УДК 519.854

В.А. МИХАЙЛЮК

О ПОРОГЕ ОТНОШЕНИЯ АППРОКСИМАЦИИ ДЛЯ РЕОПТИМИЗАЦИИ ЗАДАЧИ О МАКСИМАЛЬНОМ КОЛИЧЕСТВЕ ВЫПОЛНЕННЫХ УРАВНЕНИЙ В ЛИНЕЙНЫХ СИСТЕМАХ НАД КОНЕЧНЫМ ПОЛЕМ

Ключевые слова: *C-приближенный алгоритм, реоптимизация, дискретный Фурье-анализ, PCP-теорема.*

Произвольную оптимизационную проблему P можно решить с помощью эффективного приближенного алгоритма. Однако многие оптимизационные проблемы являются NP-трудными и, следовательно, при $P \neq NP$ решить их точно за полиномиальное время вряд ли возможно. Поэтому для решения таких задач рассматриваются эффективные приближенные алгоритмы. Для максимизационной проблемы считается, что полиномиальный алгоритм есть C-приближенным алгоритмом, если он для произвольного экземпляра дает решение со значением целевой функции, не меньшим, чем OPT / C, где OPT — глобальный оптимум. При этом C называют отношением аппроксимации. Подобное определение можно сформулировать для минимизационных проблем.

Для проблемы P установлена верхняя оценка отношения аппроксимации C, если существует полиномиальный C-приближенный алгоритм для решения P. Для данной проблемы установлена нижняя оценка отношения аппроксимации c, если для произвольного $\varepsilon > 0$ не существует полиномиального приближенного алгоритма для P, на котором достигается отношение аппроксимации $c - \varepsilon$. Если $C = c$, то для проблемы P установлен порог отношения аппроксимации ($C = c$). Соответствующий алгоритм называют приближенным оптимальным (или пороговым) алгоритмом.

Проблема установления нижних оценок отношения аппроксимации является трудноразрешимой задачей. Для такой проблемы существует термин неаппроксимируемость (inapproximability) или трудность аппроксимации (hardness of approximation). Техника получения нижних оценок отношения аппроксимации для некоторой исследуемой проблемы состоит в построении полиномиальной сводимости некоторой NP-трудной проблемы к исследуемой проблеме с такими свойствами. Положительные экземпляры NP-трудной проблемы дают новые экземпляры со значением целевой функции, не меньшим c, а отрицательные экземпляры дают новые экземпляры со значением целевой функции, не большим s. Тогда можно утверждать, что аппроксимировать проблему с отношением, меньшим c / s, является NP-трудным. Этого можно достичь чисто комбинаторным путем, однако эффективно использование известной PCP-теоремы (Probabilistically Checkable Proof theorem) [1] и дискретного анализа Фурье для тестирования свойств проблем (property testing) [2, 3]. В настоящей работе используется метод получения нижних оценок аппроксимации для проблемы $Max - E3 - Lin - 2$ (о максимальном числе выполненных уравнений от трех переменных в линейных системах над полем $GF(2)$), исходя из PCP-теоремы, рассмотренной в работе [4].

Один из вариантов решения NP-трудных задач — использование предварительных знаний о подобных экземплярах проблем, если они доступны. Таких предварительных знаний нет, поскольку начальные данные для проблем рас-

сматриваются изолировано. Доступными они могут оказаться тогда, когда экземпляры проблем возникают как некоторые локальные модификации предыдущих экземпляров. Исходя из оптимального решения экземпляра проблемы (или близкого к нему), возникает вопрос, можно ли использовать эту информацию для нахождения оптимального (или близкого к нему) решения экземпляра проблемы, полученного в результате незначительных локальных модификаций первоначального экземпляра. Данный подход, названный реоптимизацией [6–12], в некоторых случаях позволяет получить приближенные решения лучшего качества в локально модифицированных экземплярах по сравнению с первоначальными. Например, при вставке или удалении элемента из множества задача о покрытии множествами реоптимизирована с отношением $(2-1/(\ln m+1))$, где m — число элементов множества [13]. Жадный алгоритм дает качество приближения $\ln m+1$. При любом $m>1$ имеем $2-\dfrac{1}{\ln m+1}<\ln m+1$, т.е. качество приближения лучше.

В данной работе для реоптимизации проблемы $Max-E3-Lin-2$ при вставке нового уравнения (проблема $Ins-Max-E3-Lin-2$) получен приближенный алгоритм с соотношением $\dfrac{3}{2}$ (для проблемы $Max-E3-Lin-2$ оптимальный приближенный алгоритм имеет отношение 2). Показано, что оценка отношения аппроксимации $\dfrac{3}{2}$ является пороговой. Подобный результат имеет место для $Ins-Max-Ek-Lin-2$ при $k=O(\log n)$.

1. ПОСТАНОВКА ЗАДАЧИ

Пусть задана система линейных уравнений над некоторым полем $\sum_{i=1}^{n} a_{ij}x_i=b_j$, $1\le j\le m$, и нужно найти значения x_i, которые удовлетворяют этой системе в определенном смысле. Если x_i удовлетворяют уравнению j системы, то будем считать, что уравнение j выполнено. Если требуется, чтобы все уравнения системы были выполнены, то, как известно, для этого необходим полиномиальный алгоритм — метод исключения Гаусса (если система совместна). Если система несовместна, т.е. выполнить все уравнения системы невозможно, возникают различные определения «наилучших решений». Если рассматривать систему над полем рациональных чисел, можно определить наилучшее решение — метод наименьших квадратов, т.е. минимизировать $\sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}x_j-b_j\right)^2$, и в этом случае можно найти наилучшее решение за полиномиальное время.

Если полем является конечное поле из двух элементов: 0 и 1 ($GF(2)$), и сложение выполняется по модулю 2, возможная мера — максимизировать число выполненных уравнений.

Пусть L — система линейных уравнений. Приписывая конкретному вектору $x=(x_1,\ldots,x_n)$ некоторые значения, получаем $N(L,x)$ — число выполненных уравнений с помощью x.

Определение 1. Пусть $Max-Lin-F$ — оптимизационная проблема отыскания для данной системы L уравнений над полем F такого x, который максимизирует $N(L,x)$. Если F — поле из p элементов, то проблему назовем $Max-Lin-p$.

Теорема 1 [5]. Для произвольного простого p $Max-Lin-p$ является NP-трудной проблемой, это справедливо и для $Max-Lin-Q$, где Q — поле рациональных чисел.

Определение 2. $Max-Ek-Lin-2$ есть проблема для данной системы L линейных уравнений (каждое из которых содержит ровно k переменных) — найти такое x, которое максимизирует $N(L,x)$.

Пример. Рассмотрим экземпляр (систему L) проблемы $Max-E3-Lin-2$ из шести уравнений для $n=9$ переменных (+ представляет сложение по mod 2):

$$\begin{cases} x_1+x_2+x_3=1, \\ x_4+x_5+x_6=1, \\ x_7+x_8+x_9=1, \\ x_1+x_4+x_7=0, \\ x_2+x_5+x_8=0, \\ x_3+x_6+x_9=0. \end{cases}$$

Приписывая значения $x_1=x_2=\ldots=x_6=1$, $x_7=x_8=x_9=0$, получаем, что выполнены все уравнения, кроме третьего. Поскольку все уравнения этой системы не могут быть выполненными, поскольку система несовместна (если сложить все левые части системы, получим 0, а если правые — 1), то в данном случае $N(L,x)=5$, и это значение для L оптимально.

Рассмотрим реоптимизационный вариант проблемы $Max-Ek-Lin-2$ $(k\geq 3)$, который состоит из системы L, имеющей m уравнений $E_1,\ldots,E_m$ $(L(E_1,\ldots,E_m))$, каждое содержит ровно k переменных из множества переменных $\{x_1,\ldots,x_n\}$, и пусть $x^*=(x_1^*,\ldots,x_n^*)$ — оптимальное решение.

Проблема *Ins* – *Max* – *Ek* – *Lin* – 2. Входные данные. К системе $L(E_1,\ldots,E_m)$ с оптимальным решением x^* добавляется уравнение E_{m+1} (содержит ровно k переменных из множества $\{x_1,\ldots,x_n\}$).

Результат. Найти оптимальное решение системы $L(E_1,\ldots,E_m,E_{m+1})$, используя x^*.

Цель. Найти x, которое максимизирует $N(L(E_1,\ldots,E_m,E_{m+1}),x)$.

Пусть P — некоторая оптимизационная проблема. Для экземпляра I проблемы $P(I\in P)$ размера N значение оптимального решения — $OPT(I)$. Пусть для приближенного полиномиального алгоритма $ALG(I)$ обозначает значение решения, которое находит алгоритм (или ожидаемое значение, если алгоритм случайный); $C>1$ — параметр, который может быть функцией от N.

Определение 3. Считается, что алгоритм достигает отношения аппроксимации C (C-приближенный алгоритм) в случае, когда для каждого экземпляра $I\in P$

$$ALG(I)\geq\frac{OPT(I)}{C},\ \text{если}\ P\ —\ \text{максимизационная проблема};$$
$$ALG(I)\leq C\cdot OPT(I),\ \text{если}\ P\ —\ \text{минимизационная проблема}.$$

2. НЕКОТОРЫЕ СВЕДЕНИЯ ИЗ ДИСКРЕТНОГО ФУРЬЕ-АНАЛИЗА БУЛЕВЫХ ФУНКЦИЙ

Все приведенные ниже сведения взяты из [15, 16]. Булевы функции будем рассматривать как отображения $f:\{0,1\}^n\to\{0,1\}$; если интерпретировать 0 и 1, как -1 и 1, то получим представление булевых функций $f:\{-1,1\}^n\to$ $\to\{-1,1\}$. Существует следующий способ представить f в виде полинома. Например, для $n=3$ рассмотрим функцию majority (большинство):

$$Maj_3(x)=Maj_3(x_1,x_2,x_3):Maj_3(1,1,1)=1,$$
$$Maj_3(1,1,-1)=1,\ldots,\ Maj_3(-1,-1,-1)=-1.$$

Для $x=(x_1, x_2, x_3)$ запишем

$$Maj_3(x)=\left(\frac{1+x_1}{2}\right)\left(\frac{1+x_2}{2}\right)\left(\frac{1+x_3}{2}\right)(+1)+$$
$$+\left(\frac{1+x_1}{2}\right)\left(\frac{1+x_2}{2}\right)\left(\frac{1-x_3}{2}\right)(+1)+\ldots+\left(\frac{1-x_1}{2}\right)\left(\frac{1-x_2}{2}\right)\left(\frac{1-x_3}{2}\right)(-1).$$

После умножения всех скобок и сведения подобных получаем

$$Maj_3(x)=\frac{1}{2}x_1+\frac{1}{2}x_2+\frac{1}{2}x_3-\frac{1}{2}x_1x_2x_3. \qquad (1)$$

Аналогичную процедуру можно выполнить для произвольной функции $f:\{-1,1\}^n\to R$ (R — множество действительных чисел), умножая соответствующий x-интерполятор на значение $f(x)$.

Утверждение 1. Произвольная функция $f:\{-1,1\}^n\to R$ единственным образом может быть представлена в виде полинома

$$f(x)=\sum_{S\subseteq[n]}c_S\prod_{i\in S}x_i, \qquad (2)$$

где $[n]=\{1,\ldots,n\}$.

Формула (2) называется формулой Фурье для f.

Традиционно коэффициенты c_S обозначаем $\hat{f}(S)$, а $\prod_{i\in S}x_i$ — как $\chi_S(x)$. Тогда (2) можем записать в виде

$$f(x)=\sum_{S\subseteq[n]}\hat{f}(S)\chi_S(x).$$

Рассмотрим пространство $G=\{g\mid g:\{-1,1\}\to R\}$. Определим в G скалярное произведение

$$\langle f,g\rangle=\frac{1}{2^n}\sum_{x\in\{-1,1\}^n}f(x)\cdot g(x).$$

Линейные функции $\chi_S(x)$ для различных подмножеств S формируют ортонормированный базис по отношению к введенному скалярному произведению. Очевидно, что для всех $S\subseteq[n]$ и произвольного $x\in\{-1,1\}^n$ имеем $\langle\chi_S,\chi_S\rangle=1$, $|\chi_S(x)|=1$. Тогда выполняются следующие свойства.

Утверждение 2. Имеем:

1) если $S\neq T$, то $\langle\chi_S,\chi_T\rangle=0$;

2) $\hat{f}(S)=\langle f,\chi_S\rangle=\frac{1}{2^n}\sum_{x\in\{-1,1\}^n}f(x)\cdot\chi_S(x)$.

Рассмотрим $x=(x_1,\ldots,x_n)$ как случайную строку, равномерно распределенную на $\{-1,1\}^n$. Такое случайное $x=(x_1,\ldots,x_n)$ будет генерироваться выбором каждого x_i независимо и равновероятно из $\{-1,1\}^n$. Математическое ожидание случайной булевой функции $f(x)$ относительно распределения x, обозначим $\underset{x}{E}[f(x)]$.

Теорема 2 (Парсеваля). Для произвольной $f:\{-1,1\}^n\to R$ имеем

$$\sum_{S\subseteq[n]}\hat{f}(S)^2=\underset{x}{E}[f(x)^2].$$

Утверждение 3. Имеем:

1) $\chi_S(x)\chi_T(x)=\chi_{S\Delta T}(x)$, где $S\Delta T$ — симметрическая разность S и T;

2) $\chi_S(xy) = \chi_S(x)\chi_S(y)$;

3) $\underset{x}{E}[\chi_U(x)] = \begin{cases} 0, & \text{если } U \neq \varnothing, \\ 1 & \text{иначе;} \end{cases}$

4) для произвольных $f : \{-1,1\}^n \to R$ и $S \subseteq [n]$ имеем $\hat{f}(S) = \underset{x}{E}[f(x)\chi_S(x)]$;

5) если $f : \{-1,1\}^n \to \{-1,1\}$, то $\sum\limits_{S \subseteq [n]} \hat{f}(S)^2 = 1$ (следствие из теоремы 2 — равенство Парсеваля).

Пусть $F_B = \{f \mid f : \{-1,1\}^n \to \{-1,1\}, \underset{x}{E}[f(x)] = 0\}$ — множество сбалансированных булевых функций, $DICT = \{f \mid f \in F_B \ \forall x \in \{-1,1\}^n, f(x) = x_{i_0}, i_0 \in [n]\}$ — класс диктаторских функций. Диктаторская функция зависит только от единственной координаты. Влияние i-й координаты функции f определим как

$$Infl_i(f) = \underset{x}{Pr}[f(x_1,\ldots,x_i,\ldots,x_n) \neq f(x_1,\ldots,-x_i,\ldots x_n)]$$

($\underset{x}{Pr}[\cdot]$ — вероятность относительно распределения x).

Для диктаторской функции $f(x) = x_{i_0}$ $Infl_{i_0}(f) = 1, Infl_i(f) = 0$ при $i \neq i_0$.

Утверждение 4. Справедливо равенство $\boldsymbol{Infl_i(f) = \sum\limits_{i \in S} \hat{f}(S)^2}$.

Определим влияние степени d как $Infl_i^d(f) = \sum\limits_{i \in S, |S| \leq d} \hat{f}(S)^2$ и класс функций, которые имеют «малые» влияния. Для целого d и параметра $\eta > 0$ положим

$$FFD_{d,\eta} = \{f \mid f \in F_B \ \forall i \in [n], \ Infl_i^d(f) \leq \eta\}.$$

Таким образом, $FFD_{d,\mu}$ — класс функций, которые «далеки» от диктаторских в том смысле, что все влияния степени d не больше, чем η.

Определение 4. Для данного $0 \leq \varepsilon \leq 1$ будем считать, что x, $y \in \{-1,1\}^n$ есть $(1-2\varepsilon)$-коррелированные случайные векторы, если x равномерно распределенный, а y генерируется с помощью x отрицанием каждого бита независимо с вероятностью ε.

Легко видеть, что $E[x_i y_i] = Pr[x_i = y_i] - Pr[x_i \neq y_i] = 1 - 2\varepsilon$, откуда следует название коррелируемых и случайных векторов.

3. PCP-ТЕОРЕМА И НЕАППРОКСИМИРУЕМОСТЬ

Используем результаты работы [16]. Пусть P — произвольная оптимизационная (для определенности — на максимум) проблема. Под (c,s)-*gap*-версией проблемы P ($GapP_{c,s}$) будем понимать проблему, для которой либо $OPT(I) \geq c$, либо $OPT(I) \leq s$ для произвольного экземпляра $I \in P$. Рассмотрим NP-полную проблему $3SAT$ (3-выполнимость). Произвольная $3SAT$-формула ($E3-CNF$-формула) — это конъюнкция множества скобок, где каждая скобка — дизъюнкция трех булевых переменных или их отрицаний. Нужно определить приписывания булевым переменным таких значений истинности, что формула становится логически истинной (выполнимой). Пусть CNF-формула φ с m скобками c-выполнима ($c \in [0,1]$) тогда и только тогда, когда некоторое приписывание выполняет cm скобок и никакое не выполняет больше cm скобок.

Допустим, что существует полиномиальная сводимость от $3SAT$ к $GapP_{c,s}$ для некоторых $0 < s < c$, т.е. сводимость, которая отображает $3SAT$-формулу ψ на экземпляр I проблемы P такой, что получаем два случая:

1) если ψ имеет приписывание, которое делает ее выполнимой, то $OPT(I) \geq c$ (утвердительный ответ);

2) если ψ не имеет приписываний, которые делают ее выполнимой, то $OPT(I) \leq s$ (отрицательный ответ).

Такая сводимость предполагает, что если существует полиномиальный алгоритм с отношением аппроксимации, строго меньшим c/s для проблемы P, то определить, выполнима ли $3SAT$-формула и, следовательно, $P = NP$. Таким образом, при стандартном предположении $P \neq NP$ эта сводимость — источник получения результатов по неаппроксимируемости для проблемы P.

На практике сводимость, описанная выше, есть последовательность сводимостей. Причем первая сводимость в этой последовательности — известная PSP-теорема, которая имеет множество формулировок (PSP — Probabilistic Checkable Proof (вероятностно проверяемые доказательства)). В данном случае она может быть сформулирована как сводимость от $3SAT$ к *gap*-версии $3SAT$. А именно, пусть для формулы ψ $OPT(\psi)$ обозначает максимальную часть скобок, которые могут быть выполнены в результате произвольного приписывания. Таким образом, $OPT(\psi) = 1$ тогда и только тогда, когда ψ выполнима. PCP-теорема утверждает, что существуют универсальная константа $\alpha < 1$ и полиномиальная сводимость, которая отображает экземпляр ψ $3SAT$ на другой $3SAT$ экземпляр φ, такой, что:

1) если $OPT(\psi) = 1$, то $OPT(\varphi) = 1$ (свойство полноты (completeness));

2) если $OPT(\psi) < 1$, то $OPT(\varphi) \leq \alpha$ (свойство корректности (soundness)).

Отсюда следует, что $Max-3SAT$ неаппроксимируема с отношением аппроксимации $\alpha^{-1} > 1$. Здесь PCP-теорема была представлена как комбинаторная сводимость. Существует эквивалентная формулировка в терминах проверки доказательств (proof checking). Теорема утверждает, что каждое *NP*-утверждение имеет полиномиальное доказательство, которое можно проверить полиномиальным вероятностным проверяющим V (verifier), считывающим только константное число битов в доказательстве. Проверяющий имеет свойства полноты и корректности: каждое доказательство корректного утверждения принимается с вероятностью 1 и каждое доказательство некорректного утверждения принимается с малой вероятностью (не большей 1 %). Это и есть два метода (комбинаторная сводимость и проверка доказательств) для установления неаппроксимируемости оптимизационных проблем (которые кратко рассмотрены ниже).

Приведем формальные определения [4] системы доказательств (proof systems) с помощью свойств проверяющего V. Для проверки утверждений ему нужны помощники; будем считать, что они имеют доступ к одному или нескольким оракулам. Во многих вариантах систем доказательств обсуждаются понятия доказывающих (proovers, пруверы) и записанных доказательств (written proofs), эквивалентных доказательствам, использующим оракулы, где считывание *i*-го бита соответствует вопросу к оракулу. Заметим, что пруверы более могущественны, чем оракулы, поскольку могут быть случайными и исторически зависимыми.

Определение 5. Оракул есть функция $\Sigma^* \to \{0,1\}$, представляющая множество конечных строк в алфавите Σ.

Типичный проверяющий $V^{\pi}(x, r)$ — это вероятностная машина Тьюринга, где π — оракул, x — ввод, r — внутренняя случайная лента. Считается, что проверяющий принимает решение, если он выводит единицу ($V^{\pi}(x, r) = 1$), иначе отвергает решение.

Определение 6. Пусть c и s — действительные числа такие, что $0 \le s < c \le 1$. Полиномиальная вероятностная машина Тьюринга V есть проверяющий в вероятностно-проверяемом доказательстве (PCP) с полнотой c и корректностью s для языка L тогда и только тогда, когда:

- для $x \in L$ существует оракул π такой, что $\Pr_r[V^{\pi}(x, r) = 1] \ge c$;
- для $x \notin L$ и всех π имеем $\Pr_r[V^{\pi}(x, r) = 1] \le s$.

Определение 7. Проверяющий V использует логарифмическую случайность, если существует абсолютная константа c такая, что для каждого входа x и доказательства π длина случайной строки r, которую использует V^{π}, оценивается сверху как $c \log |x|$.

Определение 8. Проверяющий V читает c бит в PCP, если для каждого результата случайных испытаний и каждого доказательства π V^{π} задает не больше c вопросов оракулу.

Теорема 3 (PCP-теорема) [4]. Существует универсальное целое c такое, что язык в NP имеет PCP проверяющего V с корректностью $1/2$ и полнотой 1, где V использует логарифмическую случайность и читает не больше c бит в доказательстве.

Теорема 4 (вариант PCP-теоремы) [4]. Пусть L — язык в NP и x — строка. Существует универсальная константа $c < 1$ такая, что за время, полиномиальное относительно $|x|$, можно сконструировать $E3-CNF$-формулу $\varphi_{x,L}$ такую, что если $x \in L$, то $\varphi_{x,L}$ выполнима; если $x \notin L$, то формула $\varphi_{x,L}$ не более чем c-выполнима. Кроме того, каждая переменная встречается ровно пять раз.

Опишем однораундовую интерактивную систему доказательств с двумя пруверами (two prover one-round proof system — 2P1R-система). Проверяющий в такой системе имеет доступ к двум оракулам и может задать один вопрос каждому из них (два вопроса формулируются до того момента, когда на них отвечают).

Размер ответов оракулов не ограничивается, но поскольку проверяющий работает в полиномиальное время, он не может прочитать больше, чем полиномиальное число битов. Пусть P_1, P_2 — два оракула и q_1, q_2 — два вопроса. Оракулы имеют доступ только к этим вопросам, и если V принимает, то $V(x, r, P_1(q_1), P_2(q_2)) = 1$.

Определение 9. Пусть c, s — действительные числа, $0 \le s < c \le 1$. Полиномиальная вероятностная машина Тьюринга V с двумя оракулами есть проверяющий в 2P1R-системе с полнотой c и корректностью s для языка L, если на входе x она формирует (без согласия со своими оракулами) две строки (q_1, q_2) такие, что:

- для $x \in L$ существуют таких два оракула: P_1, P_2, для которых $\Pr_r[V(x, r, P_1(q_1), P_2(q_2)) = 1] \ge c$;
- для $x \notin L$ и для любых оракулов P_1, P_2 имеем $\Pr_r[V(x, r, P_1(q_1), P_2(q_2)) = 1] \le s$.

В обоих случаях q_1, q_2 — вопросы, которые V задает оракулам, $P_1(q_1)$ зависит от x, но не зависит от q_2, это же имеет место и для $P_2(q_2)$.

Используя однораундовый протокол с корректностью s, согласно определению 9 можно повторить его последовательно дважды, тогда корректность улучшится (уменьшится) до s^2. Применяя протокол последовательно u раз, получаем корректность s^u. Это даст многораундовый протокол. Чтобы оставить его однораундовым, применим технику параллельных повторов. Проверяющий V повто-

ряет свои случайные выборы u раз для получения u независимых пар вопросов $(q_1^{(i)}, q_2^{(i)})_{i=1}^u$ и посылает вопрос $(q_1^{(i)})_{i=1}^u$ к P_1, а вопрос $(q_2^{(i)})_{i=1}^u$ — к P_2.

Затем V получает u ответов от каждого прувера и принимает их так, как будто он работет в однораундовой системе u раз. Корректность такого протокола может быть больше s^u, однако Рац (Raz [17]) доказал, что при малом размере ответа корректность экспоненциально уменьшается относительно u.

Теорема 5 [17]. Для всех целых d и $s<1$ существует $c_{d,s}<1$ такая, что для данной 2P1R-системы с корректностью s и размерами ответов, не большими d, для всех целых u корректность u протоколов, работающих параллельно, не больше $c_{d,s}^u$.

Определение 10. Пусть $2\mathrm{P1}R_{c,s}(r(n))$ — класс языков L, для которых существует 2P1R-система с проверяющим V, которому доступно случайное число $r(n)$ бит.

Теорема 6 [18]. Существует константа $\varepsilon_P > 0$ такая, что $NP = 2\mathrm{P1}R_{1,1-\varepsilon_P}(\log n)$.

4. О ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ РЕОПТИМИЗАЦИИ ЗАДАЧИ

Рассмотрим вопрос установления *NP*-трудности реоптимизации дискретных задач оптимизации. Используя результаты работы [14] (в частности, теорему 2 [14]), предложим такой критерий установления *NP*-трудности реоптимизации, суть которого для большинства *NP*-трудных проблем заключается в использовании полиномиальной сводимости Тьюринга [19] исходной задачи к ее реоптимизационному варианту.

Лемма 1. Пусть P — *NP*-трудная проблема и *mod-P* — некоторая локальная модификация для P. Если существует полиномиальный алгоритм A, который для произвольного экземпляра I проблемы P вычисляет экземпляр I' для P (условие 1), оптимальное решение x' для I' (условие 2), последовательность локальных модификаций типа *mod* (не более, чем полиномиальную), которая преобразует I' в I (условие 3), то проблема *mod-P* является *NP*-трудной.

Доказательство. Сведем P к *mod-P*, используя полиномиальную сводимость Тьюринга. Поскольку проблема P является *NP*-трудной, то таковой (т.е. *NP*-трудной) будет и *mod-P* [19].

Пусть q — число локальных модификаций типа *mod* для A, которые экземпляр I' преобразуют в I. Допустим, что существует полиномиальный алгоритм A_1 (со сложностью p) для *mod-P*. Тогда, применяя A_1 точно q раз, начиная с I', получаем оптимальное решение для I. При этом как число вычислений (q), так и время каждого вычисления (p) полиномиальны относительно размера P, получена полиномиальная сводимость (со сложностью $q \cdot p$).

Лемма доказана.

Теорема 7. Проблема $Ins-Max-Ek-Lin-2$ является *NP*-трудной.

Доказательство. Используем лемму 1. В качестве P возьмем *NP*-трудную проблему $Max-Ek-Lin-2$ (теорема 1), а в качестве *mod-P* — проблему $Ins-Max-Ek-Lin-2$. Пусть I — произвольный экземпляр проблемы $Max-Ek-Lin-2$ (ему соответствует система L, состоящая из m линейных уравнений). Пусть $x_{i_1}+x_{i_2}+\ldots+x_{i_k}=b$ — одно из этих уравнений (его берем в качестве I'). Построим за полиномиальное время такое приписывание значений истинности вектору $x=(x_1,\ldots,x_n)$, которое делает это уравнение выполнимым. Припишем множеству $\{x_1,\ldots,x_n\}$ произвольные значения истинности. Если при этом $\{x_{i_1}, x_{i_2},\ldots, x_{i_k}\}$ удовлетворяют экземпляру I', построение выполнено, иначе произвольное значение x_{i_l} ($l\in[k]$) меняем на противоположное, в результате экземпляр I' будет выполнен за полиномиальное время, т.е. первые два условия

леммы 1 выполнены. Поскольку I' можно преобразовать в I не более чем m модификациями *mod-P* (т.е. добавить не больше m уравнений), то условие 3 леммы 1 также выполнено.

Теорема доказана.

5. ВЕРХНЯЯ ОЦЕНКА ОТНОШЕНИЯ АППРОКСИМАЦИИ

Воспользуемся некоторыми сведениями из [4]. Пусть k — целое, а P — это предикат $\{-1,1\}^k \to \{-1,1\}$. Определим проблему выполнения с ограничениями $CSP-P$ (constraint satisfaction problem). Экземпляр этой проблемы — множество $(C_i)_{i=1}^m$ k-последовательностей литералов. При некотором приписывании значений переменных k-последовательность выполнима в P, если при применении к ней P дает значение -1 (истина). Для экземпляра I и последовательности $x=(x_1,\ldots,x_k)$ обозначим $N(I,x,P)$ число ограничений I, выполненных с помощью x для предиката P.

Определение 11. $Max-CSP-P$ есть проблема для данного экземпляра I: найти x, которое максимизирует $N(I,x,P)$.

Легко видеть, что $Max-Ek-Lin$ — частный случай $Max-CSP-P$.

Определение 12. Вес $w(P,k)$ *CSP*-проблемы с данным предикатом P от k булевых переменных определяется как $p2^{-k}$, где p — число значений в $\{-1,1\}^k$, которые выполняют P.

Легко видеть, что для $Max-Ek-Lin-2$ вес равен $1/2$ при всех k, а для $Max-Ek-SAT$ с отношением $w(P,x)=1-2^{-k}$.

Теорема 8 [4]. Для проблемы $Max-CSP-P$ существует полиномиальный приближенный алгоритм с отношением аппроксимации $w(P,k)^{-1}$.

Теорема 9. Для проблемы $Max-Ek-Lin-2$ существует полиномиальный приближенный алгоритм с отношением аппроксимации 2.

Доказательство следует из теоремы 8 ($w(P,k)=1/2$ для задачи $Max-Ek-Lin-2$). Поскольку данный алгоритм является вероятностным, его нужно дерандомизировать с помощью известного метода условных вероятностей [18].

Теорема 10. Для проблемы $Ins-Max-Ek-Lin-2$ (реоптимизация $Max-Ek-Lin-2$) существует полиномиальный приближенный алгоритм с отношением аппроксимации $3/2$, если $k=O(\log n)$.

Доказательство. Применим подход, рассмотренный в [13]. Пусть I — экземпляр проблемы $Max-Ek-Lin-2$, который состоит из системы $L(E_1,\ldots,E_m)$ и оптимального решения x^*; $c(x^*)$ — число выполненных уравнений в системе $L(E_1,\ldots,E_m)$ решением x^*. К системе добавляется уравнения E_{m+1}, в результате получаем экземпляр I' проблемы $Ins-Max-Ek-Lin-2$; пусть $x^*_{I'}$ — его оптимальное решение. Если $x^*_{I'}$ не выполняет уравнения E_{m+1}, то x^* — оптимальное решение экземпляра I' проблемы $Ins-Max-Ek-Lin-2$, отсюда

$$c(x^*) \geq c(x^*_{I'})-1 \tag{3}$$

(в левой части записано условие, что x^* — оптимальное решение I', а в правой — что оптимальное решение не выполняет уравнения E_{m+1}). Пусть $x^*_{I'}$ выполняет уравнение E_{m+1}. Существует 2^{k-1} приписываний переменным, которые выполняют уравнение E_{m+1}. Построим 2^{k-1} приближенных решений

x^i ($i \in [2^{k-1}]$) следующим образом. Берем i-е приписывание, которое выполняет уравнение E_{m+1}. Из системы удаляем E_{m+1} и к оставшимся уравнениям (учитывая результат приписывания) применяем некоторый полиномиальный ρ-приближенный алгоритм, в результате имеем приближенное решение x^i:

$$c(x^i) \ge \frac{1}{\rho}(c(x^*_{I'}) - 1) + 1 = \frac{1}{\rho} c(x^*_{I'}) + 1 - \frac{1}{\rho}. \tag{4}$$

Умножая (3) на $1 - \frac{1}{\rho}$ и складывая с (4), получаем

$$\left(1 - \frac{1}{\rho}\right) c(x^*) + c(x^i) \ge \left(1 - \frac{1}{\rho}\right) c(x^*_{I'}) - \left(1 - \frac{1}{\rho}\right) + \frac{1}{\rho} c(x^*_{I'}) + 1 - \frac{1}{\rho} = c(x^*_{I'}).$$

Из решений x^* и x^i выбираем наилучшее (т.е. с наибольшим значением целевой функции c) и обозначаем $\bar{x}$. Имеем

$$c(x^*_{I'}) \le \left(1 - \frac{1}{\rho} + 1\right) \max\{c(x^*), c(x^i)\} = \left(2 - \frac{1}{\rho}\right) c(\bar{x}),$$

откуда $c(\bar{x}) \ge \left(2 - \frac{1}{\rho}\right)^{-1} c(x^*_{I'})$. Для того чтобы описанный алгоритм был полиномиальным, достаточно потребовать, чтобы $2^{k-1} \le n^c$ (n — общее число переменных, $c = \text{const}$), откуда следует $k = O(\log n)$ (см. условие теоремы 10). Таким образом, в результате выполнения описанного алгоритма получено приближенное решение $\bar{x}$ экземпляра I' с отношением аппроксимации $2 - 1/\rho$. Ясно, что всегда $2 - 1/\rho < \rho$ ($\rho \ne 1$). Положим $\rho = 2$, т.е., применив приближенный алгоритм из теоремы 9, получим утверждение данной теоремы.

6. НИЖНЯЯ ОЦЕНКА ОТНОШЕНИЯ АППРОКСИМАЦИИ

Линейная функция, которая соответствует подмножеству $S \subset [n]$, определяется как $L_S(x) = \sum_{i \in S} x_i$ (суммирование по модулю 2).

Определение 13. Функция $f : \{0,1\}^n \to \{0,1\}$ линейна, если

$$\forall x, y \in \{0,1\}^n : f(x + y) = f(x) + f(y). \tag{5}$$

Наоборот, функция f линейна, если она равна L_S для некоторого $S \subset [n]$.

Равенство (5) берем в качестве теста для определения на линейность функции $f(x)$:

1) $x, y \in \{0,1\}^n$ выбираются равновероятно и независимо;

2) если $f(x + y) = f(x) + f(y)$, то тест принимается, иначе отвергается.

Введем новые обозначения для булевых значений. Рассмотрим преобразование для $a \in \{0,1\} : a \to (-1)^a$, которое отображает 0 в 1, а 1 — в -1. При этом суммирование по mod 2 преобразуется в умножение $a + b \to (-1)^{a+b} = (-1)^a (-1)^b$. Для функции $f : \{-1,1\}^n \to \{-1,1\}$ будем иметь новую форму линейных функций, связанную с подмножествами $S \subset [n] : \chi_S(x) = \prod_{i \in S} x_i$.

Теперь новый линейный тест проверяет $f(x \cdot y) = f(x) \cdot f(y)$ для случайных $x, y \in \{-1,1\}^n$, где $x \cdot y$ — покоординатное умножение, т.е. $(x \cdot y)_i = x_i \cdot y_i$. Выражение $f(x) f(y) f(xy)$ равно 1, если тест принимается (поскольку $f(x) f(y) f(xy) = f(x) f(y) f(x) f(y) = f^2(x) f^2(y) = 1$), и равно -1, если тест от-

вергается. В таком случае величина $\frac{1-f(x)f(y)f(xy)}{2}$ — индикатор того, что тест принимается. Отсюда следует

$$Pr[\text{тест отвергается}] = \underset{x,y\in\{-1,1\}^n}{E}\left[\frac{1-f(x)f(y)f(xy)}{2}\right]. \qquad (6)$$

Теорема 11 [16] (неформальный подход). Предположим, что P — максимизационная проблема и $Val: F_B \to R^+$ — оценка (valuation) на множестве сбалансированных булевых функций. Пусть существуют константы $0< s< c$ такие, что:

1) $\forall f \in DICT \quad Val(f) \geq c$ (свойство полноты);

2) $\forall f \in FFD_{d,\eta} \quad Val(f) \leq s$ (свойство корректности).

Будем считать, что выполняется некоторая теоретическая гипотеза теории сложности вычислений. Тогда для данного экземпляра проблемы P, который имеет решение со значением, не меньшим c, не существует полиномиального алгоритма, который находит решение со значением, не большим s. В частности, не существует полиномиального алгоритма для проблемы P с отношением аппроксимации, строго меньшим c/s.

Теорема сформулирована неформально и требует некоторых комментариев:

1) выбор оценки $Val(\cdot)$ существенно зависит от проблемы P, и различные проблемы приводят к различным интересным оценкам;

2) заслуживает внимания предельный случай, когда $d \to \infty$, $\eta \to 0$; часто получается $s = s' + \delta$, где s' — специальная константа и $\delta \to 0$, как только $d \to \infty$, $\eta \to 0$.

3) теоретическая гипотеза теории сложности вычислений должна быть в идеале $P \neq NP$, но часто она имеет и другой вид;

4) аналогичная теорема справедлива для минимизационных проблем.

Фурье-анализ булевых функций — надежное средство конструирования трудных экземпляров для приближенных алгоритмов и для доказательства NP-трудности аппроксимации. Эти трудные экземпляры формируются с помощью системы тестов.

Определение 14 [15]. «Диктаторский против малых влияний тест» с q вопросами, использующий предикат $\theta: \{-1,1\}^q \to \{pass, fail\}$, состоит из случайной процедуры для выбора строк $x_1, \ldots, x_q \in \{-1,1\}^n$. Тест принимает функцию $f: \{-1,1\}^n \to \{-1,1\}$ с вероятностью $\underset{x_1,\ldots,x_q}{Pr}[\theta(f(x_1),\ldots,f(x_q)) = pass]$. Считается, что тест имеет полноту c, если n диктаторских функций проходят этот тест с вероятностью, не меньшей c; корректность s, если все функции, имеющие $o(1)$ — малые влияния ($o(1)$ относительно n), проходят тест с вероятностью не большей $s + o(1)$. Считается, что тест есть «c против s, диктаторский против малых влияний тест».

Рассмотрим проблемы $Max-E3-Lin-2$ и $Ins-Max-E3-Lin-2$. Пусть $I \in Max-E3-Lin-2$ и $I' \in Ins-Max-E3-Lin-2$. Переход от I к I' соответствует замене в «c против s, диктаторских против малых влияний тестах» числа вопросов q на $q+1$.

Линейный тест с возмущениями. Генерируем случайно две равномерно распределенные и независимые входные строки: x, $y \in \{-1,1\}^n$, и записывем $w = xy$. Определим z выбором каждого бита w независимо с вероятностью ε с последующим его отрицанием. Заметим, что корреляция каждого бита z по отношению к w есть $(1-2\varepsilon)$ (определение 4), т.е. $z \approx_{1-2\varepsilon} w$. Определим $Val(f) =$

$= \underset{x,y,z\approx_{1-2\varepsilon}w}{Pr}[f(z)=f(x)f(y)]$ для оптимизационной проблемы $Ins-Max-E3-$ $-Lin-2$, оценка линейно зависит от значений f на трех случайных (но коррелированных) входах.

Лемма 2 (свойство полноты). Если $f \in DICT$, то $Val(f)=1-\varepsilon$.

Доказательство. Для некоторой фиксированной координаты $i_0 \in [n]$ имеем $f(x)=x_{i_0}, f(y)=y_{i_0}, f(z)=z_{i_0}$ и $z_{i_0} \neq x_{i_0} y_{i_0}$ с вероятностью ε; значит, $f(z)=$ $=f(x)f(y)$ с вероятностью $1-\varepsilon$.

Лемма 3 (свойство корректности). Если $f \in FFD_{d,\eta}$, то $Val(f) \le \frac{2}{3}+\delta$.

Доказательство. В данном случае ключевое свойство состоит в том, что вероятность принятия теста можно записать в терминах коэффициентов Фурье булевой функции f. Пусть $\mu \in \{-1,1\}^n$ — случайный вектор, координаты которого принимают независимо значение 1 с вероятностью $1-\varepsilon$ и значение -1 в противном случае. Тест принимается тогда и только тогда, когда $f(x)f(y)f(\mu xy)=1$. Согласно (6) получим

$$Pr[\text{тест отвергается}] = \underset{x,y,\mu\in\{-1,1\}^n}{E}\left[\frac{1-f(x)f(y)f(\mu xy)}{2}\right],$$

отсюда

$$Pr[\text{тест принимается}] =$$

$$=1-\underset{x,y,\mu}{E}\left[\frac{1-f(x)f(y)f(\mu xy)}{2}\right]=\frac{1}{2}+\frac{1}{2}\underset{x,y,\mu}{E}[f(x)f(y)f(\mu xy)]. \qquad (7)$$

Вычислив $\underset{x,y,\mu}{E}[f(x)f(y)f(\mu xy)]$, получим

$$\underset{x,y,\mu}{E}[f(x)f(y)f(\mu xy)]=$$

$$=\underset{x,y,\mu}{E}\left[\left(\sum_S \hat{f}(S)\chi_S(x)\right)\left(\sum_T \hat{f}(T)\chi_T(x)\right)\left(\sum_U \hat{f}(U)\chi_U(\mu xy)\right)\right]=$$

$$=\underset{x,y,\mu}{E}\left[\sum_{S,T,U}(\hat{f}(S)\hat{f}(T)\hat{f}(U)\chi_S(x)\chi_T(y)\chi_U(\mu xy)\right]=$$

$$=\sum_{S,T,U}\hat{f}(S)\hat{f}(T)\hat{f}(U)\underset{x,y,\mu}{E}[\chi_S(x)\chi_T(y)\chi_U(\mu xy)].$$

Найдем

$$\underset{x,y,\mu}{E}[\chi_S(x)\chi_T(y)\chi_U(\mu xy)]=\underset{x,y,\mu}{E}[\chi_S(x)\chi_T(y)\chi_U(\mu)\chi_U(x)\chi_U(y)]=$$

$$=\underset{x,y,\mu}{E}[\chi_{S\Delta U}(x)\chi_{T\Delta U}(y)\chi_U(\mu)]=\underset{x,y,\mu}{E}\left[\left(\prod_{i\in S\Delta U}x_i\right)\left(\prod_{j\in T\Delta U}y_j\right)\left(\prod_{k\in U}\mu_k\right)\right]=$$

$$=\underset{x}{E}\left[\prod_{i\in S\Delta U}x_i\right]\underset{y}{E}\left[\prod_{j\in T\Delta U}y_j\right]\underset{\mu}{E}\left[\prod_{k\in U}\mu_k\right].$$

Если $S\neq U$ либо $T\neq U$, то одна из симметрических разностей непуста и одно из математических ожиданий $\underset{x}{E}\left[\prod_{i\in S\Delta U}x_i\right], \underset{y}{E}\left[\prod_{j\in T\Delta U}y_j\right]$ равно нулю. Поэтому должно быть $S=T=U$. Вычислим $\underset{\mu}{E}\left[\prod_{k\in U}\mu_k\right]=\prod_{k\in S}(E\mu_k)=\prod_{k\in S}(1-2\varepsilon)=(1-2\varepsilon)^{|S|}$, по-

скольку $E\mu_k = 1-\varepsilon-\varepsilon = 1-2\varepsilon$ (везде использовалась независимость x, y, μ и утверждение 3). В результате получим $\underset{x,y,\mu}{E}[f(x)f(y)f(\mu xy)] = \sum_S \hat{f}(S)^3(1-2\varepsilon)^{|S|}$.

Таким образом,

$$Val(f) = Pr[\text{тест принимается}] = \frac{1}{2} + \frac{1}{2}\sum_S \hat{f}(S)^3(1-2\varepsilon)^{|S|},$$

$$Val(f) \le \frac{1}{2} + \frac{1}{2}\max_S\{\hat{f}(S)(1-2\varepsilon)^{|S|}\}\sum_S \hat{f}(S)^2 = \frac{1}{2} + \frac{1}{2}\max_S\{\hat{f}(S)(1-2\varepsilon)^{|S|}\}$$

(согласно равенству Парсеваля).

В силу равенства Парсеваля и того факта, что функция сбалансирована, $\hat{f}(\varnothing) = 0$. Покажем, что для любого $S \neq \varnothing$ имеем $|\hat{f}(S)(1-2\varepsilon)^{|S|}| \le \delta$. Поскольку влияние степени d каждой координаты не больше η, для любого множества должно быть $S \neq \varnothing$ либо $|S| > d$, либо $\hat{f}(S)^2 \le \eta$, иначе любая координата в S имела бы влияние степени d не меньше η. Таким образом, положив $\delta = \max\{(1-2\varepsilon)^d, \sqrt{\eta}\}$, получим $Val(f) \le \frac{1}{2} + \frac{1}{2}\delta \le \frac{2}{3} + \delta$.

Лемма доказана.

Теорема 12. Пусть $P \neq NP$; $\varepsilon, \delta > 0$ — произвольные малые константы. Для данного экземпляра проблемы $Ins-Max-E3-Lin-2$, который имеет решение не меньше, чем с $(1-\varepsilon)$ частью выполненных уравнений, никакой полиномиальный алгоритм не сможет найти решение x не более чем с $(2/3+\delta)$ частью выполненных уравнений. Заметим, что не существует полиномиального алгоритма для $Ins-Max-E3-Lin-2$ с отношением аппроксимации, строго меньшим $3/2$.

Доказательство следует из применения лемм 2 и 3 к теореме 11.

Замечание. Согласно определению 14 линейный тест с возмущениями NP-трудный «$1-\varepsilon$ против $2/3+\delta$, диктаторский против малых влияний тест» для проблемы $Ins-Max-E3-Lin-2$.

Из теорем 10, 12 можно заключить, что $3/2$ — порог отношения аппроксимации для проблемы $Ins-Max-E3-Lin-2$.

Используя результатами работы [4], схематически рассмотрим второй способ доказательства теоремы 12, применяя технику систем доказательств (где явно продемонстрирована сводимость к экземплярам проблемы $Ins-Max-E3-Lin-2$).

Центральным понятием для Фурье-анализа булевых функций есть так называемый длинный код (long code). Пусть $U \subseteq [n]$, $U \subseteq W$, для $x \in \{-1,1\}^{|W|}$ обозначим $x_{/U}$ ограничение для переменных, которые встречаются в U. Пусть F_U — множество функций $f : \{-1,1\}^{|U|} \to \{-1,1\}$. Центральным вопросом есть изучение функций $A : F_U \to \{-1,1\}$, воспринимаемых как множество всех булевых функций от $u = |U|$ переменных (составляет всего 2^{2^u} функций).

Определение 15. Длинный код приписывания $x \in \{-1,1\}^n$ есть отображение $A_x : F_U \to \{-1,1\}$ такое, что $A_x(f) = f(x)$ для всех $f \in F_U$.

Если отождествить булеву функцию с ее таблицей истинности, то длинный код — это строка длиной 2^{2^u}.

Определение 16. Для функции $A : F_U \to \{-1,1\}$ определим функцию A_{true}, которая для каждой пары $(f, -f)$ выбирает одну из двух функций. Если выбирается f, то $A_{true}(f) = A(f)$ и $A_{true}(-f) = -A(f)$, если выбирается $-f$, то $A_{true}(f) = -A(-f)$ и $A_{true}(-f) = A(-f)$.

Отсюда следует, что всегда $A_{true}(f) = -A_{true}(-f)$.

Определение 17. Для функций $A : F_U \to \{-1, 1\}$ и $h \in F_U$ определим функцию $A_h : F_U \to \{-1, 1\}$, положив $A_h(f) = A(f \wedge h)$ для каждой f.

Ниже исследуем несколько PCP-систем на основе Фурье-анализа функций A.

Начнем с 3 *CNF*-формулы φ, полученной в результате применения теоремы 4 к произвольному языку L из *NP*. Таким образом, либо φ выполнима, либо не более чем c-выполнима для некоторой $c < 1$, и отличить эти два случая представляется *NP*-трудным. При этом каждая скобка в φ имеет длину ровно 3 переменных и каждая переменная участвует ровно в пяти скобках.

Базовая 2P1R-система

Ввод. $3-CNF$-формула $\varphi = C_1 \wedge C_2 \wedge \ldots \wedge C_m$, где C_j содержит переменные $x_{a_j}, x_{b_j}, x_{c_j}$.

Проверяющий. 1. Случайно и равновероятно выбирает $j \in [m]$ и $k \in \{a_j, b_j, c_j\}$, j посылается к P_1, а k посылается к P_2.

2. Получает значения для $x_{a_j}, x_{b_j}, x_{c_j}$ от P_1 и для x_k от P_2. Принимает значения тогда и только тогда, когда они для x_k согласованы и C_j выполнима.

Лемма 4 [4]. Если φ c-выполнима для произвольных P_1 и P_2, то V принимает значения в базовой 2P1R-системе с вероятностью, не большей $(2 + c)/3$.

Основная *u*-параллельная 2P1R-система

Ввод. $3-CNF$-формула $\varphi = C_1 \wedge C_2 \wedge \ldots \wedge C_m$, где C_j содержит переменные $x_{a_j}, x_{b_j}, x_{c_j}$.

Проверяющий . 1. Для $i = 1, 2, \ldots, u$ выбирает случайно, равновероятно и независимо $j_i \in [m]$ и $k_i \in \{a_{j_i}, b_{j_i}, c_{j_i}\}$, посылает $(j_i)_{i=1}^n$ к P_1, а $(k_i)_{i=1}^n$ посылает к P_2.

2. Получает значения для $x_{a_{j_i}}, x_{b_{j_i}}, x_{c_{j_i}}$ от P_1 и для x_{k_i} — от P_2 при $i = 1, 2, \ldots, u$. Принимает значения тогда и только тогда, когда они для x_{k_i} согласованы (совпадают) и C_{j_i} выполнимы для всех $1 \le i \le u$. Используя теорему 5, лемму 4 и честную стратегию, когда φ выполнима, получаем следующее утверждение.

Лемма 5 [4]. Если φ c-выполнима, где $c < 1$, то существует константа $c_c < 1$ такая, что для любого целого u оптимальные стратегии для P_1 и P_2 принуждают V утвердить в 2P1R-системе с вероятностью, не большей c_c^u. Если φ выполнима, то V всегда утверждает (принимает).

Для простоты обозначим U множество переменных $(k_i)_{i=1}^n$, которые посылаются к P_2, а множество значений $(x_{a_{j_i}}, x_{b_{j_i}}, x_{c_{j_i}})_{i=1}^u$, которые посылаются к P_1, обозначим W. Множество U имеет длину u, а множество W — длину $3u$.

В дальнейшем конвертируем 2P1R-систему в PCP-систему.

Определение 18. Стандартно записанное доказательство с параметром u или $SWP(u)$ состоит для каждого множества $V \subset [n]$ размера не более $3u$ из строки длиной $2^{2^{|V|}}$, которая интерпретируется как таблица функции $A_V : F_V \to \{-1, 1\}$.

Определение 19. Будем считать, что $SWP(u)$ — корректное доказательство для формулы φ от n переменных, если существует приписывание x, которое выполняет φ так, что A_V — длинный код $x_{/V}$ для произвольного V длины не более $3u$.

Длина $SWP(u)$ не больше $n^{3u} 2^{2^{3u}}$, и если $u = \text{const}$, то она полиномиальна.

Тест $L_2^{\varepsilon}(u)$

Ввод. Записанное доказательство $SWP(u)$.

Свойство. Проверка корректности $SWP(u)$ для формулы $\varphi = C_1 \wedge C_2 \wedge \ldots \wedge C_m$.

Проверяющий. 1. Случайно и равновероятно выбирает скобки $(C_{j_i})_{i=1}^{u}$ и для каждого i случайно и равновероятно выбирает переменную x_{k_i} из C_{j_i}. Пусть $U = \{x_{k_1}, x_{k_2}, \ldots, x_{k_u}\}$, W — множество переменных, которые встречаются в выбранных скобках, и $h = \wedge_{i=1}^{u} C_{j_i}$.

2. Выбирает $f \in F_V$ равновероятно.

3. Выбирает $g_1 \in F_W$ равновероятно.

4. Выбирает функцию $\mu \in F_W$, положив $\mu(y) = 1$ с вероятностью $1-\varepsilon$, и $\mu(y) = -1$ с вероятностью ε, независимо для каждого $y \in \{-1,1\}^{|W|}$.

5. Формирует $g_2 = fg_1\mu$, т.е. определяет g_2 для каждого $y \in \{-1,1\}^{|W|}$, как $g_2(y) = f(y_{/U})g_1(y)\mu(y)$.

6. Принимает решение тогда и только тогда, когда

$$A_{U,true}(f)A_{W,h,true}(g_1)A_{W,h,true}(g_2) = 1.$$

Поскольку исследования проводятся относительно экземпляров $Ins-Max-E3-Lin-2$, число уравнений увеличивается на 1 (u заменяется на $u+1$).

Лемма 6. Полнота теста $L_2^{\varepsilon}(u+1)$ не меньше $1-\varepsilon$.

Доказательство полностью аналогично доказательству леммы 5.1 из [4].

Лемма 7. Для произвольных $\varepsilon > 0$, $\delta > 0$ допустим, что вероятность того, что проверяющий принимает тест $L_2^{\varepsilon}(u+1)$, есть $\frac{2}{3}(1+\delta)$. Тогда существует стратегия для P_1 и P_2 в $(u+1)$-параллельной 2P1R-системе, которая дает возможность проверяющему принять с вероятностью, не меньшей $4\varepsilon\left(\frac{1+4\delta}{3}\right)^2$.

Доказательство аналогично доказательству леммы 5.2 из [4].

Пусть задано малое $\varepsilon_1 > 0$. Выберем такое $\delta > 0$, что $(1-\delta)\times\left(\frac{2}{3}(1+\delta)\right)^{-1} \geq$ $\geq \frac{3}{2} - \varepsilon_1$ (напомним, поскольку рассматривается множество $\{-1,1\}$, то в левой части линейного уравнения по mod 2 — произведение переменных, и в правой части 1 или -1).

Пусть L — произвольный язык в NP, x — некоторый вход, и нужно определить, принадлежит ли x к L. По теореме 4 за полиномиальное время можно получить $E3-CNF$-формулу φ (каждая переменная встречается пять раз) такую, что если $x \in L$, то φ выполнима, и если $x \notin L$, то φ не более чем c-выполнима, где c — константа, меньшая 1. Положим в лемме 7 $\varepsilon = \delta$ и выберем число уравнений $u+1$ так, чтобы $4\delta\left(\frac{1+4\delta}{3}\right)^2 > c_c^{u+1}$, где c_c — константа из леммы 5. Применим тест $L_2^{\delta}(u+1)$ к φ.

Для каждого бита b в $SWP(u+1)$ введем переменную x_b. Принятое утверждение в тесте $L_2^{\delta}(u+1)$ эквивалентно условию $b_{U,f}\, b_{W,h,g_1}\, b_{W,h,g_2} = b'$, где $b_{U,f}$, b_{W,h,g_1},

b_{W,h,g_2} — биты в доказательстве $A_{U,true}(f)$, $A_{W,h,true}(g_1)$, $A_{W,h,true}(g_2)$ соответственно и b' — константа.

Запишем уравнение с весами $x_{b_{U,f}} x_{b_{W,h,g_1}} x_{b_{W,h,g2}} = b'$. Вес этого уравнения — вероятность того, что проверяющий в тесте $L_2^{\delta}(u+1)$ выберет последовательность (U, W, h, f, g_1, g_2). Каждое доказательство отвечает приписываниям переменных x_b, и общий вес всех выполненных уравнений есть вероятность того, что доказательство принимается. Отсюда следует, что если $x \in L$, то максимальный вес одновременно выполненных уравнений не меньше $1-\delta$; если $x \notin L$, то по лемме 7 и по выбору u этот вес не больше $\frac{2}{3}(1+\delta)$. Число разных уравнений ограничено числом разных выборов проверяющего V. В [4] показано, что если $u = \text{const}$, множество уравнений конструируется за полиномиальное время. Отсюда следует, что любой алгоритм, который определяет максимальный общий вес одновременно выполненных уравнений с отношением, меньшим $(1-\delta)\left(\frac{2}{3}(1+\delta)\right)^{-1}$, может использоваться для определения $x \in L$, а это задание является *NP*-трудным. Тем самым доказано утверждение: для произвольного $\varepsilon_1 > 0$ аппроксимировать проблему $Ins-Max-E3-Lin-2$ с отношением $\frac{3}{2}-\varepsilon_1$ является *NP*-трудным. Это утверждение эквивалентно теореме 12.

Теорема 13. Пусть $P \neq NP$, $\varepsilon, \delta > 0$ — произвольные малые константы. Для данного экземпляра проблемы $Ins-Max-Ek-Lin-2$, $k>3$, который имеет решение с не меньше чем $(1-\varepsilon)$ частью выполненных уравнений, никакой полиномиальный алгоритм не сможет найти решение x с не больше, чем $(2/3+\delta)$ частью выполненных уравнений. Заметим, что не существует полиномиального алгоритма для $Ins-Max-Ek-Lin-2$ с отношением аппроксимации, строго меньшим $3/2$.

Доказательство. Применим сводимость от случая $k=3$ до произвольного k задачи $Mak-Ek-Lin-2$, рассмотренную в [4] при доказательстве теоремы 5.5. Пусть задана система из $m+1$ уравнений $L(E_1,\ldots,E_m,E_{m+1})$ как экземпляр проблемы $Ins-Max-E3-Lin-2$ с тремя переменными в каждом уравнении из множества переменных $(x_i)_{i=1}^{n}$. Добавим в каждое уравнение новые $k-3$ переменные $(y_i)_{i=1}^{k-3}$, чтобы все уравнения имели k переменных. Рассмотрим произвольное приписывание переменных в «большой» системе и соответствующее приписывание переменных $(x_i)_{i=1}^{n}$ в «малой» (исходной) системе. Если $\prod_{i=1}^{k-3} y_i = 1$, то оптимальное решение «большой» системы переходит в оптимальное решение «малой» системы. Если $\prod_{i=1}^{k-3} y_i = -1$, то в «малой» системе выполнены только те уравнения, которые не выполнены в «большой». Изменяя каждое значение x_i на противоположное (отрицание), получаем соответствующие выполненные уравнения в «большой» системе, т. е. оптимальное решение «малой» системы переходит в оптимальное решение «большой» системы. Таким образом, максимальное число выполненных уравнений сохраняется и легко перевести решение «большой» системы в соответствующее решение «малой» системы. Следовательно, имеем корректную сводимость от случая $k=3$ к произвольному $k>3$.

Объединяя результаты теорем 10 и 13, получаем, что при $k>3$, $k=O(\log n)$ $\frac{3}{2}$ — порог отношения аппроксимации для проблемы $Ins-Max-Ek-Lin-2$.

Таким образом, исходя из PCP-теоремы, удалось получить пороговое значение аппроксимационного отношения приближенных алгоритмов реоптимизации задачи о максимальном количестве выполненных уравнений в линейных системах над конечным полем.

СПИСОК ЛИТЕРАТУРЫ

1. Proof verification and intractability of approximation problems / S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy // J. of the ACM. — 1998. — **45**, N 3. — P. 501–555.
2. Goldreich O., Goldwasser S., Ron D. Property testing and its connection to learning and approximation abstract // Ibid. — 1998. — **45**, N 4. — P. 653–750.
3. Goldreich O., Sudan M. Locally testable codes and PCPs of almost-linear length // Ibid. — 2006. — **53**, N 4. — P. 558–655.
4. Hastad J. Some optimal inapproximability results // Ibid. — 2001. — **48**, N 4. — P. 798–859.
5. Hastad J. Complexity theory, proofs and approximation // European Congress of Mathematics. — 2005. — Stockholm, Sweden. — 15 p.
6. Ausiello G., Escoffier B., Monnot J., Paschos V.Th. Reoptimization of minimum and maximum traveling salesman's tours // Algorithmic theory. — SWAT 2006, Lect. Notes Comput. Sci. — Berlin: Springer, 2006. — **4059**. — P. 196–207.
7. On the approximability of TSP on local modifications of optimal solved instances / H.J. Bockenhauer, L. Forlizzi, J. Hromkovic, et al. // Algorithmic Oper. Res. — 2007. — **2**, N 2. — P. 83–93.
8. Bockenhauer H.J., Hromkovic J., Momke T., Widmayer P. On the hardness of reoptimization // Proc. of the 34th Intern. Conf. on Current Trends in Theory and Practice of Computer Science (SOF- SEM 2008); Lect. Notes Comput. Sci. — Berlin: Springer, 2008. — **4910**. — P. 50–65.
9. Escoffier B., Milanic M., Paschos V. Simple and fast reoptimizations for the Steiner tree problem: (Techn. Rep.) / Algorithmic Oper. Res. — 2009. — **4**, N 2. — P. 86–94.
10. Archetti C., Bertazzi L., Speranza M.G. Reoptimizing the travelling salesman problem // Networks. — 2003. — **42**, N 3. — P. 154–159.
11. Archetti C., Bertazzi L., Speranza M.G. Reoptimizing the 0–1 knapsack problem // Discrete Applied Mathematics. — 2010. — **158** (17). — P. 1879–1887.
12. Ausiello G., Bonifaci V., Escoffier B. Complexity and approximation in reoptimization // Computability in Context: Computation and Logic in the Real World. — Imperial College Press, members of the 2007 Computability Europe conf. CiE 2007: Logic and Computation in the Real World (June, 2007). — P. 24–33.
13. Михайлюк В.А. Реоптимизация задачи о покрытии множествами // Кибернетика и системный анализ. — 2010. — № 6. — С. 27–31.
14. Михайлюк В.А. Общий подход к оценке сложности постоптимального анализа дискретных задач оптимизации // Там же. — 2010. — № 2. — С. 134–141.
15. O'Donnel R. Some topics in analysis of Boolean functions // Electronic Colloquium on Comput. Complexity. — 2008. — Rep. N 55.
16. Khot S. Inapproximability of *NP*-complete problems, discrete Fourier analysis, and geometry // Proceedings of the International Congress of Mathematicians. — 2010. — Hyderabad, India.
17. Raz R. A parallel repetition theorem // SIAM J. on Computing. — 1998. — **27**, N 3. — P. 763–803.
18. Vazirani V.V. Approximation algorithms. — Berlin: Springer-Verlag, 2001. — 380 p.
19. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982 . — 416 с.

Поступила 21.03.2011