Московский физико-технический
институт

Кафедра дискретной математики

$\bigoplus \notin \mathbf{AC}^0$

Работа студентки 3 курса, гр. 294
Ичаловой Дианы

Москва
2014 г.

1 Введение

В 1970-х годах важным вопросом схемной сложности был вопрос получения нижних оценок на ресурсы, требуемые для вычисления различных функций. Считалось, что это поможет решить знаменитую проблему, доказав, что $P \neq NP$. В частности, рассматривался вопрос, какие функции можно выразить схемами из $\mathbf{AC}^0$. Ученые пытались найти функции, которые не лежат в классе схем с небольшой глубиной. Только в начале 80-х годов было доказано, что даже $\texttt{PARITY} \notin \mathbf{AC}^0$. Этот результат был получен в 1981 году [Furst, Saxe, Sipser] и независимо [Ajtai] в 1983 году. Впервые экспоненциальная оценка на PARITY была получена [Yao] в 1985 году. В 1987 году Хостад [Håstad] сформулировал и доказал лемму о переключении, которая позволила получить более точные нижние оценки для PARITY и для других функций, например, MAJORITY.

Схемы с небольшой глубиной имеют также важное прикладное значение в теории параллельных вычислений. Они имеют отношение к PRAM *(parallel random-access machine)*. Поэтому, получая нижние оценки на глубину схем, можно получить нижнюю оценку времени вычисления этой функции на PRAM.

2 Определения

Определение 1. Для всех $n \in \mathbb{N}$, *булевой схемой с n входами и одним выходом* будем называть ориентированный ациклический граф с n истоками (вершинами без входящих ребер), помеченными переменными из множества $\{x_1, ..., x_n\}$, и одним стоком (вершиной без исходящих ребер). Остальные вершины, помеченные символами $\vee, \wedge, \neg$, будем называть *функциональными элементами*. Вершины, помеченные $\vee$ и $\wedge$, могут иметь произвольное число входящих ребер, а вершины, помеченные $\neg$, имеют ровно одно входящее ребро. Каждый элемент вычисляет булеву функцию очевидным образом.
Размер схемы — это число элементов в ней. *Глубина элемента* — это максимальное число элементов на пути от данного элемента до входа. *Глубина схемы* — глубина выхода.

Везде далее, для простоты изложения, будем считать, что входными элементами являются не только сами переменные, но и их отрицания.

Также, применяя закон де Моргана, можно построить эквивалентную схему, используя только операции $\vee$ и $\neg$:

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n = \overline{\overline{A_1} \vee \overline{A_2} \vee \ldots \vee \overline{A_n}}$$

Тогда размером схемы будем называть число элементов $\vee$, а глубиной элемента — максимальное число элементов $\vee$ на пути от данного элемента до входа.

Определение 2. Язык L *разрешим семейством булевых схем* $\{C_n\}$, если для всех $x \in \{0,1\}^n$,

$$x \in L \Leftrightarrow C_n(x) = 1$$

Определение 3. Язык L лежит в сложностном классе $\mathbf{AC}^0$, если он разрешим семейством булевых схем $\{C_n\}$, где C_n имеет полиномиальный размер и константную глубину.

Определение 4. $\bigoplus = \{x \in \{0,1\}^* : \text{в } x \text{ нечетное число единиц}\}$

Определение 5. *Ограничением* набора булевых переменных $\{x_i : i \in I\}$ называется отображение $\rho : I \to \{0, 1, *\}$. Результат применения ограничения к булевой функции f есть булева функция $f|_\rho$, определяемая как результат подстановки $\rho(i)$ вместо x_i для всех i таких, что $\rho(i) \neq *$. Переменная x_i называется *неопределенной*, если $\rho(i) = *$.

Множество всех ограничений n переменных с ровно ℓ неопределенными переменными будем обозначать $\mathcal{R}_n^\ell$.

На множестве всех ограничений n переменных естественным образом определена операция произведения непересекающихся ограничений.

Будем считать, что после применения ограничения к ДНФ-формуле, формула упрощается путем удаления обнуленных конъюнктов.

Определение 6. *Дерево принятия решений* $T(F)$ для формулы F в ДНФ определяется индуктивно следующим образом:

1. Если F — это константный 0 или 1 (F не содержит термов или первый терм пустой, соответственно), тогда $T(F)$ состоит из одного листа, помеченного соответствующей константой.

2. Если $F = C_1 \vee F'$, где терм C_1 не пуст, то пусть K — множество переменных в C_1. Дерево $T(F)$ начинается с полного бинарного дерева для K, которое запрашивает переменные K в порядке увеличения их индексов. Каждый лист v_σ соответствует ограничению σ, которое присваивает переменным из K значения в соответствии с путем в дереве от корня до v_σ. Для каждого σ заменим лист v_σ на дерево принятия решений для $T(F|_\sigma)$.
   Отметим, что для единственного σ, удовлетворяющего терм C_1, лист v_σ станет листом, помеченным 1, все остальные v_σ будут заменены на поддеревья $T(F|_\sigma) = T(F'|_\sigma)$.

Высоту полученного дерева будем обозначать $|T(F)|$.

3 Лемма Хостада о переключении

Данная лемма и ее многочисленные вариации являются мощным иструментом для доказательства нижних оценок размеров схем для различных функций.

В оригинальном доказательстве [3] Йохан Хостад использовал условные вероятности. Позднее, более простое доказательство было предложено Александром Разборовым в его работе [4], оно использует понятия минтермов и макстермов КНФ и ДНФ. Доказательство, приведенное ниже, повторяет [2], которое оперирует более наглядным деревом принятия решений.

Прежде чем формулировать теорему, докажем одну несложную лемму.

Определение 7. Определим $stars(r, s)$ как множество всех последовательностей $\beta = (\beta_1, \ldots, \beta_k)$ произвольной длины таких, что выполнены условия:

1. Для всех j: $\beta_j \in \{-, *\}^r \setminus \{-\}^r$
2. Суммарное число $*$ во всех β_j равно s.

Лемма 1.

$$|stars(r, s)| < \left(\frac{r}{\ln 2}\right)^s$$

Доказательство. Доказательство индукцией по s, что $|stars(r,s)| \leq \gamma^s$ для γ, удовлетворяющего равенству $(1+\frac{1}{\gamma})^r = 2$. Прежде чем проводить индукцию, найдем отсюда оценку на γ:

$$2^{\frac{1}{r}} = 1 + \frac{1}{\gamma} < e^{\frac{1}{\gamma}},$$

где последнее неравенство следует из формулы Тейлора. Откуда

$$e^{\frac{\ln 2}{r}} < e^{\frac{1}{\gamma}},$$

$$\gamma < \frac{r}{\ln 2}.$$

База $s = 0$

$|stars(r,0)| = 1 \leq \gamma^0$ ($stars(r,0)$ содержит пустую строку).

Предположение индукции

Предположим, что для всех $s < t$ $|stars(r,s)| \leq \gamma^s$.

Шаг индукции

Докажем для $s = t$, что $|stars(r,s)| \leq \gamma^s$. Рассмотрим первый элемент последовательности $\beta - \beta_1$. Пусть он содержитk $*$. Тогда последовательность β без элемента β_1 лежит в множестве $stars(r, s-k)$. Так как β_1 можно выбрать C_r^k способами, то

$$|stars(r,s)| = \sum_{k=1}^{\min(r,s)} C_r^k |stars(r,s-k)| \leq$$

$$\leq \sum_{k=1}^{r} C_r^k \gamma^{s-k} = \gamma^s \sum_{k=1}^{r} C_r^k \left(\frac{1}{\gamma}\right)^k =$$

$$= \gamma^s \left[\left(1+\frac{1}{\gamma}\right)^r - 1\right] = \gamma^s[2-1] = \gamma^s.$$

Из этого и из определения γ следует, что

$$|stars(r,s)| \leq \gamma^s < \left(\frac{r}{\ln 2}\right)^s$$

□

Теорема 2 (Håstad's switching lemma)**.** *Пусть F — r–ДНФ формула от n переменных, $Bad(F,s)$ — множество ограничений $\rho \in \mathcal{R}_n^\ell$, для которых $|T(F|_\rho)| \geq s$. Тогда для любого $s \geq 0$, $\ell = pn$ и $p \leq 1/7$*

$$\frac{|Bad(F,s)|}{|\mathcal{R}_n^\ell|} < (7pr)^s.$$

Доказательство. Лемма доказывается построением биекции: $Bad(F,s) \to \mathcal{R}_n^{\ell-s} \times stars(r,s) \times 2^s$.

Инъективность

Докажем инъективность, предъявив для каждого ограничения $\rho \in \mathcal{R}_n^\ell$ элемент из $\mathcal{R}_n^{\ell-s} \times stars(r,s) \times 2^s$ однозначным образом.

Зафиксируем формулу $F = \bigvee_{i=1}^{H} C_i$, где C_i — некоторые дизъюнкты. Обозначим $\{x_1, \ldots, x_n\}$ — множество переменных F. Пусть $\rho \in Bad(F,s)$ и пусть π — некоторый путь в дереве $T(F|_\rho)$, длина которого больше или равна s. Если π присваивает значения больше, чем s переменным, то обрежем π до первых s переменных.

Рассмотрим первый терм C_{ν_1}, который не обнуляется под действием ρ. Такой обязательно найдется, так как дерево принятия решений $T(F|_\rho)$ не вырождается в лист. Пусть K — множество переменных, содержащихся в $C_{\nu_1}|_\rho$. Определим σ_1 — ограничение переменных K, которое обращает терм $C_{\nu_1}|_\rho$ в 1 (σ_1 определена единственным образом). Определим

$$\pi_1(i) = \begin{cases} \pi(i), \text{ если } x_i \in K, \\ *, \text{ иначе} \end{cases}$$

Тогда есть 2 случая:

1. $\pi_1 \neq \pi$. Тогда из построения дерева принятия решений и ограничения π следует, что π_1 определяет все переменные в K. Очевидно, $\pi_1 \neq \sigma_1$, так как иначе $C_{\nu_1}|_{\rho\pi_1} = 1$ и $T(F|_{\rho\pi_1})$ вырождается в лист, чего не может быть так как $\pi_1 \neq \pi$. Следовательно, $C_{\nu_1}|_{\rho\pi_1} = 0$.

2. $\pi_1 = \pi$. Обрежем σ_1 так, чтобы в нем содержались лишь переменные, которые содержатся в π_1. Тогда $C_{\nu_1}|_{\rho\sigma_1}$ не обращается в ноль.

Определим $\beta_1 \in \{-,*\}^r \setminus \{-\}^r$: j-ая компонента β_1 равна $*$ тогда и только тогда, когда σ_1 определяет j-ую переменную в C_{ν_1}. Таким образом, зная C_{ν_1} и β_1, можно восстановить σ_1 следующим образом: рассмотреть только те переменные $x_{\nu_{1j}}$, для которых $\beta_1^j = *$ и если $x_{\nu_{1j}}$ входит без отрицания в конъюнкт C_{ν_1}, то положить $\sigma(\nu_{1j}) = 1$ и 0 иначе.

Если $\pi_1 \neq \pi$, то рассмотрим $\pi \backslash \pi_1$, которое является корректным ограничением в дереве $T(F|_{\rho\pi_1})$ и повторим рассуждения выше для $\widetilde{\pi} = \pi \backslash \pi_1$, $\widetilde{\rho} = \rho\pi_1$ и рассматривая первый терм C_{ν_2} не обнуляющийся под действием $\widetilde{\rho}$. Таким образом мы получаем, что $\pi = \pi_1\pi_2 \ldots \pi_k$, $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$, $\beta = (\beta_1, \beta_2, \ldots, \beta_k)$.

Определим вектор $\delta \in \{0,1\}^s$, который показывает, равны ли соответствующие значения переменных, определенные ограничениями π и σ.

Итак, каждому ρ мы поставили в соответствие тройку $< \rho\sigma, \beta, \delta >$, где $\rho\sigma \in \mathcal{R}_n^{\ell-s}$, $\beta \in stars(r,s)$, $\delta \in \{0,1\}^s$.

Сюръективность

Покажем, как по тройке $< \rho\sigma = \rho\sigma_1\sigma_2 \ldots \sigma_k, \beta = (\beta_1, \beta_2, \ldots, \beta_k), \delta >$ восстановить ρ.

Будем восстанавливать ρ итеративно. Пусть на i-ом шаге уже восстановлены $\pi_1, \ldots, \pi_{i-1}$, $\sigma_1, \ldots, \sigma_{i-1}$ и построено $\rho\pi_1 \ldots \pi_{i-1}\sigma_i \ldots \sigma_k$.

Заметим, что для всех $i < k$ $C_{\nu_i}|_{\rho\pi_1 \ldots \pi_{i-1}\sigma_i\sigma_{i+1}\ldots\sigma_k} = 1$ и $C_j|_{\rho\pi_1 \ldots \pi_{i-1}\sigma_i\sigma_{i+1}\ldots\sigma_k} = 0$ для всех $j < \nu_i$.

Если же $i = k$, то $C_{\nu_i}|_{\rho\pi_1 \ldots \pi_{i-1}\sigma_i\sigma_{i+1}\ldots\sigma_k} \neq 0$ и $C_j|_{\rho\pi_1 \ldots \pi_{i-1}\sigma_i\sigma_{i+1}\ldots\sigma_k} = 0$. Тогда можно восстановить C_{ν_i} как индекс первого терма, который не обнуляется под действием $\rho\pi_1 \ldots \pi_{i-1}\sigma_i \ldots \sigma_k$. Как было описано выше по C_{ν_i} и β_i мы можем восстановить σ_i. По σ_i и δ восстанавливаем π_i. Зная переменные, которые присваивает σ_i, мы можем из $\rho\pi_1 \ldots \pi_{i-1}\sigma_i \ldots \sigma_k$ построить $\rho\pi_1 \ldots \pi_{i-1}\pi_i \ldots \sigma_k$. В конце концов, зная все π_i и $\rho\pi_1 \ldots \pi_{i-1}\pi_i \ldots \pi_k$ можно восстановить ρ.

Получение верхней оценки

Очевидно, что $\mathcal{R}_n^\ell = C_n^\ell 2^{n-\ell}$. (Выбираем ℓ неопределенных переменных, остальные переменные полагаем 0 или 1.) Тогда

$$\frac{|\mathcal{R}_n^{\ell-s}|}{|\mathcal{R}_n^\ell|} = \frac{n!}{(\ell-s)!(n-\ell+s)!} \cdot \frac{\ell!(n-\ell)!}{n!} \cdot \frac{2^{n-\ell+s}}{2^{n-\ell}} =$$
$$= \frac{\ell(\ell-1)\ldots(\ell-s+1)}{(n-\ell+s)(n-\ell+s-1)(n-\ell+1)} \cdot 2^s \leq \frac{\ell^s}{(n-\ell)^s} \cdot 2^s.$$

Применяя лемму 1, получаем

$$\frac{|Bad(F,s)|}{|\mathcal{R}_n^\ell|} = \frac{|\mathcal{R}_n^{\ell-s}|}{|\mathcal{R}_n^\ell|} \cdot |stars(r,s)| \cdot 2^s <$$
$$< \frac{(2\ell)^s}{(n-\ell)^s} \cdot \left(\frac{r}{\ln 2}\right)^s \cdot 2^s = \left(\frac{4\ell r}{(n-\ell)\ln 2}\right)^s.$$

Учитывая, что $\ell = pn$ и $p < 1/7$, окончательно получаем, что

$$\frac{|Bad(F,s)|}{|\mathcal{R}_n^\ell|} < (7pr)^s.$$

□

4 $\bigoplus \notin \mathbf{AC}^0$

Доказательство использует вероятностный метод: рассматриваются случайные ограничения и доказывается, что некоторое «хорошее» ограничение существует.

Лемма 3. Пусть C — булева схема и $|C|$ — её размер, а d — глубина. Определим $n_i = \dfrac{n}{14}\dfrac{1}{(14\log_2|C|)^{i-1}}$ для всех $1 \le i \le d$.
Тогда если $n_i \ge \log_2|C|$, то существует ограничение $\rho_i \in \mathcal{R}_n^{n_i}$ такое, что для любого функционального элемента g на глубине не больше i в C, $g|_{\rho_i}$ представимо в виде дерева принятия решений высоты не больше $\log_2|C|$.

Доказательство. Напомним, что входными элементами булевой схемы являются переменные и их отрицания, в схеме используются только операции $\vee$ и $\neg$. В подсчете глубины схемы элементы $\neg$ не учитываются.

Достаточно доказать теорему для элементов $g = \vee$, так как $\neg g$ имеет такое же дерево принятия решений, как g, но с инвертированными значениями на листьях.

Докажем теорему индукцией по глубине d схемы C.

База $d = 1$, $n_1 = \frac{n}{14}$

Входами элемента $\vee$ на глубине 1 являются переменные и их отрицания, следовательно, каждый такой элемент g задает 1-ДНФ формулу.

Положим $p = 1/14$, $n_1 = np$. По лемме о переключении число ограничений $\rho \in \mathcal{R}_n^{n_1}$ таких, что $|T(g|_\rho)| \ge \log_2|C|$ строго меньше $(7p\cdot 1)^{\log_2|C|} = (1/2)^{\log_2|C|} = 1/|C|$. Так как число элементов на глубине 1 не может превосходить общего числа элементов |C|, то найдется такое ограничение $\rho_1 \in \mathcal{R}_n^{n_1}$, что для всех элементов g на глубине 1 $|T(g|_{\rho_1})| \le \log_2|C|$.

Предположение индукции

Предположим, что для всех $d < i$ существует ограничение $\rho_d \in \mathcal{R}_n^{n_d}$ такое, что для всех элементов g на глубине не больше чем d, $|T(g|_{\rho_d})| \le \log_2|C|$.

Шаг индукции

Докажем утверждение для $d = i$.
По предположению индукции существует $\rho_{i-1} \in \mathcal{R}_n^{n_{i-1}}$ такое, что для всех элементов g на глубине не больше чем $i-1$, $|T(g|_{\rho_{i-1}})| \le \log_2|C|$. Тогда $g|_{\rho_{i-1}}$ можно представить в виде $(\log_2|C|)$-ДНФ формулы. Рассмотрим элемент $g = \vee$ на глубине i и применим ограничение ρ_i. Так как все

входы этого элемента могут быть представлены в виде $(\log_2 |C|)$-ДНФ формул, то и g представима в виде $(\log_2 |C|)$-ДНФ формулы.

Положим $p = n_i/n_{i-1} = 1/(\log_2 |C|)$. По лемме о переключении число ограничений $\pi \in \mathcal{R}_{n_{i-1}}^{n_i}$ таких, что $|T((g|_{\rho_{i-1}})|_\pi)| \geq \log_2 |C|$ строго меньше $(7p \log_2 |C|)^{\log_2 |C|} = (1/2)^{\log_2 |C|} = 1/|C|$. Так как на уровне i не больше, чем $|C|$ элементов, то найдется такое ограничение π, что $|T(g|_{\rho_{i-1}\pi})| \leq \log_2 |C|$. Полагая $\rho_i = \rho_{i-1}\pi \in \mathcal{R}_n^{n_i}$, получаем требуемое ограничение.

□

Теорема 4.

$$\bigoplus \notin \mathbf{AC}^0$$

Доказательство. Докажем, что любая схема C константной глубины, вычисляющая $\bigoplus$ имеет размер $|C| \geq 2^{\frac{1}{14} n^{\frac{1}{d}}}$. А так как $\mathbf{AC}^0$ содержит схемы с полиномиальным размером, то отсюда будет следовать условие теоремы.

Рассмотрим некоторую схему C глубины d, не зависящей от длины входа n. Заметим, что для любого ограничения $\rho \in \mathcal{R}_n^\ell$ глубина каждой ветви дерева принятия решений для $\bigoplus$ равна ℓ. Следовательно, $|T(g|_\rho)| = \ell$.

Применим ограничение ρ_d из предыдущей леммы к схеме C. Тогда для любого элемента g (и в частности для выходного) $|T(g|_{\rho_d})| \leq \log_2 |C|$. Но $|T(g|_{\rho_d})| = n_d = \dfrac{n}{14^d \log_2^{d-1} |C|}$.
Отсюда получаем неравенство:

$$\frac{n}{14^d \log_2^{d-1} |C|} \leq \log_2 |C|,$$

$$\log_2^d |C| \geq \frac{n}{14^d},$$

$$|C| \geq 2^{\frac{1}{14} n^{\frac{1}{d}}}.$$

□

Список литературы

[1] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[2] Paul Beame. A Switching Lemma Primer. April 1994.

[3] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *RANDOMNESS AND COMPUTATION*, pages 6–20. JAI Press, 1989.

[4] Alexander A. Razborov. Bounded arithmetic and lower bounds in boolean complexity. In *Feasible Mathematics II*, pages 344–386. Birkhauser, 1993.