ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2004. Серия 1. Том 11, № 4, 44–55

УДК 519.16

О СЛОЖНОСТИ ОБРАЩЕНИЯ ДИСКРЕТНЫХ ФУНКЦИЙ ИЗ ОДНОГО КЛАССА*)

А. А. Семенов

Рассматривается обращение некоторых дискретных функций, встречающихся в криптографии. Устанавливается сводимость по Куку задач обращения таких функций к задачам, принадлежащим NP∩co-NP. Изучаются конъюнктивные нормальные формы (КНФ), выполнимые в точности на одном наборе. Показывается, что задача поиска выполняющего набора в таких КНФ сводится по Куку к проблеме из NP∩co-NP, тогда как задача распознавания таких КНФ является co-NP трудной.

Введение

Через $\{0,1\}^n$ обозначается множество всех двоичных векторов длины n. В качестве формальной вычислительной модели рассматривается машина с неограниченными регистрами (МНР). Введем в рассмотрение семейство дискретных функций $F = \{f_n(x)\}_{n\in N}$, $x \in \{0,1\}^n$, обладающее следующими свойствами. Для каждого $n \in$N существует МНР-программа $M(f_n)$, вычисляющая $f_n(x)$. Область определения функции $f_n(x)$ обозначим через $\mathrm{Dom}(f_n)$, $\mathrm{Dom}(f_n)\subseteq \{0,1\}^n$. Областью значений функции $f_n(x)$ является множество, обозначаемое через $\mathrm{Ran}(f_n)$, такое, что $\mathrm{Ran}(f_n)\subseteq \{0,1\}^m$ для некоторого $m \in$N. Каждой функции f_n ставится в соответствие наибольшее (по всем векторам из множества $\mathrm{Dom}(f_n)$) число шагов, совершаемых МНР, выполняющей программу $M(f_n)$. Полученную функцию обозначаем через $\rho(f_n)$. Данная функция выражает алгоритмическую сложность семейства функций F. Далее рассматриваются только такие семейства дискретных функций, для которых функция $\rho(f_n)$ ограничена сверху некоторым полиномом от n.

Проблема обращения произвольной дискретной функции из семейства F ставится следующим образом. По данному $y \in\mathrm{Ran}(f_n)$ требуется найти хотя бы одно $x \in\mathrm{Dom}(f_n)$ такое, что $f_n(x) = y$.

*)Исследование выполнено при поддержке программы РАН № 19 (проект 2.5).

Далее показывается, что задачи обращения дискретных функций из определяемого ниже класса допускают сводимость по Куку к проблемам из NP∩co-NP. При этом используется следующее определение сводимости по Куку ([3],[8]).

Определение 1. Под *полиномиальной сводимостью* по Тьюрингу проблемы Π_1 к проблеме Π_2 понимается возможность решить проблему Π_1 за полиномиальное время (от длины данных, кодирующих Π_1) после однократного обращения к оракулу, выдающему решение проблемы Π_2. Сводимость в смысле Кука допускает полиномиальное от длины входа число раз использование полиномиальной сводимости по Тьюрингу.

§ 1. Обращение функций с ограничениями на число прообразов

Ниже рассматривается один класс дискретных функций, которому принадлежат многие известные на сегодняшний день предположительно односторонние функции. Последние широко используются в несимметричной криптографии.

Рассмотрим произвольное семейство F дискретных функций из определенного выше класса. Обозначим через $\Delta_{f_n}(y)$ число таких $x \in \mathrm{Dom}(f_n)$, что $f_n(x) = y$. Семейству $F = \{f_n(x)\}_{n \in N}$ поставим в соответствие следующую функцию

$$\delta(f_n) = \max_{y \in Ran(f_n)} \Delta_{f_n}(y).$$

Обозначим через Λ класс таких дискретных функций, для которых функция $\delta(f_n)$ ограничена сверху некоторым полиномом от n.

Обозначим через $\Pi(F^{-1})$ следующую проблему. По произвольной функции f_n семейства $F \in \Lambda$, произвольному $y \in \mathrm{Ran}(f_n)$ и числу $\Delta_{f_n}(y)$ требуется найти такое $x \in \mathrm{Dom}(f_n)$, что $f_n(x) = y$.

Пример 1. 2-ФАКТОРИЗАЦИЯ. Дано натуральное число K, про которое известно, что существуют два простых числа p и q такие, что $p \neq q$ и $K = p \cdot q$. Требуется найти p и q. Данную проблему сформулируем в контексте проблемы $\Pi(F^{-1})$. Рассмотрим два натуральных числа r и s из множества $\{0, 1, \ldots, 2^k - 1\}$. Пусть r_b и s_b — векторы из $\{0,1\}^k$, являющиеся представлениями чисел r и s по степеням $2^0, \ldots, 2^{k-1}$. Обозначим через $\Gamma(r_b, s_b)$ алгоритм перемножения «столбиком» чисел r и s, оперирующий векторами r_b, и s_b. Семейство дискретных функций $F = \{f_n(x)\}_{n \in N}$ определим следующим образом. Для каждого нечетного n функция $f_n(x)$ не определена. Для каждого четного n функция $f_n(x)$ определена всюду на $\{0,1\}^n$. Опишем алгоритм вычисления

$f_n(x)$. Двоичный вектор $x \in \{0,1\}^n$ представляется в следующем виде: $x = (x^1|x^2)$, где $x^1 \in \{0,1\}^{\frac{n}{2}}$ и $x^2 \in \{0,1\}^{\frac{n}{2}}$. После этого находится вектор $y = \Gamma(x^1, x^2)$, $y \in \{0,1\}^n$. Таким образом, 2-ФАКТОРИЗАЦИЯ является частным случаем проблемы обращения функций из введенного выше класса: предполагается, что известен вектор y, являющийся представлением числа K по степеням $2^0, \ldots, 2^{n-1}$, и известно, что существует в точности два вектора $x^1 \in \{0,1\}^{\frac{n}{2}}$ и $x^2 \in \{0,1\}^{\frac{n}{2}}$, перемножение которых «столбиком» дает y, требуется найти векторы x^1 и x^2. Предположение, что данная проблема не может быть решена за полиномиальное от n время для почти всех K является аргументом стойкости криптосистемы Ривеста–Шамира–Адлмана (RSA) [9].

Пример 2. Дискретное логарифмирование по простому модулю. Дано простое число p, мультипликативная группа вычетов по модулю p, обозначаемая через H_p^*, и примитивный элемент $\omega \in H_p^*$. По произвольному $y \in H_p^*$ требуется вычислить его «дискретный логарифм», т. е. такое натуральное число $x \in \{1, \ldots, p-1\}$, что $y \equiv \omega^x (\mathrm{mod}\, p)$. Каждому $x \in \{1, \ldots, p-1\}$ соответствует в точности один $y \in H_p^*$ такой, что $y \equiv \omega^x (\mathrm{mod}\, p)$. Дискретное возведение в степень реализуется за время, ограниченное сверху полиномом от $\log p$. Таким образом, задача дискретного логарифмирования является частным случаем проблемы $\Pi(F^{-1})$. Эта проблема также предположительно не может быть решена за полиномиальное от $\log p$ время для почти всех $y \in H_p^*$.

Следующее утверждение (в несколько ином виде сформулированное автором в [5]) использует простейшую схему поиска, основанную на дихотомии.

Лемма. *Проблема* $\Pi(F^{-1})$ *сводится по Куку к проблеме из* NP∩co-NP.

Доказательство. Рассматриваем произвольное семейство дискретных функций $F \in \Lambda$. Пусть дано некоторое $y \in \mathrm{Ran}(f_n)$. Требуется найти произвольное $x \in \mathrm{Dom}(f_n)$ такое, что $f_n(x) = y$. Множество всех двоичных векторов длины n разобьем на два подмножества S_0 и S_1 (первый уровень разбиения). Подмножество S_0 состоит из всех двоичных векторов, старшим разрядом которых является 0, S_1 состоит из всех двоичных векторов, старшим разрядом которых является 1. Произвольному $y \in \mathrm{Ran}(f_n)$ поставим в соответствие предикат

$$\Theta_1(y) = \begin{cases} 1, & \text{если существует } x \in S_0 \text{ такое, что } f_n(x) = y, \\ 0, & \text{если } f_n(x) \neq y \text{ для любого } x \in S_0. \end{cases}$$

Ясно, что данный предикат принадлежит классу NP. Действительно, ес-

ли $\Theta_1(y) = 1$, то полиномиально проверяемым сертификатом является двоичный вектор $x \in S_0$ такой, что $f_n(x) = y$. Менее очевидно, что $\Theta_1(y) \in$co-NP. Убедимся в этом. Предикат, дополнительный к $\Theta_1(y)$, имеет вид

$$\Theta_1^{co}(y) = \begin{cases} 1, \text{ если } f_n(x) \neq y \text{ для любого } x \in S_0, \\ 0, \text{ если существует } x \in S_0 \text{ такое, что } f_n(x) = y. \end{cases}$$

Обозначим через $X_y \subset \mathrm{Dom}(f_n)$ множество прообразов y. Предположим, что $\Theta_1^{co}(y) = 1$. Тогда ни один из прообразов y не лежит в S_0. Это означает, что все прообразы находятся в $S_1 = \{0,1\}^n \backslash S_0)$. Однако число $\Delta_{f_n}(y) = |X_y|$ для произвольного $y \in \mathrm{Ran}(f_n)$ известно по постановке проблемы $\Pi(F^{-1})$. Функция $\delta(f_n)$ ограничена сверху некоторым полиномом от n. Таким образом, сертификатом для предиката $\Theta_1^{co}(y)$, проверяемым за полиномиальное от n время, является множество X_y: достаточно перебрать все $\Delta_{f_n}(y)$ элементов из X_y, убеждаясь относительно каждого $x \in X_y$, что $x \notin S_0$ (достаточно убедиться, что старший разряд каждого $x \in X_y$ равен 1). Таким образом, $\Theta_1(y) \in$NP$\cap$co-NP.

Предположим, что существует оракул, который вычисляет предикат $\Theta_1(y)$ для произвольного $y \in \mathrm{Ran}(f_n)$. После того как выяснено, какое из множеств S_0 и S_1 содержит прообраз y (хотя бы один), данное множество снова разбивается на пару подмножеств (второй уровень разбиения), например, $S_0 = S_{00} \cup S_{01}$, где S_{00} — это множество векторов из S_0, начинающихся фрагментом 00, а S_{01} — множество векторов из S_0, начинающихся фрагментом 01. Аналогичным образом для произвольного $y \in \mathrm{Ran}(f_n)$ вводятся предикаты $\Theta_2(y)$, $\Theta_2^{co}(y)$ и показывается, что $\Theta_2(y) \in$ NP$\cap$ co-NP (полиномиально проверяемым сертификатом, подтверждающим, что ни один из прообразов y не лежит, скажем, в S_{00}, снова является множество X_y: для каждого $x \in X_y$ достаточно убедиться, что x не начинается с 00). Нижний индекс предиката Θ соответствует уровню разбиения.

Очевидно, что результатом n-кратного применения описанной схемы к произвольному $y \in \mathrm{Ran}(f_n)$ является некоторый прообраз y. В ходе реализации данной схемы использовался оракул, решающий задачу из NP$\cap$co-NP. Поэтому проблема нахождения по произвольному $y \in \mathrm{Ran}(f_n)$ такого $x \in \mathrm{Dom}(f_n)$, что $f_n(x) = y$, для рассматриваемого класса функций допускает сводимость по Куку к проблеме из NP$\cap$co-NP. Лемма доказана.

§ 2. Сложность некоторых проблем поиска

Определение 2. Полиномиально вычислимыми перестановками будем называть такие семейства дискретных функций $F = \{f_n(x)\}$, где $n \in N$ и $x \in \{0,1\}^n$ такие, что для каждого $n \in$N область значений функции $f_n(x)$ совпадает с ее областью определения.

Следствие 1. *Проблема* $\Pi(F^{-1})$*, где* F *— семейство полиномиально вычислимых перестановок, сводится по Куку к проблеме из* NP∩co-NP.

В качестве примера, иллюстрирующего данный факт, рассмотрим проблему дискретного логарифмирования. Пусть p — простое число. Каждому натуральному числу из $\{1, ..., p-1\}$ поставим в соответствие двоичный вектор длины $n = \lceil \log p \rceil$, являющийся двоичной записью данного числа. Таким образом, имеем множество двоичных векторов $B = \{b_1, ..., b_{p-1}\}$ и перестановку $f_n : B \to B$ — дискретное возведение в степень по модулю p. Для произвольного вычета $y \in H_p^*$ (в двоичной кодировке) ставим вопрос: верно ли, что единственный прообраз y при отображении f_n находится среди векторов множества B, старший разряд которых равен 0? Если ответ на поставленный вопрос «нет», то прообраз y обязательно находится среди векторов B, старший разряд которых равен 1. Рассуждая по аналогии с доказательством леммы, убеждаемся в том, что задача дискретного логарифмирования сводится по Куку к проблеме из NP∩co-NP.

Теперь рассмотрим следующую проблему поиска, известную как ФАКТОРИЗАЦИЯ. Дано составное натуральное число K. Требуется найти его каноническое представление, т. е. представить число K в виде

$$K = p_1^{r_1} \cdot ... \cdot p_{\lambda(K)}^{r_{\lambda(K)}}, \tag{1}$$

где $p_1, ..., p_{\lambda(K)}$ — различные простые числа, $r_1, ..., r_{\lambda(K)}$ — натуральные показатели.

Приведем полное доказательство следующего утверждения, поскольку аналогичный результат в доступных источниках найти не удалось.

Теорема 1. *Проблема* ФАКТОРИЗАЦИЯ *сводится по Куку к проблеме из NP∩co-NP.*

Доказательство. Согласно основной теореме арифметики произвольное составное число K может быть единственным образом представлено в виде (1). Воспользуемся следующей очевидной (и весьма грубой) оценкой: $\lambda(K) \leqslant O(\log K)$. Сразу не очевидно, что ФАКТОРИЗАЦИЯ может рассматриваться в контексте проблемы $\Pi(F^{-1})$. Действительно,

число $\tau(K)$ различных делителей натурального числа K, как известно (например, из [2]), может вести себя следующим образом:

$$\tau(K) = O(K^{\varepsilon}),$$

где $\varepsilon > 0$ — некоторая константа. Следовательно, величина $\tau(K)$ в общем случае не ограничена никаким полиномом от $\log K$.

Тем не менее в качестве искомого «прообраза» для данного составного числа K можно рассматривать набор всех его простых делителей (такой набор единствен). После чего остается построить детерминированную процедуру с полиномиальным (от $\log K$) временем работы, которая по предъявленному набору чисел решает, верно ли, что данный набор образован *всеми* простыми делителями числа K. В этом состоит основная идея доказательства.

Ясно, что если число K составное, то существует его простой делитель, не превосходящий $\lfloor\sqrt{K}\rfloor$. Далее везде полагаем, что число K не является степенью двойки. Тогда ему можно поставить в соответствие множество $B_{\lfloor\sqrt{K}\rfloor}$ двоичных векторов длины $\lceil\log\lfloor\sqrt{K}\rfloor\rceil$, являющихся двоичными представлениями чисел от 0 до $\lfloor\sqrt{K}\rfloor$. Дальнейшая схема полностью аналогична приведенной в доказательстве леммы. На первом этапе решаем следующую задачу: верно ли, что множество векторов из $B_{\lfloor\sqrt{K}\rfloor}$, старший разряд которых равен нулю, содержит двоичное представление простого делителя числа K? Соответствующий данной проблеме предикат обозначим через $\Theta_1(K)$. Очевидно, что $\Theta_1(K) \in$NP, поскольку если x — простой делитель числа K, то данный факт может быть подтвержден при помощи алгоритма Евклида (так как в этом случае Н.О.Д. $(K, x) = x$) и полиномиального алгоритма, устанавливающего простоту числа x (алгоритм описан в [6]). Дополнительный к $\Theta_1(K)$ предикат $\Theta_1^{co}(K)$, принимает значение «истина», если множество векторов из $B_{\lfloor\sqrt{K}\rfloor}$, старший разряд которых равен нулю, не содержит двоичных представлений простых делителей K. Покажем, что $\Theta_1^{co}(K) \in$NP. Предположим, что $\Theta_1^{co}(K) = 1$. Сертификатом, проверяемым за полиномиальное (от $\log K$) время, являются *все* различные простые делители числа K, т. е. числа $p_1, ..., p_{\lambda(K)}$. Простота каждого числа подтверждается за полиномиальное время при помощи алгоритма из [6]. Остается показать, как по набору различных простых чисел $p_1, ..., p_\mu$ за полиномиальное от $\log K$ время проверить, выполняется ли равенство $\mu = \lambda(K)$. Итак, даны числа $p_1, ..., p_\mu$, относительно которых установлено, что они простые. Последовательно делим число K на $p_1, p_1^2, ...$ до тех пор, пока

не будет получено соотношение

$$\text{Н.О.Д.}\left(\frac{K}{p_1^{r_1}}, p_1\right) = 1.$$

Время, которое на это потребуется, ограничено полиномом от $\log K$. После этого от числа K осуществляется переход к числу $\frac{K}{p_1^{r_1}}$, которое последовательно делится на степени числа p_2 и так далее. Очевидно, что $\mu = \lambda(K)$ тогда и только тогда, когда итогом данной процедуры является равенство

$$\frac{K}{p_1^{r_1} \cdot \ldots \cdot p_\mu^{r_\mu}} = 1.$$

При этом максимальное число шагов деления равно $\sum\limits_{i=1}^{\lambda(K)} r_i$. Последнее число ограничено полиномом от $\log K$. Таким образом, предикат $\Theta_1^{co}(K) \in$NP. Дальнейшее применение дихотомической схемы к следующим уровням разбиения множества $B_{\lfloor\sqrt{K}\rfloor}$ дает сводимость по Куку общей задачи ФАКТОРИЗАЦИЯ к задаче из NP∩co-NP. Теорема 1 доказана.

Следствие 2. *Если в общем случае* ФАКТОРИЗАЦИЯ *не может быть решена за полиномиальное время, то справедливо строгое включение* P⊂NP∩co-NP.

§ 3. О сложности задачи, полной в смысле обращения полиномиально вычислимых перестановок

В криптографических приложениях особый интерес представляют полиномиально вычислимые перестановки и аргументация сложности задач их обращения. В работе [4] ставится проблема построения полных односторонних функций. В данном параграфе рассмотрим задачу, полную в смысле обращения полиномиально вычислимых перестановок.

Рассматриваем произвольную конъюнктивную нормальную форму C над множеством булевых переменных $X = \{x_1, \ldots, x_n\}$:

$$C = D_1 \cdot \ldots \cdot D_m. \tag{2}$$

Каждый дизъюнкт D_j в (2) имеет вид $D_j = z_1 \vee \ldots \vee z_{s(j)}$, где z_i — некоторые литералы над X, $1 \leqslant i \leqslant s(j)$, $1 \leqslant s(j) \leqslant n$, $j \in \{1, \ldots, m\}$.

Определение 3. Конъюнктивную нормальную форму (КНФ) C над множеством булевых переменных $X = \{x_1, \ldots, x_n\}$ назовем *сильно обусловленной,* если она выполнима на единственном наборе значений истинности переменных из X.

Теорема 2. *Класс сильно обусловленных* КНФ *обладает перечисленными ниже свойствами*:

1) *проблема поиска выполняющего набора для произвольной сильно обусловленной* КНФ *сводится по Куку к проблеме из* NP∩co-NP;

2) *проблема распознавания сильно обусловленных* КНФ *находится в* Σ_2^p *и является* co-NP *трудной.*

Доказательство. Пусть имеется КНФ C вида (2), про которую известно, что она сильно обусловлена. Обозначим через $(\alpha_1, ..., \alpha_n)$ единственный вектор из $\{0,1\}^n$, выполняющий C. Проблема «верно ли, что первый бит набора, выполняющего C, равен 1?» находится в NP. Действительно, если ответ на данный вопрос есть «да», то существует подтверждающий этот ответ и проверяемый за полиномиальное время сертификат — вектор $(\alpha_1, ..., \alpha_n)$. Сформулируем проблему, дополнительную к данной. Это проблема «верно ли, что первый бит набора, выполняющего C, не равен 1 (т. е. равен 0)?». Так как КНФ C выполнима на единственном наборе, то и данная проблема (в случае ответа «да») имеет сертификат, проверяемый за полиномиальное от n время, и этим сертификатом является вектор $(\alpha_1, ..., \alpha_n)$. Таким образом, если C сильно обусловлена, то задача «верно ли, что первый бит выполняющего C набора равен 1?» лежит в NP∩co-NP. Предположим, что данная задача решена и найдено значение $x_1 = \alpha_1$. Подставив α_1 в C вместо x_1, получим КНФ, обозначаемую через $C|_{x_1=\alpha_1}$. Несложно понять, что данная КНФ также является сильно обусловленной над множеством булевых переменных $\{x_2, \ldots, x_n\}$. К ней снова применяем описанную процедуру. Таким образом, для нахождения вектора $(\alpha_1, ..., \alpha_n)$, выполняющего произвольную сильно обусловленную КНФ, требуется n раз решить задачу, находящуюся в NP∩co-NP. Данный факт означает справедливость первой части теоремы.

Докажем вторую часть. Покажем, что проблема распознавания сильно обусловленных КНФ находится в Σ_2^p. В самом деле, КНФ C над множеством булевых переменных мощности n является сильно обусловленной тогда и только тогда, когда существует такой вектор $x \in \{0,1\}^n$, что $C|_x = 1$, и $C|_y = 0$ для любого вектора $y \in \{0,1\}^n$, отличного от x. Введем в рассмотрение предикат $R(C, x, y)$, истинный тогда и только тогда, когда выполнены одновременно условия: $C|_x = 1, C|_y = 0, y \neq x$. Очевидно, что для любой КНФ C, произвольного $x \in \{0,1\}^n$ и любого $y \in \{0,1\}^n$ истинность предиката R проверяется за полиномиальное от n время. Последнее означает, что проблема распознавания сильно обусловленных КНФ находится в Σ_2^p. Покажем, что данная проблема

co-NP-трудна. Рассмотрим произвольную КНФ C вида (2). Выберем произвольный вектор $(\alpha_1, ..., \alpha_n) \in \{0,1\}^n$. Рассмотрим пропозициональное выражение

$$C^* = C \vee x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}, \tag{3}$$

где

$$x^\alpha = \begin{cases} x, \text{если } \alpha = 1, \\ \overline{x}, \text{если } \alpha = 0. \end{cases}$$

Очевидно, что C^* выполнимо на всех тех наборах, на которых выполнима C, и на наборе $(\alpha_1, ..., \alpha_n)$. Используя дистрибутивность, преобразуем (3) в выражение

$$C^* = (C \vee x_1^{\alpha_1}) \cdot ... \cdot (C \vee x_n^{\alpha_n}). \tag{4}$$

Снова воспользуемся дистрибутивностью и последнее выражение запишем в виде КНФ

$$C^* = D_1^* \cdot ... \cdot D_r^*, \tag{5}$$

где $r = mn$. Очевидно, что в (4) литерал $x_i^{\alpha_i}, i \in \{1, ..., n\}$, «внедряется» в логическое произведение $C = \bigwedge\limits_{j=1}^{m} D_j$ следующим образом:

$$\left(\bigwedge_{j=1}^{m} D_j \right) \vee x_i^{\alpha_i} = \bigwedge_{j=1}^{m} (D_j \vee x_i^{\alpha_i}).$$

Если при этом в дизъюнкции D_j содержится литерал $x_i^{\overline{\alpha}_i}$, то $D_j \vee x_i^{\alpha_i} \equiv 1$. Таким образом, при описанной процедуре преобразования C в C^* ряд дизъюнкций в (5) могут превратиться в тождественно истинные (фиктивные). Окончательно имеем процедуру преобразования исходной произвольной КНФ C в выполнимую КНФ C^*, состоящую не более чем из mn дизъюнктов над над X. Очевидно, что сложность описанной процедуры в общем случае ограничена полиномом от mn.

Рассмотрим проблему, дополнительную к проблеме ВЫПОЛНИМОСТЬ: «по произвольной КНФ C над $X = \{x_1, ..., x_n\}$ определить, верно ли, что C невыполнима». Данная проблема co-NP полна ([3]). Выберем произвольный вектор $(\alpha_1, ..., \alpha_n) \in \{0,1\}^n$. Если C выполнима на $(\alpha_1, ..., \alpha_n)$, то ответ на поставленный вопрос «нет». Если $C|_{(\alpha_1,...,\alpha_n)} = 0$, преобразовываем C в КНФ C^* с использованием соотношений (2)–(5). Полученная КНФ выполнима в точности на одном наборе (а именно, на $(\alpha_1, ..., \alpha_n)$) тогда и только тогда, когда C невыполнима. Построенная сводимость является полиномиальной сводимостью по Тьюрингу

co-NP-полной проблемы к проблеме распознавания сильно обусловленных КНФ. Следовательно, последняя co-NP-трудна. Теорема 2 доказана.

Приведем рассуждения, которые позволяют считать задачу поиска выполняющих наборов для сильно обусловленных КНФ полной в том смысле, что за полиномиальное время к ней можно свести задачу обращения произвольной дискретной перестановки. Для этого потребуется понятие консервативной сводимости, впервые, по-видимому, использованное Дж. Саймоном в [10] (также см. [3]).

Определение 4. Пусть φ — полиномиальная сводимость Карпа и $\varphi(\Pi_1) = \Pi_2$. Сводимость φ называется *консервативной* тогда и только тогда, когда $|S(I_2)| = |S(I_1)|$ для любой индивидуальной задачи $I_2 \in D_{\Pi_2}$, $I_2 = \varphi(I_1)$. Здесь D_Π обозначает множество всех индивидуальных задач данной массовой проблемы Π, а $S(I)$ — множество всех сертификатов, подтверждающих ответ «да» для $I \in D_\Pi$ (если ответ на I — «нет», то $S(I) = \oslash$).

В [1] построена консервативная сводимость проблемы 2-ФАКТОРИЗАЦИЯ к проблеме поиска выполняющих наборов сильно обусловленных КНФ. Данная сводимость осуществляет преобразование *алгоритма* умножения «столбиком» пары натуральных чисел в КНФ и может рассматриваться как модификация сводимости, впервые предложенной С. А. Куком в работе [7]. Идею редукции из [1] технически несложно перенести на проблему обращения произвольного семейства полиномиально вычислимых перестановок. Результатом является консервативная сводимость данной проблемы к проблеме поиска выполняющих наборов для семейств сильно обусловленных КНФ.

Заключительные замечания

Основной результат настоящей статьи состоит в том, что проблемы обращения дискретных функций из достаточно широкого класса допускают сводимость по Куку к проблемам из NP∩co-NP. Сказанное относится к проблеме факторизации составного числа и проблеме дискретного логарифмирования по простому модулю. В предположении, что данные проблемы почти всегда не могут быть решены за полиномиальное время, приводятся аргументы стойкости разнообразных несимметричных криптосистем. Таким образом, принципиальный для криптографии вопрос состоит в аргументации включения P⊂NP∩co-NP, а также в поиске задач, которые, находясь в NP∩co-NP, не попадают в P. Интересной кандидатурой на роль такой задачи является следующая проблема распознавания. По произвольной сильно обусловленной КНФ C, заданной

над множеством булевых переменных $X = \{x_1, ..., x_n\}$, и натуральному числу $k, 1 \leqslant k \leqslant n$, определить, верно ли, что k-й разряд набора, выполняющего C, равен 1.

С другой стороны, вызывает интерес вопрос о том, существуют ли полиномиальные редукции проблемы поиска выполняющего набора сильно обусловленной КНФ к проблемам обращения известных предположительно односторонних функций, в первую очередь к проблеме факторизации и проблеме дискретного логарифмирования. Наличие таких редукций дало бы дополнительные аргументы в пользу высокой вычислительной сложности данных задач.

ЛИТЕРАТУРА

1. **Беспалов Д. В., Семенов А. А.** О логических выражениях для задачи 2-ФАКТОРИЗАЦИЯ// Вычислительные технологии. 2002. Т. 7, часть 2. С. 18–25.
2. **Виноградов И. М.** Основы теории чисел. М.: Наука, 1981.
3. **Гэри М., Джонсон Д.** Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
4. **Левин Л. А.** Односторонние функции// Проблемы передачи информации. 2003. Т. 39, вып. 1. С. 103–117.
5. **Семенов А. А.** Замечание о вычислительной сложности известных предположительно односторонних функций// Труды XII Байкальской международной конференции «Методы оптимизации и их приложения» (Иркутск, 24 июня – 1 июля 2001 г.). Т. 5. Дискретная математика. Иркутск: Изд-во ИрГУ, 2001. С. 142–146.
6. **Agrawal M., Kayal N., Saxena N.** Primes is in P. 2002. Preprint. Department of Computer Science and Engineering Indian Institute of Technology, Kanpur, India.
7. **Cook S. A.** The complexity of theorem-proving procedures// Proc. of the third annual ACM symposium on theory of computing (Ohio, May 3–5, 1971). New York: IEEE, 1971. P. 151–158. (Русский перевод: Кук С. А. Сложность процедур вывода теорем// Кибернетический сборник. Новая серия. Вып. 12. М.: Мир, 1975. С. 5–15.)
8. **Goldreich O.** Introduction to complexity theory. Lecture Notes, Weizmann Institute of Science, Israel, 1999.

9. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public–key cryptosystems// Commun. ACM. 1978. V. 21, N 2. P. 120–126.

10. Simon J. On some central problems in computational complexity. Doctoral Thesis, Cornel University, Ithaca, NY, 1975.

Адрес автора:
Институт динамики систем
и теории управления СО РАН,
ул. Лермонтова, 134,
664033 Иркутск, Россия.

Статья поступила
15 апреля 2004 г.

Переработанный вариант —
23 августа 2004 г.