КИБЕРНЕТИКА

В.А. МИХАЙЛЮК, И.В. СЕРГИЕНКО

УДК 519.854

РЕОПТИМИЗАЦИЯ ОБОБЩЕННЫХ ПРОБЛЕМ О ВЫПОЛНИМОСТИ С АППРОКСИМАЦИОННО-УСТОЙЧИВЫМИ ПРЕДИКАТАМИ

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

ВВЕДЕНИЕ

Обобщенные проблемы о выполнимости или CSP-проблемы (Constraint Satisfaction Problems) являются обобщениями многих задач дискретной оптимизации. В таких проблемах ограничения задаются k-местным предикатом P. Так, проблема $Max-CSP-P$ заключается в следующем: найти такое приписывание значений истинности переменным, при котором число выполненных ограничений максимально. Многие оптимизационные проблемы являются NP-трудными, а значит, решить их точно за приемлемое время вряд ли представляется возможным. Здесь рассматриваются эффективные приближенные алгоритмы для решения таких задач. Относительно максимизационной проблемы считают, что алгоритм является C-приближенным, если он для произвольного экземпляра дает решение со значением целевой функции, не меньшим $C \cdot \text{OPT}$, где OPT — глобальный оптимум, C — отношение аппроксимации. Подобное определение можно дать для минимизационных проблем.

Фундаментальный вопрос для заданной NP-трудной проблемы залючается в следующем: определить, для каких значений C можно полагаться на эффективный (полиномиальный) C-приближенный алгоритм? Это большая исследовательская область, охватывающая теоретическую информатику со своими позитивными и негативными результатами.

Понятие реоптимизации [1–7] состоит в следующем. Пусть Q — некоторая NP-трудная (возможно, NP-полная) проблема, I — начальный экземпляр проблемы Q, оптимальное решение которого известно. Предлагается новый экземпляр I' задачи Q с некоторыми «незначительными» изменениями экземпляра I. Возникает вопрос: как можно эффективно использовать знания об оптимальном решении I для вычисления точного или приближенного решения экземпляра I'? Суть реоптимизации при использовании приближенных методов — применение знаний о решении начального экземпляра I с целью либо достижения лучшего качества приближения (аппроксимационного отношения) I', либо создания более эффективного (по времени) алгоритма определения оптимального или близкого к нему решения I', либо выполнения обоих условий.

Считают, что для проблемы Q установлена верхняя оценка отношения аппроксимации C, если существует полиномиальный C-приближенный алгоритм для решения Q. Для этой проблемы установлена нижняя оценка отношения аппроксимации c, если для произвольного $\varepsilon > 0$ не существует полиномиального приближенного алгоритма для Q, на котором достигается отношение аппроксимации $c+\varepsilon$. Если $C=c$, то для проблемы Q установлен порог отношения аппроксимации.

Для некоторых проблем удалось установить порог отношения аппроксимации, например для $Max-E3-SAT$ — порог $\frac{7}{8}$, для $Max-E3-Lin-2$ — порог $\frac{1}{2}$ [8], для задачи о покрытии множествами — порог $\ln n$ [11].

Проблема установления нижних оценок отношения аппроксимации (как и любая проблема получения нижних оценок сложности) является довольно трудной. Для такой проблемы существует термин «неаппроксимируемость» (inapproximability), т.е. трудность аппроксимации (hardness of approximation). Большое влияние на развитие методов получения нижних оценок оказали известная PCP-теорема [12] и дискретный анализ Фурье для тестирования свойств проблем (property testing) [13, 14].

Известны следующие результаты, полученные при реоптимизации дискретных задач оптимизации. При вставке элементарной дизъюнкции в экземпляр проблемы реоптимизация задачи Max Weighted Sat (взвешенная задача о выполнимости на максимум) аппроксимируема с отношением 0.81, хотя задача Max Weighted Sat аппроксимируема с отношением 0.77 [7]. При вставке вершины в граф реоптимизация Min Vertex Cover (минимальное вершинное покрытие графа) аппроксимируема с отношением 1.5, Min Vertex Cover — с отношением 2 [7]. При вставке вершины (терминальной или нетерминальной) реоптимизация Min Steiner Tree (минимальное дерево Штейнера) аппроксимируема с отношением 1.5, а задача Min Steiner Tree аппроксимируема с отношением $1+\ln(3)/2\approx 1.55$ [4].

При вставке или удалении элемента из множества задача о покрытии множествами аппроксимируема с отношением $(2-\frac{1}{\ln m+1})$, где m — число элементов множества. Подобный результат имеет место при вставке или удалении произвольного числа $1< p< m$ элементов из множества [23]. Следует отметить цикл работ по реоптимизации задачи о коммивояжере (TSP — Travelling Salesman Problem) [1–3, 5]. Например, задача Minimum Metric TSP (Min TSP — задача о коммивояжере на минимум с метрическими расстояниями) аппроксимируема с отношением 1.5, ее реоптимизация при вставке нового узла — с отношением 1.34, реоптимизация этой задачи при изменении расстояний аппроксимируема с отношением 1.4 [7]. Для общей задачи о коммивояжере (Min TSP) неизвестны оценки аппроксимации как непосредственно для нее, так и для различных версий реоптимизации.

Известно, что проблема $Max-CSP-P$ является NP-трудной для предикатов P, которые зависят не менее чем от двух переменных [16]. Представляет интерес нахождение эффективного аппроксимационного алгоритма для этой проблемы. Тривиальный алгоритм — приписать переменным случайные значения. В [8–10] Хастад показал, что, используя эти случайные приписывания, можно получить аппроксимационный оптимальный алгоритм для $Max-CSP-P$ (с достижением порога аппроксимационного отношения) при некоторых предикатах P. Такие предикаты называют аппроксимационно-устойчивыми (approximation resistant).

Основной результат настоящей статьи: получен полиномиальный алгоритм с некоторым отношением аппроксимации для реоптимизации проблемы $Max-CSP-P$ при вставке некоторого ограничения. Показано, что это отношение является пороговым, если предикат P принадлежит классу аппроксимационно-устойчивых предикатов. Доказана теорема.

Теорема 1. Если $k=O(\log n)$ и предикат P аппроксимационно-устойчивый, то для проблемы $Ins-Max-EkCSP-P$ (реоптимизация $Max-EkCSP-P$) существует полиномиальный приближенный алгоритм с отношением аппроксимации $q(P)=\frac{1}{2-d(P)}$, где $d(P)=2^{-k}|P^{-1}(1)|$ — пороговое «случайное» отношение аппроксимации предиката P. Отношение аппроксимации $q(P)$ является пороговым.

ПОСТАНОВКА ЗАДАЧИ. АППРОКСИМАЦИОННО-УСТОЙЧИВЫЕ ПРЕДИКАТЫ И ПРОБЛЕМЫ

Введем необходимые обозначения и определения [8, 16]. Под предикатом P размерности k будем понимать отображение $P:\{-1,1\}^k \to \{0,1\}$. Для удобства обозначений входные данные со значением –1 интерпретируем как «истина», со значением 1 — как «ложь». Если предикат P принимает входное значение y, то $P(y)=1$, иначе $P(y)=0$. Таким образом, множество значений, принимаемых предикатом P, обозначается $P^{-1}(1)$. Логические AND, OR и XOR от двух переменных обозначим как $x \wedge y$, $x \vee y$ и $x \oplus y$ соответственно. Для целого k обозначим предикаты $kOR, kAND$ и $kXOR$ как логическое OR, AND и XOR от k переменных соответственно. Если $kXOR(x_1, \ldots, x_k)=1$, то $(x_1, \ldots, x_k)$ имеет нечетный паритет, иначе — четный паритет. Булеву переменную или ее отрицание будем считать литералом.

Определение 1. Пусть $P:\{-1,1\}^k \to \{0,1\}$ есть предикат. Экземпляр проблемы $Max-CSP-P$ состоит из m взвешенных ограничений, каждое из которых представляет k — кортеж литералов $(z_{i_1}, \ldots, z_{i_k})$, взятых из множества $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$. Все переменные в этом кортеже считаются разными. Ограничение выполнено тогда и только тогда, когда P принимает этот кортеж. Решение состоит в приписывании истинностных значений к множеству $\{x_1, \ldots, x_n\}$. В результате решения имеем $\sum_{i=1}^{m} w_i P(z_{i_1}, \ldots, z_{i_k})$, где w_i есть (не отрицательный) вес i-го ограничения. Цель проблемы состоит в максимизации этого значения. Когда P зависит не более чем от k литералов, $Max-CSP-P$ будем называть $Max-kCSP-P$; если в P точно k литералов, то будем называть $Max-EkCSP-P$.

Наряду с проблемами типа $Max-CSP-P$ рассматриваются проблемы типа $CSP-P$, цель которых состоит в нахождении такого приписывания, когда все ограничения выполнены (аналогично определяются проблемы $kCSP-P$ и $EkCSP-P$).

Определение 2. Два k-местных предиката P и P'имеют одинаковый тип тогда и только тогда, когда существует перестановка π на $[k]=\{1, \ldots, k\}$ и $a \in \{-1,1\}^k$ такое, что $P(x_1, \ldots, x_k) = P'(a_1 x_{\pi(1)}, \ldots, a_k x_{\pi(k)})$ для всех $x \in \{-1,1\}^k$.

Если P и P' имеют одинаковый тип, то экземпляр проблемы $Max-CSP-P$ может быть выражен как экземпляр $Max-CSP-P'$, переставляя кортежи согласно маске, т.е. эти проблемы эквивалентны.

Определение 3. Проблема $Max-kCSP-P$, где каждое ограничение есть дизъюнкция не более k литералов, является проблемой $Max-k-SAT$. Если каждое ограничение содержит точно k литералов, то это является проблемой $Max-Ek-SAT$.

Определение 4. Проблема $Max-kCSP-P$, где каждое ограничение есть произведение не более k литералов, равное константе, является проблемой $Max-k-LIN$. Если каждое ограничение содержит точно k литералов, то это проблема $Max-Ek-LIN$.

Пусть $w_{\text{opt}}(I)$ — значение оптимального решения экземпляра I. Тогда имеет место определение.

Определение 5. Алгоритм A является C-приближенным алгоритмом для максимизационной проблемы, если для всех экземпляров I проблемы имеем $w(A,I) \geq C \cdot w_{\text{opt}}(I)$, где $w(A,I)$ — значение решения алгоритма A на входе I. При этом считают, что A имеет аппроксимационное отношение C. Для вероятностных алгоритмов $w(A,I)$ является ожидаемым значением (математическим ожиданием) среди случайных выборов алгоритма A.

Считают, что предикат P является аппроксимационно-устойчивым (как и соответствующая проблема $Max-CSP-P$), если NP-трудным находить решение $Max-CSP-P$, которое значительно лучше, чем ожидаемое значение при случайном приписывании. Поскольку случайное приписывание выполняет произвольное P-ограничение с вероятностью $d(P)=2^{-k}|P^{-1}(1)|$, то имеем следующее определение.

Определение 6. Предикат $P:\{-1,1\}^k \to \{0,1\}$ называется аппроксимационно-устойчивым, если для произвольной константы $\varepsilon>0$ найти решение x экземпляра I проблемы $Max-CSP-P$ такое, что значение x, не меньшее $(d(P)+\varepsilon)w_{\mathrm{opt}}(I)$, является NP-трудным.

Определение 7. Проблема $Max-CSP-P$ всегда аппроксимируема, если для произвольного $\delta>0$ существует $\varepsilon_\delta>0$ и эффективный алгоритм, который исходя из экземпляра, где $(d(P)+\delta)$ — часть ограничений одновременно выполнена, находит приписывание, которое выполняет часть ограничений, не меньшую, чем $(d(P)+\varepsilon_\delta)$.

Если проблема не всегда аппроксимируема, то она аппроксимационно-устойчива.

Определение 8. Предикат $P:\{-1,1\}^k \to \{0,1\}$ называется наследственно аппроксимационно-устойчивым, если все предикаты P', которые являются следствиями P (т. е. $(P(y)=1)\Rightarrow(P'(y)=1)$ для всех y), аппроксимационно-устойчивы.

Теорема 2 [10]. Проблема $Max-CSP-P$ допускает полиномиально-приближенный алгоритм с отношением аппроксимации $d(P)$.

Доказательство. Допустим, что имеется экземпляр с m ограничениями. Случайное приписывание выполняет каждое данное ограничение с вероятностью $d(P)$, т.е. выполняет $d(P)\cdot m$ ограничений в среднем. Поскольку оптимальное приписывание выполняет не более m ограничений, имеем случайный $d(P)$-приближенный алгоритм. Методом условных вероятностей этот случайный алгоритм может быть дерандомизирован [21].

Замечание 1. Для аппроксимационно-устойчивых предикатов P порог отношения аппроксимации проблемы $Max-CSP-P$ достигается (теорема 2) и равен $d(P)=2^{-k}|P^{-1}(1)|$.

Это значение будем называть пороговым «случайным» отношением аппроксимации предиката P.

Имеют место следующие результаты по аппроксимационно-устойчивым предикатам проблемы $Max-EkCSP-P$. Не существует предикатов размерности $2(k=2)$, которые являются аппроксимационно-устойчивыми [15]. При $k=3$ проблема $Max-E3-LIN$ является наследственно аппроксимационно-устойчивой [8], и это исчерпывает все аппроксимационно-устойчивые предикаты размерности 3 [17]. Аппроксимационно-устойчивые предикаты размерности 4 $(k=4)$ исследованы в работе [16], где существует 400 различных предикатов (с точностью до перестановки переменных и их отрицаний). Из них 79 идентифицированы как аппроксимационно-устойчивые; 275 — как неаппроксимационно-устойчивые; статус оставшихся 46 предикатов определить не удалось.

Приведем основные результаты для аппроксимационно-устойчивых предикатов размерности 3 $(Max-E3CSP-P)$.

Теорема 3 [8]. Для произвольного $\varepsilon>0$ является NP-трудным аппроксимировать проблему $Max-E3-LIN$ с отношением $\frac{1}{2}+\varepsilon$. Иными словами, проблема $Max-E3-LIN$ аппроксимационно-устойчива.

Теорема 4 [8]. Для произвольного $\varepsilon>0$ является NP-трудным аппроксимировать проблему $Max-E3-SAT$ с отношением $\frac{7}{8}+\varepsilon$. Иными словами, проблема $Max-E3-SAT$ аппроксимационно-устойчива.

Теорема 5 [8]. Пусть P — предикат от трех переменных такой, что $P(x,y,z)=1$ для произвольных x, y, z, удовлетворяющих уравнению $xyz=1$, тогда проблема CSP, определяемая с помощью P, аппроксимационно-устойчива.

Теорема 5 остается правильной при замене уравнения $xyz=1$ на $xyz=-1$. Обобщением теоремы 5 есть следующая теорема.

Теорема 6 [10]. Предикат P от трех переменных является аппроксимационно-устойчивым тогда и только тогда, когда он является следствием нечетного или четного паритета.

Введем следующие трехместные предикаты [17]:

$$XOR(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3,\ \ NTW(x_1, x_2, x_3) = (\bar{x}_1 \vee \bar{x}_2)\bar{x}_3 \vee (x_1 \equiv x_2)x_3,$$

$$OXR(x_1, x_2, x_3) = x_1 \vee (x_2 \oplus x_3),\ \ OR(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3.$$

Приведенные выше результаты можно обобщить в виде следующего утверждения.

Теорема 7. Предикаты XOR, NTW, OXR, OR являются аппроксимационно-устойчивыми предикатами. Из них XOR, NTW, OXR — наследственно аппроксимационно-устойчивые предикаты.

Пусть $Max-EkCSP-P$ — произвольная невзвешенная CSP-проблема ($w_i = 1,\ i \in [m]$). Пусть I — произвольный экземпляр проблемы $Max-EkCSP-P$, экземпляр I' этой проблемы образуется из экземпляра I добавлением произвольного $(m+1)$-го ограничения

$$z^{(m+1)} = (z_{i_1}^{(m+1)}, \ldots, z_{i_k}^{(m+1)}),\ \ z_{i_j}^{(m+1)} \in \{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}, j \in [k].$$

Определим реоптимизационный вариант проблемы $Max-EkCSP-P$.

Проблема $Ins-Max-EkCSP-P$. **Входные данные.** Произвольный экземпляр I проблемы $Max-EkCSP-P$, x^* — оптимальное решение экземпляра I.

Результат. Найти оптимальное решение экземпляра I', полученного исходя из экземпляра I (как описано выше) проблемы $Max-EkCSP-P$, используя x^*.

Цель. Найти x, которое максимизирует число выполненных ограничений экземпляра I'.

Поскольку проблема $Max-EkCSP-P$ является NP-трудной для $k \geq 2$, то легко показать, что таковой будет и $Ins-Max-EkCSP-P$.

НЕКОТОРЫЕ СВЕДЕНИЯ ИЗ ДИСКРЕТНОГО АНАЛИЗА ФУРЬЕ БУЛЕВЫХ ФУНКЦИЙ И ТЕОРИИ PCP-СИСТЕМ

Приведенная ниже информация взята из [18, 19]. Будем рассматривать булевы функции как отображения $f: \{0, 1\}^n \to \{0, 1\}$. Если интерпретировать 0 и 1, как 1 и –1, то получим такое представление булевых функций: $f: \{-1, 1\}^n \to \{-1, 1\}$. Существует следующий способ, представляющий f в виде полинома. Так, 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 $x = (x_1, x_2, x_3)$ можно записать

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

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

После умножения выражений в скобках и сведения подобных членов можно получить

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

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

Предложение 1. Произвольная функция $f:\{-1,1\}^n \to R$ может быть единственным образом 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 обозначим как $\hat{f}(S)$, а $\prod_{i\in S} x_i$ — как $\chi_S(x)$. Тогда получим

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

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 $\langle\chi_S,\chi_S\rangle=1$, $|\chi_S(x)|=1$. Выполняются следующие предложения.

Предложение 2: 1) если $S\neq T$, то $\langle\chi_S,\chi_T\rangle=0$;

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

Будем рассматривать $x=(x_1,\ldots,x_n)$ как случайную строку, равномерно распределенную на $\{-1,1\}^n$. Такая случайная строка $x=(x_1,\ldots,x_n)$ будет генерироваться выбором каждого x_i независимо и равновероятно с $\{-1,1\}$. Через $\underset{x}{E}[f(x)]$ будем обозначать математическое ожидание случайной булевой функции $f(x)$ относительно распределения x.

Теорема 8 (Парсеваля). Для произвольной $f:\{-1,1\}^n\to R$

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

Предложение 3: 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 $\sum_{S\subseteq[n]}\hat{f}(S)^2=1$ (следствие из теоремы 8 — равенство Парсеваля).

Определение 9. Для данного $0\le\varepsilon\le1$ 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 увидеть, что $E[x_i\, y_i] = \Pr[x_i = y_i] - \Pr[x_i \neq y_i] = 1 - 2\varepsilon$, откуда следует $(1-2\varepsilon)$-коррелированность.

Далее будем использовать информацию из работы [19]. Пусть P — произвольная оптимизационная (для определенности на максимум) проблема. Под $(c, s) - gap$ версией проблемы P (обозначение $GapP_{c,s}$) будем понимать проблему, для которой либо $\mathrm{OPT}(I) \geq c$, либо $\mathrm{OPT}(I) \leq s$ 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 есть дизъюнкция трех булевых переменных или их отрицаний. Суть проблемы состоит в приписывании булевым переменным таких значений истинности, что формула становится логически истинной (выполнимой). Будем считать, что CNF-формула φ с m скобками c-выполнима ($c \in [0, 1]$) тогда и только тогда, когда некоторое приписывание выполняет не более 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. При этом если ψ имеет приписывание, которое делает ее выполнимой, то $\mathrm{OPT}(I) \geq c$. В противном случае $\mathrm{OPT}(I) \leq s$.

Такая сводимость предполагает, что если существует полиномиальный алгоритм с отношением аппроксимации строго большим, чем $\frac{s}{c}$ для проблемы P, то существует возможность эффективно определить, выполнима ли $3SAT$-формула, т.е. $P = NP$. Таким образом, при стандартном предположении $P \neq NP$ эта сводимость является источником получения результатов по неаппроксимируемости для проблемы P.

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

1) если $\mathrm{OPT}(\psi) = 1$, то $\mathrm{OPT}(\varphi) = 1$ (полнота (Completeness));

2) если $\mathrm{OPT}(\psi) < 1$, то $\mathrm{OPT}(\varphi) \leq \alpha$ (корректность (Soundness)).

Отсюда следует, что проблема $Max - 3SAT$ неаппроксимируема с отношением аппроксимации $\alpha < 1$. PCP-теорема была представлена выше в качестве комбинаторной сводимости. Существует эквивалентная формулировка в терминах проверки доказательств (proof checking). Теорема утверждает, что каждое NP-утверждение имеет полиномиальное доказательство, которое может быть проверено полиномиальным вероятностным проверяющим (verifier), считывающим только константное число бит в доказательстве. Проверяющий имеет свойства полноты и корректности: каждое доказательство корректного утверждения принимается с вероятностью единица, и каждое доказательство некорректного утверждения принимается с малой вероятностью (например, не большей 1%). Таким образом, комбинаторная сводимость и проверка доказательств являются методами для установления неаппроксимируемости оптимизационных проблем.

Для описания этих методов приведем формальные определения [8]. Будем определять системы доказательств (proof systems) с помощью свойств проверяющего (verifier). Для проверки утверждений проверяющему необходимы помощники. Будем считать, что он имеет доступ к одному или нескольким оракулам — функциям. Во многих вариантах систем доказательств обсуждаются понятия доказывающих (proovers (пруверы)) и записанных доказательств (written proofs).

Записанные доказательства эквивалентны доказательствам, использующих оракулы, где считывание i-го бита соответствует вопросу к оракулу. Отметим, что пруверы более мощные, чем оракулы, поскольку могут быть случайными и исторически зависимыми.

Определение 10. Оракул есть функция $\Sigma^* \to \{0,1\}$ (где Σ^* — множество конечных строк в алфавите Σ).

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

Определение 11. 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 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 12. Проверяющий V использует логарифмическую случайность, если существует абсолютная константа c такая, что для каждого входа x и доказательства оракула π длина случайной строки r, которую использует V^{π}, оценивается сверху как $c \log|x|$.

Определение 13. Проверяющий V считывает c бит в вероятностно-проверяемом доказательстве, если для каждого результата случайных испытаний и каждого доказательства π проверяющий V^{π} задает не более c вопросов оракулу.

Теорема 9 (PCP-теорема) [8]. Существует универсальное целое c такое, что язык в NP имеет PCP проверяющего V с полнотой единица и корректностью $\frac{1}{2}$, где V использует логарифмическую случайность и считывает не более c бит в доказательстве.

Теорема 10 (вариант PCP-теоремы) [8]. Пусть L — язык в NP и x— строка. Существует универсальная константа $c<1$ такая, что за время, полиномиальное относительно $|x|$, можно сконструировать формулу $\varphi_{x,L}$ $E3-CNF$ такую, что если $x \in L$, то $\varphi_{x,L}$ выполнима; если $x \notin L$, то $\varphi_{x,L}$ не более чем c-выполнима. Кроме того, каждая переменная встречается в формуле точно пять раз.

Опишем однораундовую интерактивную систему доказательств с двумя пруверами (two prover one-round proof system, сокращенно 2P1R-система). Проверяющий в такой системе имеет доступ к двум оракулам и может задать один вопрос каждому из них.

Поскольку проверяющий работает в полиномиальное время, то он не может считать больше, чем полиномиальное число бит. 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 решение, то $V(x, r, P_1(q_1), P_2(q_2)) = 1$.

Определение 14. Пусть c, s — действительные числа, $0 \le s < c \le 1$. Полиномиальная вероятностная машина Тьюринга V с двумя оракулами — это 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 два оракула P_1, P_2 такие, что $\Pr_r[V(x, r, P_1(q_1), P_2(q_2)) = 1] \ge c$;
- для $x \notin L$ и 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. Аналогичная ситуация имеет место для $P_2(q_2)$.

Используя однораундовый протокол с корректностью s, согласно определению 14 можно повторить его последовательно дважды. Тогда корректность улучшится (уменьшится) до s^2. Последовательно повторяя протокол u раз, получаем корректность s^u. В результате получим многораундовый протокол. Чтобы он не изменился, применим технику параллельных повторов. Проверяющий V повторяет свои случайные выборы u раз для получения u независимых пар вопросов $(q_1^{(i)}, q_2^{(i)})_{i=1}^u$ и посылает $(q_1^{(i)})_{i=1}^u$ к P_1, а $(q_2^{(i)})_{i=1}^u$ — к P_2.

Затем V получает u ответов от каждого прувера и принимает их так, как будто он работает в однораундовой системе u раз. Корректность такого протокола может быть больше s^u. Однако Рац (Raz) [20] доказал, что при малом размере ответа корректность экспоненциально уменьшается относительно u.

Теорема 11 [20]. Для всех целых d и $s < 1$ существует $c_{d,s} < 1$ такая, что для данной 2P1R-системы при корректности s и с размерами ответов, не бóльшими d, для всех целых u корректность протоколов, работающих параллельно, не больше $c_{d,s}^u$.

Определение 15. Обозначим через $2\mathrm{P1R}_{c,s}$ $(r(n))$-класс языков L, для которых существует 2P1R-система с проверяющим V, которому доступно случайное число $r(n)$ бит.

Теорема 12 [21]. Существует константа $\varepsilon_P > 0$ такая, что $NP = 2\mathrm{P1R}_{1,1-\varepsilon_P}(\log n)$.

ПОРОГ ОТНОШЕНИЯ АППРОКСИМАЦИИ ДЛЯ РЕОПТИМИЗАЦИИ АППРОКСИМАЦИОННО-УСТОЙЧИВЫХ ПРОБЛЕМ

Теорема 13. Для проблемы $Ins - Max - EkCSP - P$ (реоптимизация $Max - EkCSP - P$) существует полиномиальный приближенный алгоритм с отношением аппроксимации $q(P) = \dfrac{2^k}{2^{k+1} - |P^{-1}(1)|}$, если $k = O(\log n)$.

Доказательство. Применим подход, рассмотренный в [23]. Пусть I — экземпляр проблемы $Max - EkCSP - P$, который состоит из системы ограничений $C = \{z^{(i)}, i \in [m]\}$ и оптимального решения x^*; $w(x^*)$ — число выполненных ограничений в системе C решением x^*. К системе добавлено ограничение $z^{(m+1)}$, в результате получаем экземпляр I' проблемы $Max - EkCSP - P$. Пусть $x_{I'}^*$ — его оптимальное решение. Если $x_{I'}^*$ не выполняет ограничения $z^{(m+1)}$, то x^* есть оптимальное решение экземпляра I' проблемы $Ins - Max - EkCSP - P$, отсюда

$$w(x^*) \geq w(x_{I'}^*) - 1. \tag{3}$$

Из левой части неравенства следует, что x^* — оптимальное решение I', а из правой части — что оптимальное решение не выполняет ограничения $z^{(m+1)}$. Пусть $x_{I'}^*$ выполняет ограничение $z^{(m+1)}$ и представляет l вариантов, при которых будет выполнено ограничение $z^{(m+1)}$ (очевидно, что $l < 2^k$). Построим l приближенных решений x^i $(i \in [l])$ следующим образом. Выберем i-е приписывание, которое выполняет ограничение $z^{(m+1)}$. Из системы ограничений удаляем $z^{(m+1)}$ и к оставшимся ограничениям (учитывая результат приписывания) применяем некоторый полиномиальный ρ-приближенный алгоритм. Получаем приближенное решение x^i. Тогда

$$w(x^i) \geq \rho(w(x_{I'}^*) - 1) + 1 = \rho w(x_{I'}^*) + 1 - \rho. \tag{4}$$

Умножая обе части неравенства (3) на $1-\rho$ и складывая с (4), получаем

$$(1-\rho)w(x^*)+w(x^i)\geq(1-\rho)w(x^*_{I'})-(1-\rho)+\rho w(x^*_{I'})+1-\rho=w(x^*_{I'}).$$

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

$$w(x^*_{I'})\leq(1-\rho+1)\max\{w(x^*),w(x^i)\}=(2-\rho)w(\bar{x}),$$

откуда $w(\bar{x})\geq\frac{1}{2-\rho}w(x^*_{I'})$. Для полиномиальности описанного алгоритма достаточно потребовать, чтобы $2^k\leq n^c$ (n — общее число переменных $c=\text{const}$), откуда следует $k=O(\log n)$ в условии теоремы. Таким образом, в результате выполнения описанного алгоритма получено приближенное решение $\bar{x}$ экземпляра I' с отношением аппроксимации $\frac{1}{2-\rho}$. Очевидно, что всегда $\frac{1}{2-\rho}>\rho$ $(\rho\neq1)$. Положим $\rho=d(P)=2^{-k}|P^{-1}(1)|$. Тогда, применив приближенный алгоритм из теоремы 1, получим утверждение данной теоремы.

Теорема 14. Если предикат P является аппроксимационно-устойчивым и для проблемы $Ins-Max-EkCSP-P$ существует полиномиально-приближенный алгоритм с отношением аппроксимации γ, то $\gamma\leq q(P)$.

Доказательство. Пусть I — экземпляр проблемы $Max-EkCSP-P$, который состоит из системы ограничений $C=\{z^{(i)},\ i\in[m]\}$ и оптимального решения x^*. К системе добавляется ограничение $z^{(m+1)}$, в результате получаем экземпляр I' проблемы $Ins-Max-EkCSP-P$. Пусть $\bar{x}$ — решение проблемы $Ins-Max-EkCSP-P$, полученное с помощью алгоритма из доказательства теоремы 13. Решение $\bar{x}$ является лучшим (большим по значению целевой функции) из решений x^* и x^i $(i\in[l],l<2^k)$. Оно получается полиномиальным приближенным алгоритмом с отношением аппроксимации $\varphi(\rho)=\frac{1}{2-\rho}$. Доказательство проведем от противного. Пусть $\gamma>q(P)$ и $\varphi(\rho)=\gamma$. Поскольку функция $\varphi(\rho)$является возрастающей по ρ и $\varphi(\rho)=\gamma>q(P)=\varphi(d(P))$, то отсюда следует, что $\rho>d(P)$. А это противоречит тому факту, что предикат P аппроксимационно-устойчивый (т. е. для получения решения какого-то x^i применялся полиномиальный алгоритм с отношением аппроксимации, большим $d(P)$, что в силу аппроксимационной устойчивости предиката P невозможно).

Теорема 15. Если $k=O(\log n)$ и предикат P аппроксимационно-устойчивый, то для проблемы $Ins-Max-EkCSP-P$ (реоптимизация $Max-EkCSP-P$) существует полиномиальный приближенный алгоритм с отношением аппроксимации $q(P)=\frac{2^k}{2^{k+1}-|P^{-1}(1)|}$. Данное отношение аппроксимации является пороговым.

Доказательство следует из теорем 13 и 14.

ПРИМЕРЫ ДЛЯ ТРЕХМЕСТНЫХ ПРЕДИКАТОВ

Каждый предикат P от трех переменных ($k=3$) можно единственным образом представить в виде формулы Фурье $P(x)=\sum_{S\subseteq[3]}c_S^P\prod_{i\in S}x_i$, где c_S^P — коэффициенты Фурье. Имеется следующий критерий того, что предикат P всегда аппроксимирован (определение 7).

Теорема 16 [10]. Предикат P от трех переменных является всегда аппроксимируемым тогда и только тогда, когда $c^P_{\{1,2,3\}}=0.$

Если проблема не всегда аппроксимируема, то она аппроксимационно-устойчива.

Если проверяющий V в PCP-системе использует в своей работе k-местный предикат P для принятия решения, то будем считать, что такой проверяющий имеет условие принятия P. Существует следующий критерий аппроксимационной устойчивости, связанный с PCP-системами.

Теорема 17 [16]. Пусть $P:\{-1,1\}^k \to \{0,1\}$ — предикат и $L-NP$-полный язык. Если для произвольной константы $\varepsilon>0$ существует полиномиальный проверяющий в PCP-системе с условием принятия P для L, использующий логарифмическую случайность и имеющий полноту не менее $1-\varepsilon$ и корректность не более $2^{-k}|P^{-1}(1)|+\varepsilon,$ то P аппроксимационно-устойчивый.

Доказательство. Определение принадлежности произвольного элемента υ к L является NP-трудным. Покажем, что если для экземпляра I проблемы $Max-CSP-P$ удастся найти решение со значением, не меньшим $(2^{-k}|P^{-1}(1)|+\gamma)w_{\text{opt}}(I)$ для произвольной константы $\gamma>0$, то можно определить принадлежность υ к L. Это будет означать, что P аппроксимационно-устойчивый. Пусть ε — такое значение, для которого $\dfrac{2^{-k}|P^{-1}(1)|+\varepsilon}{1-\varepsilon}<2^{-k}|P^{-1}(1)|+\gamma$.

Проверяющий использует логарифмическое число случайных бит. Значит, существует только полиномиальное число возможных исходов. Для каждого такого исхода проверяющий считывает k бит с доказательства и проверяет их с помощью P. Добавим соответствующее P-ограничение к экземпляру I проблемы $Max-CSP-P$. Заметим, что вероятность того, что проверяющий примет доказательство T (T — код приписывания), в точности равна доли выполненных ограничений в экземпляре I приписыванием, определенным T.

Корректность PCP-системы означает, что если $\upsilon\notin L$, то не существует приписывания, которое выполняет долю ограничений $2^{-k}|P^{-1}(1)|+\varepsilon$ в I. Однако если $\upsilon\in L$, то проверяющий имеет полноту, которая предполагает, что экземпляр I есть $(1-\varepsilon)$-выполненным. Тогда с помощью части $(2^{-k}|P^{-1}(1)|+\gamma)$ — приближения экземпляра I, найдем решение со значением, не меньшим

$$(2^{-k}|P^{-1}(1)|+\gamma)w_{\text{opt}}(I)\ge(2^{-k}|P^{-1}(1)|+\gamma)(1-\varepsilon)w_{\text{tot}}(I)>(2^{-k}|P^{-1}(1)|+\varepsilon)w_{\text{tot}}(I),$$

где $w_{\text{tot}}(I)$ — общий вес выполненных ограничений в I.

Таким образом, можно определить, принадлежит ли υ к L.

Пример 1. Рассмотрим проблему $Max-3CSP-XOR$ с соответствующим реоптимизационным вариантом $Ins-Max-3CSP-XOR$. По теореме 7 предикат XOR — наследственно аппроксимационно-устойчивый (доказано в [16]). Применим теорему 15 ($k=3, |P^{-1}(1)|=4$) и получим утверждение.

Утверждение 1. Для проблемы $Ins-Max-E3CSP-XOR$ (реоптимизация $Max-E3CSP-XOR$) существует полиномиальный приближенный алгоритм с отношением аппроксимации $\dfrac{2}{3}$. Данное отношение аппроксимации является пороговым.

Пример 2. Рассмотрим проблему $Max-3CSP-Q$ с соответствующим реоптимизационным вариантом $Ins-Max-3CSP-Q,$ где $Q^{-1}(1)=\{(1,1,1),(1,-1,-1),(-1,1,-1),(-1,-1,1),(-1,-1,-1)\}$. Предикат Q — наследственно аппроксимационно-устойчивый. Рассмотрим схему доказательства этого факта, используя результаты из [8].

Представим схему доказательства наследственной аппроксимационной устойчивости Q. Разложение предиката Q по формуле Фурье (предложение 1) имеет вид

$$Q(x_1, x_2, x_3) = \frac{5 - x_1 - x_2 - x_3 + x_1x_2 + x_1x_3 + x_2x_3 + 3x_1x_2x_3}{8}. \qquad (5)$$

Чтобы показать, что предикат Q аппроксимационно-устойчивый, представим эффективную PCP-систему для произвольного NP-трудного языка с условием принятия Q и затем применим теорему 17. Кратко PCP-система конструируется следующим образом.

1. Пусть язык $L \in NP$ и $v \in L$. PCP-теорема (теорема 10) дает преобразование такое, что на основании v получается $E3-CNF$-формула $\varphi_{v,L}$ такая, что если $v \in L$, то $\varphi_{v,L}$ выполнима; если $v \notin L$, то $\varphi_{v,L}$ — не более чем c-выполнима для константы $c < 1$.

2. Вводится 2P1R-система с проверяющим и двумя пруверами для проверки того, что формула $\varphi_{v,L}$ выполнима. Вероятность, что невыполнимая формула принимается проверяющим, называется корректностью (soundness). Чтобы уменьшить корректность в 2P1R-системе, проверяющему разрешается задавать одновременно несколько вопросов.

3. Конструируется PCP-система таким образом, что доказательство T будет кодировкой ответов в параллельной 2P1R-системе. Проверяющий использует не более логарифмическое (от $|v|$) число случайных бит и по трем битовым позициям i, j и k в доказательстве принимает решение, что имеет место $Q(T_i, T_j, T_k)$. Число возможных трех кортежей будет полиномиальным от $|v|$. Если T — код приписывания, которое выполняет $\varphi_{v,L}$, то проверяющий принимает решение с вероятностью $1-\varepsilon$.

4. Если вероятность принятия в PCP-системе не менее $\frac{5}{8}(1+\delta)$, где δ — произвольная малая неотрицательная константа, то можно представить стратегию для пруверов в параллельной 2P1R-системе с вероятностью успеха, которая больше, чем корректность системы. Из этого следует, что $\varphi_{v,L}$ выполнима и $v \in L$.

Таким образом, имеем $2^{-3}|Q^{-1}(1)| = 5/8$, и далее, применяя теорему 17, получим, что предикат Q аппроксимационно-устойчивый.

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

Определение 16. 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 17. Для данной функции $A: F_U \to \{-1, 1\}$ определим функцию A_{true}, которая для каждой пары $(f, -f)$ выбирает одну из двух функций. Если выбрана f, то $A_{true}(f) = A(f)$ и $A_{true}(-f) = -A(f)$. Если выбрана функция $-f$, то $A_{true}(f) = -A(-f)$ и $A_{true}(-f) = A(-f)$.

Из этого определения следует, что всегда $A_{true}(f) = -A_{true}(-f)$. Операцию получения A_{true} из A называют сверткой относительно истины (folding over true).

Определение 18. 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.

Операцию получения A_h из A называют установлением необходимого состояния (conditioning).

В дальнейшем будет исследовано несколько PCP-систем на основе анализа Фурье функций A.

Начнем с 3-*CNF*-формулы φ, полученной в результате применения теоремы 10 к произвольному языку L из NP. Таким образом, либо φ — выполнима, либо φ — не более чем c-выполнима для некоторой $c<1$, и отличить эти два случая представляется NP-трудным. Причем, каждая скобка в φ имеет длину точно 3 и каждая переменная участвует точно в пяти скобках.

Базовая 2P1R-система

Ввод. 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 (Verifier). 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 тогда и только тогда, когда значения для x_k согласованы и C_j выполнима.

Лемма 1 [8]. Если $\varphi - c$-выполнима для произвольных P_1 и P_2, то V принимает решение в базовой 2P1R-системе с вероятностью, не большей $\frac{2+c}{3}$.

2P1R-система — *u*-параллельная

Ввод. 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 (Verifier). 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 решение тогда и только тогда, когда значения для x_{k_i} согласованы (совпадают) и C_{j_i} выполнимы для всех $1 \le i \le u$. Используя теорему 11, лемму 1 и правильную стратегию, когда φ — выполнима, получим следующее утверждение.

Лемма 2 [8]. Если φ есть 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 обязывают V принять решение (утвердить) в 2P1R-системе с вероятностью, не большей c_c^u. Если φ — выполнима, то V всегда утверждает решение.

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

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

Определение 19. Стандартно записанное доказательство с параметром u (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 20. SWP(u) — корректное доказательство для формулы φ от n переменных, если существует приписывание x, которое выполняет функция φ так, что A_V — длинный код $x_{/V}$ для произвольного V длиной не более $3u$.

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

Тест $L_2^{\varepsilon}(u)$

Ввод. Записанное доказательство $\mathrm{SWP}(u)$.

Свойство. Проверка того, что корректное доказательство $\mathrm{SWP}(u)$ относится для данной 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 $\mu(y) = -1$ в противном случае, независимо для каждого $y \in \{-1, 1\}^{|W|}$.

5. Формирует $g_2 = f g_1 \mu$, 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 $Q(A_{U,\,true}(f), A_{W,\,h,true}(g_1), A_{W,\,h,true}(g_2)) = 1$.

Лемма 3. Полнота теста $L_2^{\varepsilon}(u)$ не меньше, чем $1-\varepsilon$.

Доказательство полностью аналогично доказательству леммы 5.1 из [8]. В данном случае условие более сильное и полнота не может уменьшится, поэтому она остается не меньшей, чем $1-\varepsilon$.

Рассмотрим теперь корректность. Выражение (5) принимает значение 1, если $Q(x_1, x_2, x_3)$ истинно, и 0 в противном случае. Таким образом, анализируем математическое ожидание (5) со значениями $x_1 = A_{U,\,true}(f), x_2 = A_{W,\,h,true}(g_1)$ и $x_3 = A_{W,\,h,true}(g_2)$. Свертка относительно истины дает $E[A_{U,\,true}(f)] = 0$ для случайной функции f, и таким образом все термы степени 1 в (5) имеют ожидаемое значение 0. Пары (f, g_1) и (f, g_2) является парами независимых функций, поэтому $E[A_{U,\,true}(f) A_{W,\,h,true}(g_i)] = 0$ для $i = 1, 2$. Поскольку тройки (f, g_1, g_2) и $(-f, g_1, -g_2)$ выбираются тестом с одинаковой вероятностью, то $E[A_{W,\,h,true}(g_1) A_{W,\,h,true}(g_2)] = 0$. Отсюда следует, что если тест принимается с вероятностью $\frac{5+\delta}{8}$, то из (5) получим

$$E[A_{U,\,true}(f) A_{W,\,h,true}(g_1) A_{W,\,h,true}(g_2)] = \delta / 3.$$

Отсюда, повторяя рассуждения при доказательстве леммы 5.2 из [8] (в частности, о существовании успешных стратегий для P_1 и P_2 в 2P1R-системе), получим доказательство следующего утверждения.

Лемма 4. Для произвольных $\varepsilon > 0$, $\delta > 0$ допустим, что вероятность того, что проверяющий принимает тест $L_2^{\varepsilon}(u)$, есть $\frac{5+\delta}{8}$. Тогда существует стратегия для P_1 и P_2 в u-параллельной 2P1R-системе, которая дает возможность проверяющему принять решение с вероятностью, не меньшей $4\varepsilon\left(\frac{\delta}{3}\right)^2$.

Согласно лемме 2 имеем корректность 2P1R-системы, равную c_c^u. Положив $4\varepsilon\left(\frac{\delta}{3}\right)^2 \geq c_c^u$, получим, что корректность PCP-проверяющего не больше $\left(5+\frac{3}{2}\sqrt{\frac{c_c^u}{\varepsilon}}\right)/8$, что при достаточно больших u стремится к 5/8. Следует заметить, что $2^{-3}|Q^{-1}(1)|=5/8$. Затем, применяя теорему 17, получим, что Q является аппроксимационно-устойчивым предикатом.

Наследственная аппроксимационная устойчивость следует из того факта, что вставка одного или двух наборов $\alpha=(\alpha_1,\alpha_2,\alpha_3)$ в Q не может преобразовать в нуль коэффициент $c_{\{1,2,3\}}^Q$ в разложении Фурье Q. Для этого следует применить теорему 16.

Замечание 2. Заметим, что $NTW(x_1,x_2,x_3)=Q(\bar{x}_1,\bar{x}_2,\bar{x}_3)$, т.е. согласно определению 2 предикаты NTW и Q имеют одинаковый тип. Таким образом, NTW — наследственно аппроксимационно-устойчивый. Применяя теорему 15, получаем утверждение 2.

Утверждение 2. Для проблемы $Ins-Max-E3CSP-NTW$ (реоптимизация $Max-E3CSP-NTW$) существует полиномиальный приближенный алгоритм с отношением аппроксимации $8/11$. Данное отношение аппроксимации является пороговым.

ЗАКЛЮЧЕНИЕ

Для решения проблемы $Ins-Max-EkCSP-P$ (реоптимизация $Max-EkCSP-P$) с аппроксимационно-устойчивыми предикатами существует полиномиальный пороговый (оптимальный) $\psi(q(P))$-приближенный алгоритм, где $\psi(q(P))=2-\frac{1}{q(P)}=$ $=2-d(P)=2-2^{-k}|P^{-1}(1)|$ ($d(P)$ — пороговое «случайное» отношение аппроксимации P). Заметим, что свойство аппроксимационной устойчивости, по-видимому, более сильное, чем свойство NP-полноты соответствующей проблемы распознавания, поскольку в данном случае эффективное вычисление не может дать ничего другого, чем случайное приписывание значений истинности переменным.

В дальнейшем будут исследованы вопросы существования реоптимизационных полиномиальных пороговых (оптимальных) алгоритмов для обобщенных проблем о выполнимости с другими предикатами, отличными от аппроксимационно-устойчивых.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Bockenhauer H.J., Forlizzi L., Hromkovic J. et al. On the approximability of TSP on local modifications of optimal solved instances // Algorithmic Oper. Res. — 2007. — **2**(2). — P. 83–93.
3. Bockenhauer H.J., Hromkovic J., Momke T., Widmayer P. On the hardness of reoptimization // Proc. of the 34 th 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.
4. Escoffier B., Milanic M., Paschos V. Simple and fast reoptimizations for the Steiner tree problem // Algorithmic Operations Research. — 2009. — **4**(2). — P. 86–94.

5. Archetti C., Bertazzi L., Speranza M.G. Reoptimizing the travelling salesman problem // Networks. — 2003. — **42**(3). — P. 154–159.
6. Archetti C., Bertazzi L., Speranza M.G. Reoptimizing the 0-1 knapsack problem // Discrete Applied Mathematics. — 2010. — **158** (17). — P. 1879–1887.
7. Ausiello G., Bonifaci V., Escoffier B. Complexity and approximation in reoptimization // Computability in Context: Computation and Logic in the Real World (Eds. S. Barry Cooper and Andrea Sorbi). — 2011. — London: Imperial College Press. — P. 101–130.
8. Hastad J. Some optimal inapproximability results // J. of the ACM. — 2001. — **48**, N 4. — P. 798–859.
9. Hastad J. Complexity theory, proofs and approximation // European Congress of Mathematics (Ed. A. Laptev, European Mathematical Society).— Stockholm, Sweden, 2005.
10. Hastad J. On the efficient approximability of constraint satisfaction problems // Surveys in Combinatorics 2007. — London Mathematical Society Lecture Notes Series (Eds. A. Hilton and J. Talbot). — Cambridge: University Press. — 2007. — **346**. — P. 201–222.
11. Feige U. A threshold of ln *n* for approximating set cover // J. of the ACM. — 1998. — **45**, N 4. — P. 634–652.
12. Arora S., Lund C., Motwani R., Sudan M., Szegedy M. Proof verification and intractability of approximation problems // J. of the ACM. — 1998. — **45**, N 3. — P. 501–555.
13. Goldreich O., Goldwasser S., Ron D. Property testing and its connection to learning and approximation abstract // J. of the ACM. — 1998. — **45**, N 4. — P. 653–750.
14. Goldreich O., Sudan M. Locally testable codes and PCPs of almost-linear length // J. of the ACM. — 2006. — **53**, N 4. — P. 558–655.
15. Goemans M.X., Williamson D.P. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming // J. of the ACM. — 1995. — **42**. — P. 1115–1145.
16. Hast G. Beating a random assignment. — Doctoral Thesis. — Royal Institute of Technology. — Stockholm, Sweden, 2005.
17. Zwick U. Approximation algorithms for constraint satisfaction problems involving at most three variables per constraint // Proceedings of the 9-th Annual ACM — SIAM Symposium on Discrete Algorithms, 1998. — P. 551–560.
18. O'Donnel R. Some topics in analysis of Boolean functions // Electronic Colloquium on Computational Complexity, 2008. — Report No. 55.
19. Khot S. Inapproximability of NP-complete problems, discrete Fourier analysis, and geometry // Proceedings of the International Congress of Mathematicians. — 2010. — Hyderabad, India.
20. Raz R. A parallel repetition theorem // SIAM J. on Computing. — 1998. — **27**, N 3. — P. 763–803.
21. Vazirani V.V. Approximation algorithms. — Berlin: Springer, 2001. — 380 p.
22. Михайлюк В.А. Общий подход к оценке сложности постоптимального анализа дискретных задач оптимизации // Кибернетика и системный анализ. — 2010. — **46**, № 2. — С. 134–141.
23. Михайлюк В.А. Реоптимизация задачи о покрытии множествами // Там же. — 2010. — **46**, № 6. — С. 27–31.

Поступила 12.05.2011