Записки научных
семинаров ПОМИ
Том 402, 2012 г.

С. И. Николенко, Д. С. Тугарёв

ПОЛНАЯ ОДНОСТОРОННЯЯ ФУНКЦИЯ, ОСНОВАННАЯ НА СВОБОДНОМ $(\mathbb{Z}\times\mathbb{Z})$-МОДУЛЕ КОНЕЧНОГО РАНГА

§1. Введение

В теоретической информатике полные задачи являются незаменимым инструментом для изучения сложностных классов; они позволяют сводить рассмотрение всего класса к рассмотрению единственной представляющей этот класс задачи. В определённом смысле, современная теория сложности началась с теоремы Кука–Левина [4, 22] и последовавшего за ней изучения NP-полных задач [5, 12]. Известны конструкции полных задач для разных классов сложности, в том числе (что будет важно для последующего изложения) задачи, полные с точки зрения сложности в среднем [2, 8, 13, 20]; см. также [1, 18, 19].

Однако в криптографии полные задачи практически неизвестны. Лишь совсем недавно была найдена полная задача для класса криптосистем с открытым ключом (с ограниченной ошибкой декодирования) [7, 9]. Для более простых криптографических объектов – односторонних функций – первые полные конструкции были получены Л.А. Левиным [14] (см. также [6, 21, 23]). Полнота понимается здесь в следующем смысле.

Определение 1. *Пусть функция $f\colon \{0,1\}^* \to \{0,1\}^*$ обладает следующим свойством: если существует сильно (слабо) односторонняя функция $g\colon \{0,1\}^* \to \{0,1\}^*$, то f также является сильно (слабо) односторонней. Тогда f называется* полной *сильно (слабо) односторонней функцией.*

Ключевые слова: односторонние функции, сложность в среднем, задачи замощения.

Эта работа была выполнена при финансовой поддержке гранта Президента РФ для молодых кандидатов наук МК-6628.2012.1, гранта Президента РФ для ведущих научных школ НШ-3329.2012.1 и грантов Российского Фонда Фундаментальных Исследований 11-01-12135-офи-м-2011 и 11-01-00760-а, а также Федеральной целевой программы “Научные и научно-педагогические кадры инновационной России” на 2009–2013 годы.

Обычно в теории сложности полнота подразумевает наличие *сведéний*, относительно которых полнота определяется. Однако для теории односторонних функций вопрос о сведéниях пока остаётся открытым; в [15] Левин сформулировал его как один из центральных открытых вопросов в этой области. Первая конструкция полной (слабо) односторонней функции, построенная Левиным, получила название *универсальной* односторонней функции. Эта конструкция использует универсальную машину Тьюринга U для вычисления функции

$$f_{\mathrm{uni}}(\mathrm{desc}(M), x) = (\mathrm{desc}(M), M(x)),$$

где $\mathrm{desc}(M)$ – описание машины Тьюринга M, а $M(x)$ – ответ, выдаваемый M на входе x за $\leq |x|^2$ шагов. Если среди M есть односторонние функции, то f_{uni} будет слабо односторонней функцией. Поскольку легко показать, что если есть хоть какие-то односторонние функции, то есть и односторонние функции, которые работают за квадратичное время от длины своего входа (см. предложение 1), f_{uni} является полной слабо односторонней функцией.

Левин поставил задачу поиска “комбинаторных” полных односторонних функций, которые бы не зависели от перечисления машин Тьюринга или от подачи на вход описания машин Тьюринга. В течение 15 лет проблема оставалась открытой, а затем была разрешена самим же Левиным [15]. Он использовал следующую идею: давайте полностью запретим недетерминированный выбор при вычислении самой функции, оставив его только для обращения (ниже мы подробно опишем эту конструкцию). Также Левин в [15] поставил задачу поиска других комбинаторных полных односторонних функций. В [17,21] были получены новые комбинаторные полные односторонние функции, основанные на полусистемах Туэ, задаче соответствия Поста и задаче замощения.

В этой работе мы строим новую комбинаторную полную одностороннюю функцию, основанную на представленном в [16] замощении, симулирующем работу машины Тьюринга. В [16] М. Лори и Б. Стейнберг показали неразрешимость нескольких задач, связанных с $(\mathbb{Z}\times\mathbb{Z})$-модулями и основанных на симуляции машин Тьюринга при помощи замощения.

Для конструкции полной односторонней функции мы используем идею невозвращающегося замощения, предложенную Левиным [23] и

в дальнейшем развитую в [21]. Основная идея состоит в том, чтобы симулировать детерминированную машину Тьюринга замощением таким образом, чтобы при замощении всегда можно было понять за полиномиальное время, какую плитку следует положить следующей (обычно лишь одна плитка может подходить для данного места). Мы модифицируем конструкцию замощения, предложенную в [16], так, чтобы замощение стало детерминированным, и построили новую полную одностороннюю функцию, основанную на получившейся симуляции.

Статья организована следующим образом. В разделе 2 мы вводим основные определения, и криптографические, и алгебраические, которые потребуются нам для дальнейшего. В разделе 3 мы формулируем основные результаты – конструкции новых полных односторонних функций – и доказываем соответствующие теоремы, основываясь на двух основных леммах, описывающих свойства нашей конструкции замощения. В разделе 4 мы доказываем эти основные леммы, подробно рассматривая соответствующую конструкцию замощения. Раздел 5 завершает работу.

§2. Основные определения

Сначала мы напомним основные определения теории сложности и теоретической криптографии, а затем перейдём к алгебраическим конструкциям, использующимся в нашей работе. Начнём с классического определения машины Тьюринга [10, 11].

2.1. Криптографические определения.

Определение 2. Машина Тьюринга – *это упорядоченная семёрка* $M = \langle Q, \Gamma, B, \Sigma, \pi, q_0, Q_f \rangle$, *где*

- Q – *конечное множество* состояний *машины Тьюринга*;
- Γ – *конечный алфавит* символов ленты;
- $B \in \Gamma$ – *пустой символ, пробел* (*единственный символ, который может втречаться на ленте бесконечно часто*);
- $\Sigma \subseteq \Gamma \setminus \{B\}$ – *алфавит символов, подаваемых на вход;*;
- $\pi : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ – функция перехода, *описывающая работу машины Тьюринга: L означает сдвиг головки влево, R – вправо* (*существуют также модификации определения, позволяющие головке машины Тьюринга оставаться на месте*);

- $s \in Q$ – начальное состояние *машины Тьюринга*;
- $Q_f \subseteq Q$ – *множество* конечных состояний.

Приведённые далее криптографические определения следуют книге [6].

Определение 3. *Функция* $f : \{0,1\}^* \to \{0,1\}^*$ *называется* сильно односторонней, *если выполняются следующие условия.*

(1) *Существует детерминированная машина Тьюринга* M *с входным алфавитом* $\{0,1\}$, *которая вычисляет функцию* f *за полиномиальное время.*

(2) *Для любой вероятностной машины Тьюринга* M', *любого многочлена* p *и любого достаточно большого* n

$$\Pr\left[M'(f(x), 1^n) \in f^{-1}(f(x))\right] < \frac{1}{p(n)},$$

где вероятность берётся по случайным битам машины M' *и входу* x *длины* n (*оба распределения равномерные*).

Другими словами, функция является сильно односторонней, если не существует полиномиального противника (не существует полиномиальной вероятностной машины Тьюринга), который может обратить её на какой-нибудь значительной доле входов.

Определение 4. *Функция* $f : \{0,1\}^* \to \{0,1\}^*$ *называется* слабо односторонней, *если выполняются следующие условия.*

(1) *Существует детерминированная машина Тьюринга* M *с входным алфавитом* $\{0,1\}$, *которая вычисляет функцию* f *за полиномиальное время.*

(2) *Существует такой многочлен* p, *что для любой вероятностной машины Тьюринга* M' *и для любого достаточно большого* n

$$\Pr\left[M'(f(x), 1^n) \notin f^{-1}(f(x))\right] > \frac{1}{p(n)},$$

где вероятность берётся по случайным битам машины M' *и входу* x *длины* n (*оба распределения равномерные*).

Иначе говоря, функция является слабо односторонней, если для каждого полиномиального противника найдётся существенная доля входов, на которой он не может обратить функцию. Очевидно, каждая сильно односторонняя функция является слабо односторонней, но не

наоборот. Следующее утверждение показывает, что мы можем ограничиться рассмотрением слабо односторонних функций, вычислимых за n^2 шагов детерминированной машиной Тьюринга.

Предложение 1 ([6]).

(1) *Если существует слабо односторонняя функция, то существует и сильно односторонняя функция (т.е. существование слабо и сильно односторонних функций эквивалентно).*
(2) *Если существует хотя бы одна слабо (сильно) односторонняя функция, то существует слабо (сильно) односторонняя функция, которая вычисляется машиной Тьюринга за не более чем n^2 шагов на входе длины n.*

2.2. Алгебраические определения. Теперь мы переходим к основным алгебраическим конструкциям, которые лежат в основе результатов [16] и результатов этой статьи; в описании этих структур мы будем следовать [16]. Рассмотрим группу G. (Левый) G-модуль – это абелева группа с левым действием на G автоморфизмами (модуль над групповым кольцом $\mathbb{Z}G$). Аналогично, G-полумодуль – это коммутативный моноид с левым действием на G автоморфизмами (полумодуль над групповым полукольцом $\mathbb{N}G$). Элементы G-модуля M с порождающим множеством B могут быть представлены как элементы $\widetilde{M}$ – свободного $\mathbb{Z}\Sigma^{\pm}$-модуля на B, где $\Sigma^{\pm} = \Sigma \cup \Sigma^{-1}$, а Σ – множество порождающих элементов G; это представление даётся канонической проекцией $\rho : \widetilde{M} \to M$. В [16] Лори и Стейнберг рассматривают *задачу принадлежности для подполумодуля*: для конечного множества элементов $F \subset \widetilde{M}$ и другого элемента $x \in \widetilde{M}$ определить, принадлежит ли соответствующий элемент $\rho(x) \in M$ подполумодулю $\mathbb{N}G \cdot \rho(F)$.

Все конструкции в этой работе основаны на группе $(\mathbb{Z} \times \mathbb{Z})$ и соответствующем графе Кэли Γ. Множество его вершин – это $(\mathbb{Z} \times \mathbb{Z})$, а множество рёбер графа Γ – это

$$\mathcal{E} = \{\{(p,q),(r,s)\} \mid p,q,r,s \in \mathbb{Z}, |u-x| + |v-y| = 1\}.$$

$\mathcal{M}$ является абелевой группой всех функций с конечным носителем, действующих из $\mathcal{E} \times C$ в $\mathbb{Z}$.

Пусть C – конечное множество цветов с фиксированным нулевым цветом c_0. *Системой плиток* будем называть множество $T \subseteq C^4$; элементы системы будем называть *плитками*. Поставим каждой плитке

$t = (C_N,\ C_E,\ C_S,\ C_W)$ в соответствие отображение $[\![t]\!] :\ \mathcal{E} \times C \to \mathbb{Z}$ (здесь, как и ранее, $\mathcal{E}$ – множество рёбер графа Кэли $\mathbb{Z} \times \mathbb{Z}$):

$$\begin{aligned}
[\![t]\!](\{(0,0),\ (1,0)\},\ c_S) &= -1 \cdot (1 - \delta_{c_S,c_0}),\\
[\![t]\!](\{(1,0),\ (1,1)\},\ c_E) &= 1 \cdot (1 - \delta_{c_E,c_0}),\\
[\![t]\!](\{(1,1),\ (0,1)\},\ c_N) &= 1 \cdot (1 - \delta_{c_N,c_0}),\\
[\![t]\!](\{(0,1),\ (0,0)\},\ c_W) &= -1 \cdot (1 - \delta_{c_W,c_0}),\\
[\![t]\!](e,\ c) &= 0 \text{ во всех остальных случаях.}
\end{aligned}$$

Для функции $f : \mathcal{E} \times C \to \mathbb{Z}$ с конечным носителем и вектора $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ определим трансляцию $\tau_{(a,b)} f :\ \mathcal{E} \times C \to \mathbb{Z}$ по правилу

$$\tau_{(a,b)} f(e,\ c) = f(e - (a,b),\ c) \text{ для } e \in \mathcal{E} \text{ и } c \in C.$$

Множество функций $f :\ \mathcal{E} \times C \to \mathbb{Z}$ с конечным носителем образует абелеву группу относительно поточечного сложения, и эта группа является $(\mathbb{Z}\times\mathbb{Z})$-модулем относительно операции трансляции. Определим *формальную сумму плиток* для системы плиток T как функцию вида

$$f = \sum_{i=1}^{n} \tau_{x_i,y_i} [\![t_i]\!].$$

Под *замощением* квадрата $n \times n$ будем понимать такой набор из n^2 плиток, что

$$f(e,c) = \left(\sum_{i=1}^{n^2} \tau_{x_i,y_i} [\![t_i]\!] \right)(e,c) = 0 \text{ для всех } e \in \mathcal{E},\ c \in C.$$

Напомним несколько результатов из [16].

Предложение 2 (формальное обобщение теоремы 4, [16])**.** *Каждая система плиток T с неразрешимой задачей поиска замощения, при котором формальная сумма плиток равна нулю (задача нулевого замощения), соответствует конечнопорождённому подполумодулю некоторого свободного $(\mathbb{Z}\times\mathbb{Z})$-модуля конечного ранга с неразрешимой задачей принадлежности.*

Доказательство. Рассмотрим абелеву группу $\mathcal{M}$ всех функций с конечным носителем, действующих из $\mathcal{E}\times C$ в $\mathbb{Z}$. Она является свободным $(\mathbb{Z} \times \mathbb{Z})$-модулем ранга $2|C|$ относительно действия трансляцией [16].

Тогда сумма плиток $f = \sum_{i=1}^{n} \tau_{x_i,y_i}[\![t_i]\!]$ является элементом подполумодуля N полумодуля M, порождённого плитками $\{[\![t]\!] \mid t \in T\}$. Задача нулевого замощения соответствует следующему вопросу: существует ли такой элемент $f \in N$, что $f + f_0 = 0$ для данного f_0? А это в точности задача принадлежности для обратного элемента $-f_0$. Таким образом, каждая система плиток T с неразрешимой задачей нулевого замощения соответствует подполумодулю $\mathcal{N}$ с неразрешимой задачей принадлежности. □

Используя Предложение 2, Лори и Стейнберг получили замощение, для которого задача нулевого замощения кодирует задачу остановки для детерминированной машины Тьюринга (см. также [3]). Следовательно, задача нулевого замощения очевидно неразрешима для такой системы плиток, для которой проблема останова неразрешима.

§3. Конструкции и результаты

Чтобы получить полную одностороннюю функцию, нам нужно модифицировать замощение, описанное в теореме 7 работы [16], так, чтобы оно стало детерминированным в следующем смысле: мы должны всегда иметь возможность достаточно быстро определить, какую плитку поместить в замощение следующей, и при этом никогда не попадать в тупик (если же мы всё же попадаем в тупик, то мы "признаём поражение" и выдаём ответ по умолчанию). Такая модификация замощения описана в следующей лемме; подробно эта конструкция рассматривается в разделе 4, где и доказывается лемма 1.

Лемма 1. *Для каждой детерминированной машины Тьюринга* $M = \langle Q, \Gamma, B, \Sigma, \pi, s, H\rangle$, *работающей не более* n^2 *шагов на входе длины* n, *существует такая система плиток* T_M *над множеством меток* C *и такое отображение* $f_C : \Gamma \to C$ *(расширенное покомпонентно до* $f_C : \Gamma^* \to C^*$*), что выполняются следующие утверждения.*

(1) *Для любого входа* $x \in \Gamma^*$ *задача нулевого замощения для множества плиток* T_M *с метками* $f_C(x)$ *на верхних рёбрах входа является детерминированной и может быть решена детерминированно за полиномиальное время.*

(2) *Правильное замощение квадрата* $n^2 \times n^2$ *с метками в верхнем ряду* $f_C(y)$ *существует тогда и только тогда, когда* $M(x)=y$.

По лемме 1, мы можем определить функцию, которая полиномиально симулирует процесс замощения (пока он происходит детерминированно, это гарантируется по лемме 1 для систем плиток, соответствующих машинам Тьюринга), и таким образом симулировать детерминированные машины Тьюринга, которые работают не более n^2 шагов.

А именно, для системы плиток T, множества цветов C и отображения $f_C : \Gamma \to C$ определим отношение $x \Rightarrow y$ ("y получается из x за один шаг") для $x, y \in \Gamma^*$, $|x| = |y| = m$, так: $x \Rightarrow y$, если существует детерминированная последовательность шагов замощения, которая преобразует замощение прямоугольника $k \times m$ с $f_C(x)$ на верхних рёбрах в замощение прямоугольника $(k+1) \times m$ с $f_C(y)$ на верхних рёбрах. Напомним, что под детерминированной последовательностью шагов замощения мы понимаем такую последовательность укладываний плиток, что для каждой новой плитки существует единственная возможность добавить её в замощение. Расширим $\Rightarrow$ до его транзитивного замыкания $\Rightarrow^*$ и частичного транзитивного замыкания $\Rightarrow_k^*$: $x \Rightarrow_k^* y$, если и только если существует последовательность $x = x_0 \Rightarrow x_1 \Rightarrow \ldots \Rightarrow x_l = y$ длины $l \leq k$. Теперь мы можем определить функцию суммы плиток и показать, что она полная односторонняя.

Определение 5. *Зафиксируем алфавит $\mathcal{A}$ и некоторое однозначное кодирование системы плиток и меток на плитках в виде строк в алфавите $\mathcal{A}^*$.* Функция суммы плиток $F_{\text{tile}} : \mathcal{A}^* \to \mathcal{A}^*$ *действует следующим образом: на входной строке $s \in \mathcal{A}^*$,*

- *если s кодирует $\langle T, x\rangle$ для некоторой системы плиток T и строки x, $|x| = n$, и $x' \Rightarrow_{n^2}^* y'$, где x' получается из x добавлением $(n^2 - n)$ символа "$\square$", F_{tile} выдаёт y, где y получается из y' удалением символов "$\square$" из конца строки;*
- *F_{tile} возвращает s во всех остальных случаях.*

Теорема 1. *Если односторонние функции существуют, то F_{tile} с равномерным распределением на входных строках является слабо односторонней функцией.*

Доказательство. Пусть g – сохраняющая длину односторонняя функция (т.е. такая односторонняя функция, что $|g(x)| = |x|$ для любого x), для которой существует машина Тьюринга M_g, вычисляющая g за не более чем n^2 шагов на длине входа n. По предложению 1, если односторонние функции существуют, то существует и такая g. По лемме 1,

существует система плиток T_{M_g}, которая симулирует работу машины Тьюринга M_g. Остаётся заметить, что с константной вероятностью вход для F_{tile} имеет вид $\langle T_{M_g}, x\rangle$ для некоторой входной строки x (точное значение вероятности зависит от конкретного вида кодирования в определении 5, но обычно она получается порядка $|\mathcal{A}|^{-l}$, где l –длина закодированного T_{M_g}). □

Более того, мы можем сейчас вернуться к подполумодулю свободного $(\mathbb{Z}\times\mathbb{Z})$-модуля и определить соответствующую полную одностороннюю функцию. Сумма плиток $f = \sum_{i=1}^{n} \tau_{x_i,y_i}[\![t_i]\!]$ может быть представлена как элемент подполумодуля M, порождённого $\{[\![t]\!] \mid t \in T\}$ (см. доказательство предложения 2). Укладыванию новой плитки t на место (x, y) соответствует добавление слагаемого $\tau_{x,y}[\![t]\!]$ в сумму.

В разделе 4 мы определим функцию $\varphi : N \to N$, результат применения которой соответствует добавлению корректного порождающего элемента (плитки) t в формальную сумму $f \in \mathcal{N}$:

$$\varphi : f \mapsto f + \tau_{x,y}[\![t]\!].$$

Следующая лемма также доказана в разделе 4.

Лемма 2. *Для любой детерминированной машины Тьюринга M с алфавитом Γ, останавливающейся за не более n^2 шагов, существует такой конечнопорождённый подполумодуль $\mathcal{N}$ и такая функция $g_C : \Gamma^* \to \mathcal{N}$, что*

$$\tau_{(0,m)}\varphi^{mn^2}(g_C(x)) = g_C(M^m(x)),$$

где $M^m(x)$ – состояние ленты M после m шагов работы машины M.

Теперь мы можем определить полиномиальную по времени функцию на абстрактных подполумодулях свободных $(\mathbb{Z}\times\mathbb{Z})$-модулей, которая симулирует, для подходящих входов, детерминированные машины Тьюринга. Функция получает на вход элемент подполумодуля M как линейную комбинацию его образующих (порождающих элементов), перечисляет все возможные корректные новые плитки (их полиномиальное число) и добавляет одну из найденных. Тогда, если этот процесс продолжается достаточно долго, результат замощения будет соответствовать результату работы машины Тьюринга. Снова мы определяем отношение $f \overset{\text{alg}}{\Rightarrow} f'$ (f' получается из f за один шаг), теперь для двух формальных сумм f и f': $f \overset{\text{alg}}{\Rightarrow} f'$, если $f' = \varphi(f)$.

Расширим $\overset{\text{alg}}{\Rightarrow}$ до транзитивного замыкания $\overset{\text{alg}}{\Rightarrow}^*$ и частичного транзитивного замыкания $\overset{\text{alg}}{\Rightarrow}_k^*$. Чтобы формально определить полную одностороннюю функцию, будем кодировать генераторы подполумодуля в некотором конечном алфавите.

Определение 6. *Зафиксируем алфавит* $\{0,1\}$ *и однозначное кодирование элементов* $\mathcal{M}$*, их формальных сумм и пар строк* $\{0,1\}^*$. Функция алгебраической суммы плиток $F_{\text{alg}} : \mathcal{A}^* \to \mathcal{A}^*$ *действует следующим образом: на входной строке* $s \in \mathcal{A}^*$*,*

- *если* s *кодирует* $\langle \mathcal{N}, x\rangle$ *для некоторого множества образующих* $\mathcal{N}=\{n_i\}$ *и строки* x*, и если* $f_x=\sum_{i=1}^n \tau_{x_i,y_i} n_i$ *и* $f_x \overset{alg}{\Rightarrow}^*_{n^4-n^2} f_y$ *для некоторой формальной суммы* f_y*, то* F_{alg} *возвращает* f_y*;*
- F_{alg} *возвращает* s *во всех остальных случаях.*

Теорема 2. *Если односторонние функции существуют, то* F_{alg} *с равномерным распределением на входных строках является слабой односторонней функцией.*

Доказательство. Доказательство в точности совпадает с доказательством теоремы 1, поскольку для любой машины Тьюринга M существует подполумодуль $\mathcal{N}$ полумодуля $\mathcal{M}$, который симулирует M посредством замощения. □

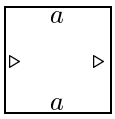
§4. Детерминированное замощение

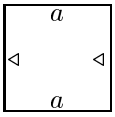
Этот раздел посвящён доказательству лемм 1 и 2. Рассмотрим детерминированную машину Тьюринга $M = (Q, \Gamma, \Sigma, \delta, q_0, q_f)$ и поставим ей в соответствие следующее множество цветов:

$$C = \Sigma \cup (Q \times \Sigma) \cup (Q \times \{L, R\}) \cup \{\rightarrow, \uparrow, \leftarrow, \downarrow, \swarrow, \triangleleft, \triangleright, c_0\}$$

Система плиток T_M будет состоять из плиток четырёх типов.

(1) Алфавитные плитки:

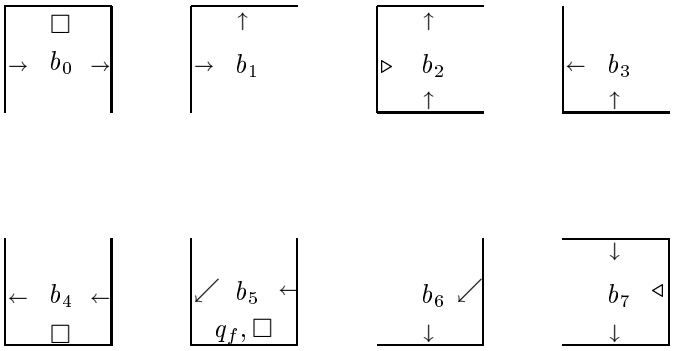




(2) Плитки слияния:

(3) Плитки действия (они соответствуют перемещению головки машины Тьюринга):

(4) Граничные плитки:



Предположим, что после очередного шага машина Тьюринга M находится в состоянии q_j, на ленте записано $y = y_1 y_2 y_3 \ldots y_k \square\square\square \ldots$, и головка находится в позиции l. Поставим этому состоянию в соответствие функцию $f_y^0 \in \mathcal{N}$ по следующему правилу:

$$\begin{aligned}
f_y^0(\{(0,0),\ (1,0)\},\ \downarrow) &= 1,\\
f_y^0(\{(i,1),\ (i+1,1)\},\ y_i) &= 1,\ 1 \leqslant i \leqslant l-1,\\
f_y^0(\{(0,0),\ (1,0)\},\ q_j y_l) &= 1,\\
f_y^0(\{(i,1),\ (i+1,1)\},\ y_i) &= 1,\ l+1 \leqslant i \leqslant k,\\
f_y^0(\{(k,1),\ (k+1,1)\},\ \rightarrow) &= 1,\\
f_y^0(e,\ c) &= 0,\ \text{в других случаях},
\end{aligned}$$

а затем рассмотрим $f_y \in \mathcal{N}$:

$$f_y = f_y^0 + \sum_{i=1}^{n^2-k-2} \tau_{x_i,0}[\![b_0]\!] + \tau_{n,0}[\![b_1]\!],$$

Пусть теперь $x = x_1x_2x_3\ldots x_k$ – вход машины M; рассмотрим следующую функцию $f_x \in N$:

$$f_x = f_x^0 + \sum_{i=1}^{n^2-k-2} \tau_{x_i,0}[\![b_0]\!] + \tau_{n,0}[\![b_1]\!],$$

Отображение $x \mapsto f_x$ даёт нам и f_C, и g_C: теперь $g_C : x \mapsto f_x$, а f_C отображает x в последовательность цветов на верхних рёбрах f_x.

Чтобы симулировать машину Тьюринга, нужно построить такую функцию $f \in \mathcal{N}$, что $\forall e \in \mathcal{E}, c \in C\ (f_x + f)(e,c) = 0$. Покажем, что процесс построения функции f детерминирован.

Представим каждый шаг машины M в виде n^2 укладываний плиток. Рассмотрим частичное замощение квадрата $n \times n$, которому соответствует функция

$$f = \sum_{i=1}^{k} \tau_{x_i,y_i}[\![t_i]\!].$$

Определим доступную на данный момент плитку. Назовём плитку t *доступной*, если для некоторого $(x,y) \in \mathbb{Z} \times \mathbb{Z}$:

$$\left(|\{e \in \mathcal{E} |\ (f + \tau_{x,y}[\![t]\!])(e,c) = 0\}| - \sum_{e\in\mathcal{E},\ c\in C} |(f + \tau_{x,y}[\![t]\!])(e,c)| \right) \to \max,$$

т.е. разница между числом сокращённых рёбер и числом новых окрашенных рёбер максимальна среди всех размещений всех плиток.

Однако этого пока недостаточно. Мы также должны прибегнуть к трюку, впервые использовавшемуся в [21], – заглядыванию на один шаг вперёд. Будем проверять каждую доступную плитку на *корректность*: доступная плитка t называется *корректной*, если после её добавления в частичное замощение существует доступная плитка, которая может быть её соседом, т.е. если существуют такая доступная плитка t_1, такое ребро $e \in \mathcal{E}$ и такой цвет $c \in C$, что

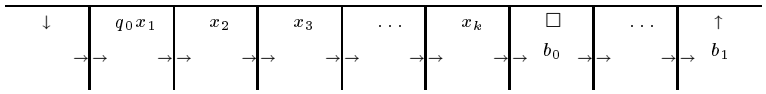
$$(\tau_{x,y}[\![t]\!])(e,c) \neq 0, \qquad (\tau_{x,y}[\![t]\!]) - \tau_{x_1,y_1}[\![t_1]\!])(e,c) = 0.$$

Теперь функция $\varphi : N \to N$ добавляет корректную допустимую плитку t к частичному замощению f:

$$\varphi : f \mapsto f + \tau_{x,y}[\![t]\!].$$

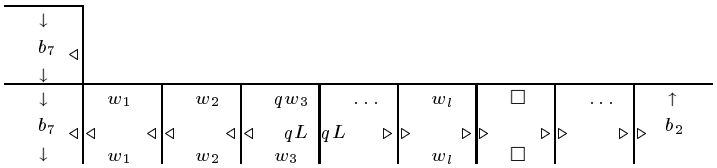
Заметим, что даже при правильной симуляции машины Тьюринга может возникнуть ситуация, в которой две или более корректных плитки можно разместить в одно и то же время в различных местах квадрата; в этом случае φ может выбрать один из корректных вариантов произвольно, скажем, выбрать из найденных мест размещения плитки крайнее нижнее левое.

Рассмотрим теперь вход x и соответствующую сумму плиток $f_C(x)$:



Предположим, что к текущему шагу мы замостили прямоугольник $m \times n^2$. Покажем, как происходит замощение следующей строки. Существуют две доступные плитки, b_2 и b_7; каждая из них сокращает одно ребро и добавляет два новых, а любая другая плитка сокращает не более одного ребра и добавляет три новых.

Обе плитки b_2 и b_7 являются корректными из-за наличия алфавитных плиток и плиток действия. Добавим одну из них, например $\tau_{0,m-1} b_7$, в сумму:



На данном шаге существует плитка $[\![t]\!]$, которая сокращает два ребра и добавляет два новых, т.е. множество доступных плиток непусто. Если среди доступных плиток есть корректная, то она единственна, потому что это либо алфавитная плитка с соответствующим символом алфавита на южном ребре и цветом "$\triangleleft$" на западном ребре:

$\downarrow$	w_1							
b_7 $\triangleleft$	$\triangleleft$ $\triangleleft$							
$\downarrow$	w_1							
$\downarrow$	w_1	w_2	qw_3	$\dots$	w_l	$\square$	$\dots$	$\uparrow$
b_7 $\triangleleft$	$\triangleleft$ $\triangleleft$	$\triangleleft$ $\triangleleft$	$\triangleleft$ qL	qL $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ b_2
$\downarrow$	w_1	w_2	w_3		w_l	$\square$		

либо плитка действия с южной границей вида "qa" (тоже единственная, так как мы симулируем работу детерминированной машины Тьюринга):

$\downarrow$	b							
b_7 $\triangleleft$	$\triangleleft$ q_jR							
$\downarrow$	q_iw_1							
$\downarrow$	q_iw_1	a	$\dots$	$\dots$	w_l	$\square$	$\dots$	$\uparrow$
b_7 $\triangleleft$	$\triangleleft$ q_iL	q_iL $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ b_2
$\downarrow$	w_1	q_jw_2	$\dots$	$\dots$	w_l	$\square$		

либо плитка слияния, корректность которой подтверждается соседней с ней (единственной) плиткой действия:

$\downarrow$	q_jw_1							
b_7 $\triangleleft$	$\triangleleft$ q_jL							
$\downarrow$	w_1							
$\downarrow$	w_1	q_iw_2	$\dots$	$\dots$	w_l	$\square$	$\dots$	$\uparrow$
b_7 $\triangleleft$	$\triangleleft$ $\triangleleft$	$\triangleleft$ q_iR	q_iR $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ $\triangleright$	$\triangleright$ b_2
$\downarrow$	w_1	w_2	$\dots$	$\dots$	w_l	$\square$		

Корректность одной из этих плиток исключает возможность корректности остальных. Если ни одна из доступных плиток не является корректной, то процесс замощения останавливается, и функция возвращает свой вход. Таким образом, за $(n^4 - n^2)$ шагов мы либо замостим квадрат $n^2 \times n^2$, либо остановим процесс замощения из-за отсутствия корректной доступной плитки; это завершает доказательство леммы 1.

Перейдём теперь к доказательству леммы 2; доказательство здесь точно такое же, нам нужно только убедиться, что всё, что мы делали выше, можно выразить на уровне подполумодуля $\mathcal{N}$, без явных конструкций плиток. Функция $g_C : \Gamma^* \to \mathcal{N}$ совпадает с f_C, но выдаёт на выходе формальную сумму образующих $\mathcal{N}$ (т.е. плиток), а не замощение. Единственное новое замечание здесь заключается в том, что даже если у нас нет доступа к самому замощению, мы всё равно можем за полиномиальное время понять, соответствует ли добавление новой образующей $\tau_{x,y}[\![t]\!]$ размещению корректной новой плитки на пустом месте замощения. Назовём образующую $\tau_{x,y}[\![t]\!]$ *формально корректной*, если для некоторого $1 \le i \le n$,

$$e \in \{\{(0,0),(1,0)\},\{(1,0),(1,1)\},\{(1,1),(0,1)\},\{(0,1),(0,0)\}\},$$

и некоторого $c \in C$

$$\tau_{x,y}[\![t]\!](e,c) = -\tau_{x_i,y_i}[\![t_i]\!](e,c),$$

где $[\![t_i]\!]$ – образующая (плитка), которая уже встречается в f, $\tau_{x_i,y_i}[\![t_i]\!](e,c) \neq 0$, и нет такого $j \neq i$, что $\tau_{x_j,y_j}[\![t_j]\!](e,c) = -\tau_{x_i,y_i}[\![t_i]\!](e,c)$ (т.е. новая плитка сокращает по крайней мере одно уже существующее ребро, которое ранее не было сокращено).

Однако этого пока недостаточно. Как мы уже видели, может быть одновременно много формально корректных образующих, и если начать с неверной образующей, можно потом не суметь вернуться обратно. Поэтому мы определяем *допустимую* образующую как образующую, для которой для некоторого $(x,y) \in \mathbb{Z} \times \mathbb{Z}$

$$\left(|\{e \in \mathcal{E} |\ (f + \tau_{x,y}[\![t]\!])(e,c) = 0\}| - \sum_{e \in \mathcal{E},\ c \in C} |(f + \tau_{x,y}[\![t]\!])(e,c)| \right) \to \max.$$

Иначе говоря, допустимая образующая сокращает наибольшее возможное число окрашенных рёбер. Допустимая образующая t называется *корректной*, если существует допустимая образующая, которая сокращает ребро t, т.е., допустимая образующая t_1, $e \in \mathcal{E}$, и цвет $c \in C$, для которых

$$(\tau_{x,y}[\![t]\!])(e,c) \neq 0, \qquad (\tau_{x,y}[\![t]\!]) - \tau_{x_1,y_1}[\![t_1]\!])(e,c) = 0.$$

Таким образом, мы доказали лемму 2.

§5. Заключение

В этой работе мы представили новую конструкцию комбинаторной полной (слабо) односторонней функции. Наша конструкция основана на алгебраических идеях; её можно сформулировать в терминах поиска обратного к элементу некоторого полумодуля (если он существует). К сожалению, эта конструкция, хоть она и основана на групповых конструкциях, всё же остаётся по существу *полу*групповой (полумодульной). Тем не менее, нам представляется, что это первый шаг на пути к более интересному результату: комбинаторной полной односторонней функции, основанной на группах, а не полугруппах.

Благодарности. Основная идея этой работы появилась во время поездки первого автора в Математический институт Стивенса, Хобокен, Нью-Джерси, США; автор искренне благодарен проф. Алексею Мясникову за гостеприимство и плодотворные обсуждения, в которых и родилась эта идея.

Литература

1. Sanjeev Arora and Boaz Barak, *Complexity Theory: A Modern Approach.* Cambridge University Press (2009).
2. Andrej Bogdanov and Luca Trevisan, *Average-case complexity.* — Foundations and Trends in Theoretical Computer Science, **2** (2006).
3. Egon Börger, Erich Grädel, and Yuri Gurevich, *The classical decision problem.* Springer-Verlag, Berlin (2001).
4. Stephen A. Cook, *The complexity of theorem-proving procedures.* In: Proceedings of the 3rd, Annual ACM Symposium on Theory of Computing, (1971), pp. 151–158.
5. Michael R. Garey and David S. Johnson, *Computers and Intractability*, A Guide to the Theory of NP-Completeness. W. H. Freeman, San Francisco, CA (1979).
6. Oded Goldreich, *Foundations of Cryptography. Basic Tools.* Cambridge University Press (2001).
7. Dima Grigoriev, Edward A. Hirsch, and Konstantin Pervyshev, *A complete public-key cryptosystem.* — Groups, Complexity, and Cryptology **1** (2009), 1–12.
8. Yuri Gurevich, *Average case completeness.* — J. Comput. System Sciences **42**, no. 3 (1991), 346–398.
9. D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, *On robust combiners for oblivious transfers and other primitives.* In: Proceedings of EuroCrypt 2005, Lecture Notes in Computer Science, vol. 3494, (2005), 96–113.
10. John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman, *Introduction to Automata Theory*, Languages and Computation. Addison-Wesley (2000).
11. John E. Hopcroft and Jeffrey D. Ullman, *Introduction to Automata Theory, Languages and Computation.* Addison-Wesley, Reading Mass (1979).

12. Richard M. Karp, *Reducibility among combinatorial problems.* In: Complexity of Computer Computations. New York, Plenum (1972).
13. Leonid A. Levin, *Average case complete problems.* — SIAM J. of Computing **15**, no. 1 (1986), 285–286.
14. Leonid A. Levin, *One-way functions and pseudorandom generators.* — Combinatorica **7**, no. 4 (1987), 357–363.
15. Leonid A. Levin, *The tale of one-way functions.* — Probl. Information Transmission **39**, no. 1 (2003), 92–103.
16. Markus Lohrey and Benjamin Steinberg, *Tilings and submonoids of metabelian groups.* — Theory of Computing Systems **48**, no. 2 (2011), 411–427.
17. Sergey I. Nikolenko, *Provably Secure Constructions in Cryptography.* Lamberts Academic Publishing (2011).
18. Christos Harilaos Papadimitriou, *Complexity Theory.* Addison Wesley (1994).
19. Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, Vol. A: Algorithms and Complexity. The MIT Press/Elsevier (1990).
20. Jie Wang, *Average-case intractible NP problems.* Advances in Languages, Algorithms, and Complexity, 313–378 (1998).
21. А. А. Кожевников, С. И. Николенко, *О полных односторонних функциях.* — Проблемы передачи информации **45**, no. 2 (2009), 101–118.
22. Л. А. Левин, *Универсальные переборные задачи.* — Проблемы передачи информации **9**, no. 3 (1973), 265–266.
23. Л. А. Левин, *Односторонние функции.* — Проблемы передачи информации, **39**, no. 1 (2003), 92–103.

Nikolenko S. I., Tugaryov D. S. A complete one-way function based on a free finite rank $\mathbb{Z} \times \mathbb{Z}$-module.

It is known that the subsemimodule membership problem for finite rank free $\mathbb{Z} \times \mathbb{Z}$-modules is undecidable. Modifying the undecidability construction, we present a complete one-way function based on finite rank free $\mathbb{Z} \times \mathbb{Z}$-modules.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
Фонтанка 27, 191023
Санкт-Петербург,
Академический Университет РАН
Россия
E-mail: sergey@logic.pdmi.ras.ru

Поступило 16 мая 2012 г.

Академический Университет РАН
Россия
E-mail: tugaryov@mail.ru