$ и $x_j := 0$ для всех $j \neq i$. Тогда $P(x) \geqslant 0$, но $Q(x) \leqslant \langle b, x\rangle + c_b = b_i \cdot K + c_b \leqslant -K + c_b < 0$. Приходим к противоречию с $Q(x) = P(x)$. Теорема 2 доказана.

Замечание 3. То же рассуждение позволяет получить аналог теоремы 2 для $(\max, +, -x_i)$-схем, от которых требуется правильное вычисление многочлена на любых наборах входов из $\mathbb{R}^n$ (в том числе с отрицательными координатами). Чтобы установить $Q(x) > P(x)$, достаточно подать подходящее отрицательное значение на i-й вход, где $b_i < 0$.

Однако мы требуем, чтобы $(\max, +, -x_i)$-схема корректно вычисляла заданный $(\max, +)$-многочлен на *неотрицательных* наборах входов (замечание 1 поясняет смысл этого ограничения). В этом случае приведенная аргументация не работает: множество $B \subseteq \mathbb{Z}^n$ векторов показателей $(\max, +)$-многочлена Лорана Q может включать произвольный вектор $b \in \mathbb{Z}^n$, для которого выполняется $b \leqslant a$ при некотором $a \in A$. Пример на рис. 2 показывает, что, вообще говоря, отрицательные показатели неустранимы.

§ 7. Доказательство теоремы 3: максимизация

Пусть $Q(x) = \max_{b \in B} \langle b, x\rangle + c_b$ — тропический $(\max, +)$-многочлен Лорана, где $B \subseteq \mathbb{Z}^n$ и $c_b \in \mathbb{R}_+$ для всех $b \in B$. Напомним, что *степенью* (тропического) одночлена $\langle b, x\rangle + c_b$ мы называем сумму $\langle b, \vec{1}\rangle = b_1 + \cdots + b_n$ его показателей. Многочлен Лорана называется *однородным*, если все его мономы имеют одну и ту же степень. *Верхняя грань* многочлена Q — это многочлен $\lceil Q \rceil = \max_{b \in \lceil B \rceil} \langle b, x\rangle + c_b$, где $\lceil B \rceil \subseteq B$ — множество всех векторов показателей $b \in B$ многочлена Q максимальной степени. Разумеется, многочлен $\lceil Q \rceil$ — однородный.

Лемма 4. *Пусть Q — $(\max, +)$-многочлен Лорана и P — однородный нелоранов $(\max, +)$-многочлен степени m. Если P и Q эквивалентны, то $\lceil Q \rceil$ — нелоранов многочлен степени m, также эквивалентный многочлену P.*

Доказательство. Пусть $P(x) = \max_{a\in A} \langle a, x\rangle + c_a$; тогда $A \subseteq \mathbb{N}^n$, $c_a \in \mathbb{R}_+$ и $\langle a, \vec{1}\rangle = a_1 + \cdots + a_n = m$ для всех $a \in A$. Если $Q(x) = \max_{b\in B} \langle b, x\rangle + c_b$, то $B \subseteq \mathbb{Z}^n$ и $c_b \in \mathbb{R}_+$ для всех $b \in B$. По условию для всех $x \in \mathbb{R}^n_+$ выполнено $Q(x) = P(x)$. По определению многочлен $\lceil Q\rceil$ однороден. Сначала покажем, что степени $\lceil Q\rceil$ и P совпадают и равны m.

Утверждение 1. *Для любого* $b \in \lceil B\rceil$ *выполнено* $\langle b, \vec{1}\rangle = m$.

Доказательство. Обозначим $c_A = \max_{a\in A} c_a$ и $c_B = \max_{b\in B} c_b$ — максимальные «коэффициенты» многочленов P и Q. Если бы для какого-то вектора $b \in \lceil B\rceil$ выполнялось $\langle b, \vec{1}\rangle \leqslant m-1$, то же было бы верно для всех $b \in B$. Поэтому при достаточно большом r, скажем, $r = 1 + c_B$, для вектора $\vec{r} = (r, \ldots, r)$ получаем $Q(\vec{r}) = \max_{b\in B} \{r \cdot \langle b, \vec{1}\rangle + c_b\} \leqslant rm - r + c_b \leqslant rm - 1$ в то время как $P(\vec{r}) = \max_{a\in A} \{r \cdot \langle a, \vec{1}\rangle + c_a\} \geqslant rm > Q(\vec{r})$. С другой стороны, если бы для некоторого $b \in \lceil B\rceil$ выполнялось $\langle b, \vec{1}\rangle \geqslant m+1$, то для вектора $\vec{r}$ при $r = 1 + c_A$ было бы справедливо $Q(\vec{r}) \geqslant \langle b, \vec{r}\rangle \geqslant rm + r$ и $P(\vec{r}) \leqslant rm + c_A < Q(\vec{r})$. Поэтому $\langle b, \vec{1}\rangle = m$ для всех $b \in \lceil B\rceil$.

Теперь проверим, что $\lceil Q\rceil$ — нелоранов многочлен, т.е. не содержит отрицательных показателей степени.

Утверждение 2. $\lceil B\rceil \subseteq \mathbb{N}^n$.

Доказательство. Предположим, что некоторый вектор $b \in \lceil B\rceil$ имеет отрицательную компоненту, и обозначим $I = \{i\colon b_i > 0\}$. Поскольку $\langle b, \vec{1}\rangle = m$ ввиду утверждения 1, получаем $\sum_{i\in I} b_i \geqslant m + 1$. Положим $r := 1 + c_A$. Рассмотрим весовой вектор x с компонентами $x_i = r$ при всех $i \in I$, и $x_i = 0$ при всех $i \notin I$. Тогда $Q(x) \geqslant \langle b, x\rangle = r \cdot \sum_{i\in I} b_i \geqslant rm + r$, но $P(x) \leqslant P(\vec{r}) \leqslant rm + c_A < Q(x)$. Противоречие.

Утверждение 3. *Многочлен* $\lceil Q\rceil$ *эквивалентен многочленам* Q *и* P.

Доказательство. Рассмотрим произвольный вектор $x \in \mathbb{R}^n_+$ и покажем, что $\lceil Q\rceil(x) = Q(x)$. Согласно утверждениям 1 и 2, $\lceil Q\rceil$ — однородный нелоранов многочлен степени m. Следовательно, $\lceil Q\rceil(x + \vec{1}) = \lceil Q\rceil(x) + m$. Поскольку многочлены Q и P эквивалентны, а P — однородный многочлен степени m, имеет место $Q(x + \vec{1}) = P(x + \vec{1}) = P(x) + m = Q(x) + m$. Остается проверить, что $Q(x + \vec{1}) = \lceil Q\rceil(x + \vec{1})$. Пусть $b \in B$ — вектор показателей одночлена, определяющего значение многочлена Q в точке $x + \vec{1}$, т.е. $\langle b, x\rangle + c_b + \langle b, \vec{1}\rangle = Q(x) + m$. Так как $\langle b, x\rangle + c_b \leqslant Q(x)$, справедливо $\langle b, \vec{1}\rangle \geqslant m$ и, следовательно, $b \in \lceil B\rceil$. Поэтому $Q(x + \vec{1}) = \lceil Q\rceil(x + \vec{1})$, а значит и $Q(x) = \lceil Q\rceil(x)$, что и требовалось доказать.

Утверждение 3 влечет справедливость леммы 4.

Замечание 4. Заметим, что однородность многочлена P использовалась только в доказательстве утверждения 3. Если P — произвольный многочлен степени m, то при любом $x \in \mathbb{R}^n_+$ по-прежнему выполняется $Q(x + \vec{r}) = \lceil Q\rceil(x + \vec{r})$ для всех $r \geqslant 1 + Q(x)$. Действительно, если $b \in B$ — вектор, доставляющий значение $Q(x + \vec{r})$, то $\langle b, x\rangle + c_b + r \cdot \langle b, \vec{1}\rangle = Q(x + \vec{r}) = P(x + \vec{r}) \geqslant rm$. Из $\langle b, x\rangle + c_b \leqslant Q(x) \leqslant r - 1$

следует $r-1+r\cdot\langle b,\vec{1}\rangle \geqslant rm$ и далее, $\langle b,\vec{1}\rangle \geqslant m-1+1/r$. Поскольку $\langle b,\vec{1}\rangle$ — целое число, получаем $\langle b,\vec{1}\rangle \geqslant m$, т. е. $\langle b,\vec{1}\rangle = m$. Но при $0\leqslant r\leqslant Q(x)$ максимум $Q(x+\vec{r})$ может достигаться на векторе $b\in B$, для которого $\langle b,\vec{1}\rangle < m$.

Доказательство теоремы 3. Рассмотрим некоторый однородный $(\max,+)$-многочлен $P(x)=\max\limits_{a\in A}\langle a,x\rangle+c_a$ степени m; таким образом, $A\subseteq\mathbb{N}^n$, $c_a\in\mathbb{R}_+$ и $\langle a,\vec{1}\rangle = a_1+\cdots+a_n=m$ для всех $a\in A$. Предположим, что P вычисляется $(\max,+,-x_i)$-схемой Φ сложности s. Покажем, что P можно реализовать $(\max,+)$-схемой сложности $\mathcal{O}(ns^2)$.

Обозначим через $Q(x)=\max\limits_{b\in B}\langle b,x\rangle+c_b$ многочлен Лорана, порождаемый схемой Φ (значит, $B\subseteq\mathbb{Z}^n$ и $c_b\in\mathbb{R}_+$ для всех $b\in B$). Поскольку схема Φ вычисляет P, многочлены Q и P эквивалентны. Лемма 4 гарантирует, что $\lceil Q\rceil$ — нелоранов многочлен, также эквивалентный P. Поэтому, согласно лемме 3, достаточно показать, что многочлен $\lceil Q\rceil$ можно вычислить $(\max,+,-x_i)$-схемой сложности $\leqslant s$. Как отмечено в [13, теор. 2.4], требуемая схема Φ' получается из Φ путем удаления некоторых ребер (входящих в элементы max).

Более точно, многочлены Лорана x_i, $-x_i$, $c\in\mathbb{R}_+$, порождаемые входами схемы, совпадают со своими верхними гранями. Если верхние грани $\lceil Q_1\rceil$ и $\lceil Q_2\rceil$ многочленов, порождаемых на входах некоторого элемента $\circ$ схемы Φ, уже вычислены в новой схеме, то многочлен $\lceil Q_1\circ Q_2\rceil$ вычисляется так. Если $\circ=+$, тогда просто $\lceil Q_1+Q_2\rceil=\lceil Q_1\rceil+\lceil Q_2\rceil$ в силу $\langle b_1+b_2,\vec{1}\rangle=\langle b_1,\vec{1}\rangle+\langle b_2,\vec{1}\rangle$. В случае $\circ=\max$, если степень одного из многочленов $\lceil Q_1\rceil$ и $\lceil Q_2\rceil$ меньше, чем у другого, скажем, $\deg\lceil Q_1\rceil<\deg\lceil Q_2\rceil$, то $\lceil\max(Q_1,Q_2)\rceil=\lceil Q_2\rceil$. Если степени многочленов $\lceil Q_1\rceil$ и $\lceil Q_2\rceil$ равны, тогда $\lceil\max(Q_1,Q_2)\rceil=\max(\lceil Q_1\rceil,\lceil Q_2\rceil)$.

§ 8. Замечания и открытые проблемы

Мы показали (теоремы 1, 2), что добавление инверсных входов не позволяет существенно понизить сложность монотонных арифметических $(+,\cdot)$- и тропических $(\min,+)$-схем. То же верно и для $(\max,+)$-схем, вычисляющих однородные многочлены.

Открытая проблема 1. *Может ли для неоднородных* $(\max,+)$*-многочленов отношение* $(\max,+)/(\max,+,-x_i)$ *быть сверхполиномиальным?*

Положительный ответ на этот вопрос может быть связан с примером многочлена $\text{co-Path}_n(x)=\max\limits_p\sum\limits_{e\notin p}x_e$, где максимум берется по всем простым путям p в K_n, соединяющим вершины $s=1$ и $t=n$. Этот многочлен неоднороден: степени его мономов варьируются от $\binom{n}{2}-n+1$ до $\binom{n}{2}-1$. Многочлен co-Path_n является двойственным к многочлену $\text{Path}_n(x)=\min\limits_p\sum\limits_{e\in p}x_e$ из задачи поиска кратчайшего пути в графе. Методом Беллмана — Форда — Мура многочлен Path_n вычисляется $(\min,+)$-схемой сложности $\mathcal{O}(n^3)$. Поэтому, согласно следствию 3, многочлен co-Path_n реализуется $(\max,+,-x_i)$-схемой сложности $\mathcal{O}(n^3)$.

Открытая проблема 2. *Докажите или опровергните сверхполиномиальность* $(\max,+)$*-сложности* $(\max,+)$*-многочлена* co-Path_n.

Следствие 4 показывает, что отношение $(\min,+,-x_i)/(\min,+,\max)$ может быть экспоненциальным. Естественно возникает вопрос: позволяют ли инверсные входы существенно упростить $(\min,+,\max)$-схемы? Напомним, что сложность $(\min,+,\max,-x_i)$- и $(\min,+,-)$-схем пропорциональна (предложение 1). Таким образом, проблема в следующем.

Открытая проблема 3. *Может ли быть сверхполиномиальным отношение* $(\min,+,\max)/(\min,+,-)$?

Для утвердительного ответа на этот вопрос достаточно предъявить минимизационную задачу f, решаемую сравнительно простой $(\min,+,-)$-схемой, но имеющую высокую $(\min,+,\max)$-сложность. Вторая часть решения (нижняя оценка) может быть получена как следствие высокой нижней оценки монотонной булевой сложности для булева аналога задачи f. Более конкретно, булев аналог минимизационной задачи $f(x)=\min\limits_{S\in\mathcal{F}}\sum\limits_{i\in S}x_i$ определяется как булева функция $g(x)=\bigvee\limits_{S\in\mathcal{F}}\bigwedge\limits_{i\in S}x_i$.

Предложение 2. *Если* $(\min,+)$*-многочлен вычисляется* $(\min,+,\max)$*-схемой сложности* s*, то его булев аналог может быть реализован булевой* $(\wedge,\vee)$*-схемой сложности* s.

Доказательство основано на тривиальном наблюдении. Положим $[x]=1$, если $x>0$, и $[x]=0$ в противном случае. Тогда для любых $x,y\in\mathbb{R}_+$ выполняется $\big[\min(x,y)\big]=[x]\wedge[y]$ и $\big[\max(x,y)\big]=[x+y]=[x]\vee[y]$.

Таким образом, проблема 3 сводится к тому, чтобы предъявить оптимизационную задачу, которая решается сравнительно просто в модели тропических схем с вычитаниями, но булев аналог которой имеет высокую монотонную сложность. Потенциальным кандидатом может быть известная *задача о назначениях*. Соответствующий $(\min,+)$-многочлен — тропический аналог перманента $\mathrm{Per}_n(x)=\min\limits_{M}\sum\limits_{e\in M}x_e$, где минимум берется по всем совершенным паросочетаниям M в полном двудольном $n\times n$ графе. Как показано в [13], $(\min,+)$-сложность многочлена Per_n имеет величину $2^{\Omega(n)}$. На самом деле Per_n не может быть вычислен даже $(\min,+,\max)$-схемами полиномиальной сложности. Из известного результата А. А. Разборова [3] о монотонной сложности булева перманента непосредственно вытекает

Следствие 5. *Любая* $(\min,+,\max)$*-схема, вычисляющая* Per_n*, имеет сложность* $n^{\Omega(\log n)}$.

Открытая проблема 4. *Можно ли тропический перманент* Per_n *вычислить* $(\min,+,-)$*-схемой полиномиального размера?*

В действительности представляет интерес решение даже ослабленной версии проблемы 3.

Открытая проблема 5. *Может ли быть сверхполиномиальным отношение* $(\min,\max)/(\min,+,-)$?

Следующая задача состоит в получении нетривиальных *нижних* оценок сложности $(\min,+,-)$-схем, где под нетривиальными понимаются оценки для тропических многочленов не слишком высокой степени. Скажем, нижняя оценка 2^n для $(\min,+,-)$-сложности многочлена $P(x,y)=\max\{2^{2^n}x,y\}$ дважды экспоненциальной степени тривиальна.

Открытая проблема 6. *Доказать нетривиальную нижнюю оценку сложности* $(\min, +, -)$*-схем.*

Арифметический аналог $(\min, +, -)$-схем — это $(+, \cdot, /)$-схемы. С. Фомин, Д. Григорьев и Г. Кошевой [10] получили экспоненциальную нижнюю оценку сложности $(+, \cdot, /)$-схем косвенным образом, конструируя трудновычислимый многочлен при помощи *вычитания*. Хотя операции вычитания нет в базисе $(+, \cdot, /)$, некоторые многочлены с отрицательными коэффициентами все же могут быть реализованы $(+, \cdot, /)$-схемами. Например, многочлен $f(x,y) = x^2 - xy + y^2$ можно вычислить по формуле $f = (x^3 + y^3)/(x + y)$. В общем случае, согласно результату Д. Пойа [17], однородный многочлен F, принимающий положительные значения $F(x) > 0$ при любых $x \in \mathbb{R}^n_+$, $x_1 + \dots + x_n = 1$, представим в виде $F(x) = P(x)/(x_1 + \dots + x_n)^r$, где $r \geqslant 1$, и многочлен P не имеет отрицательных коэффициентов. Поэтому любой такой многочлен F может быть реализован $(+, \cdot, /)$-схемой.

Авторы [10] указали конкретный однородный многочлен F степени 4 от n переменных, имеющий отрицательные коэффициенты, но удовлетворяющий условию Пойа и поэтому представимый в виде отношения P/Q многочленов с положительными коэффициентами. При этом многочлен P в любом подобном представлении должен иметь степень $d \geqslant 2^{2^{n-2}}$. Ввиду того, что $(+, \cdot, /)$-схемой сложности s не может быть реализован многочлен степени выше 2^s, сложность любой $(+, \cdot, /)$-схемы, вычисляющей F, не меньше $s \geqslant \log_2 d \geqslant 2^{n-2}$.

Этот результат не удается перенести непосредственно на случай тропических $(\min, +, -)$-схем. Прежде всего потому, что в тропических кольцах аддитивная операция (min или max) необратима. Другое препятствие связано с формулировкой тропического аналога теоремы Пойа. Даже тот факт, что функция, реализуемая $(\min, +, -)$-схемой, неотрицательна (принимает неотрицательные значения на неотрицательных входах), не означает, что эта функция может быть вычислена $(\min, +, \max)$-схемой. Это видно на примере многочлена Лорана $P(x,y) = \max\{x - y, y - x\}$, который можно вычислить по формуле $\max\{x, y\} - \min\{x, y\}$. Таким образом, проблема 6 может быть даже труднее, чем проблема 3.

Авторы благодарны Владимиру Лысикову за плодотворные обсуждения на начальном этапе исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. — М.: Вильямс, 2004.
2. Левин А. Ю. Алгоритм кратчайшего соединения группы вершин графа // Докл. АН СССР. — 1971. — Т. 200(4). — С. 773–776.
3. Разборов А. А. Нижние оценки монотонной сложности логического перманента // Матем. заметки. — 1985. — Т. 37(6). — С. 887–900.
4. Alon N., Tarsi M. Colorings and orientations of graphs // Combinatorica. — 1992. — V. 12. — P. 125–134.
5. Bellman R. On a routing problem // Quarterly of Appl. Math. — 1958. — V. 16. — P. 87–90.
6. Bellman R. Dynamic programming treatment of the travelling salesman problem // J. ACM. — 1962. — V. 9, No 1. — P. 61–63.
7. Dreyfus S. E., Wagner R. A. The Steiner problem in graphs // Networks. — 1971. — V. 1, No 3. — P. 195–207.

8. Fan K. On systems of linear inequalities // in: Linear inequalities and related systems (AM-38). Princeton, Princeton University Press, 1956, P. 99–156.
9. Floyd R. W. Algorithm 97, shortest path // Comm. ACM. — 1962. — V. 5. — P. 345.
10. Fomin S., Grigoriev D., Koshevoy G. Subtraction-free complexity, cluster transformations, and spanning trees // Found. Comput. Math. — 2016. — V. 15. — P. 1–31.
11. Ford L. R. Network flow theory // The Rand Corp. — 1956. — Report no. P-923.
12. Held M., Karp R. M. A dynamic programming approach to sequencing problems // SIAM J. on Appl. Math. — 1962. — V. 10. — P. 196–210.
13. Jerrum M., Snir M. Some exact complexity results for straight-line computations over semirings // J. ACM. — 1982. — V. 29, No 3. — P. 874–897.
14. Jukna S., Seiwert H. Greedy can beat pure dynamic programming // Inf. Process. Letters — 2019. — V. 142. — P. 90–95.
15. Jukna S., Seiwert H. Sorting can exponentially speed up pure dynamic programming // Inf. Process. Letters — 2020. — V. 159–160. — Art. 105962.
16. Moore E. F. The shortest path through a maze // Proc. Internat. Sympos. Switching Theory. — 1957. — V. II. — P. 285–292.
17. Pólya G. Über positive Darstellung von Polynomen. in Vierteljschr. Naturforsch. Ges. Zürich. — 1928. — Jah. 73.
18. Roy B. Transitivité et connexité // C. R. Acad. Sci. Paris. — 1959. — V. 249. — P. 216–218.
19. Strassen V. Vermeidung von Divisionen // J. Reine Angew. Math. — 1973. — V. 264. — P. 184–202.
20. Tardos É. The gap between monotone and non-monotone circuit complexity is exponential // Combinatorica. — 1988. — V. 8, No 1. — P. 141–142.
21. Valiant L. G. Negation can be exponenially powerful // Theor. Comput. Sci. — 1980. — V. 12. — P. 303–314.
22. Warshall S. A theorem on boolean matrices // J. ACM. — 1962. — V. 9. — P. 11–12.

Поступило в редакцию 19 I 2022