Лекция 13. Вероятностный метод. Схемы из функциональных элементов. Схемы ограниченной глубины и сложности. Формулы. Максимальные антицепи

Лектор — Нагорный Александр Степанович
anagorny@list.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Схемы ограниченной глубины

Известно, что счётчик чётности сложно реализовать с малой глубиной в базисе из функциональных элементов И, ИЛИ, НЕ. Оказывается, что даже если в этот базис добавить элемент-счётчик чётности, всё же существуют некоторые относительно простые функции, которые сложно вычислить. Такой результат был впервые доказан Разборовым **[2]**. Этот метод был изменён и усилен Смоленским **[3]**.

Для целого $k \geq 2$ пусть $\mathrm{Mod}_k(x_1, x_2, \dots, x_n)$ есть булева функция, которая принимает значение 1 тогда и только тогда, когда $\sum x_i \not\equiv 0 \pmod{k}$. Смоленский показал, что для любых двух степеней p и q различных простых чисел функция Mod_p не может быть вычислена ограниченной по глубине схемой полиномиальной сложности в базисе из функциональных элементов И, ИЛИ, НЕ и Mod_q.

Схемы ограниченной глубины

Далее приводится частный случай этого результата, в котором $q = 3$ и $p = 2$.

Пусть C – произвольная схема глубины d и сложности s, состоящая из функциональных элементов И, ИЛИ, НЕ и Mod_q. Важный факт, доказанный Разборовым, заключается в том, что функция, которую реализует C, может быть довольно хорошо приближена (в зависимости от d и s) полиномом относительно малой степени над полем $GF(3)$.

Схемы ограниченной глубины

Теорема 2 ([2] Разборов, 1987). Для любой схемы C глубины d и сложности s от n булевых переменных, построенной из элементов И, ИЛИ, НЕ и Mod_3, и для любого целого ℓ существует полином $P = P(x_1, \dots, x_n)$ степени не больше $(2\ell)^d$ над полем $GF(3)$, значение которого совпадает с функцией реализуемой схемой C, не менее чем на $2^n(1 - s/2^\ell)$ входных наборах.

Доказательство. Применим вероятностный метод. Каждый элемент схемы C заменим приближающей полиномиальной операцией, согласно следующим правилам, гарантирующим, что в каждой вершине новой схемы мы вычисляем полином над полем $GF(3)$, принимающий только значения 0 и 1 (если на входы подаются только 0 и 1).

Доказательство (продолжение).

1. Каждый элемент-отрицание $\overline{y}$ заменяется полиномиальным элементом $(1 - y)$.
2. Каждый элемент $\mathrm{Mod}_3(y_1, y_2, \dots, y_m)$ заменяется полиномиальным элементом $(y_1 + y_2 + \cdots + y_m)^2$.

Правило для замены элементов ИЛИ и И немного сложнее. Заметим, что в двух предыдущих случаях 1. и 2. не было приближённых вычислений; новые элементы вычисляют в точности то же, что и старые, для всех возможных значений булевых переменных. В принципе, это может быть сделано и здесь.

Схемы ограниченной глубины

Доказательство (продолжение).
Элемент И $y_1 \wedge y_2 \wedge \ldots \wedge y_m$ следует просто заменить произведением $y_1 y_2 \ldots y_m$. Тогда элемент ИЛИ $y_1 \vee y_2 \vee \cdots \vee y_m$ может быть вычислен по правилам де Моргана. Поскольку $y_1 \vee y_2 \vee \cdots \vee y_m = \overline{(\bar{y}_1 \wedge \bar{y}_2 \wedge \cdots \wedge \bar{y}_m)}$ и $\bar{y}$ реализуется как $(1 - y)$, это даёт представление

$$1 - (1 - y_1)(1 - y_2) \ldots (1 - y_m). \qquad (1)$$

Проблема в том, что эта процедура слишком сильно увеличила бы степень наших полиномов. Поступим немного хитрее. Пусть ℓ – целое число, которое мы определим позже. По элементу ИЛИ $y_1 \vee y_2 \vee \cdots \vee y_m$ мы выбираем ℓ случайных подмножеств $I_1, \ldots, I_\ell$ множества $\{1, \ldots, m\}$, где для каждого $1 \leq i \leq \ell$ и для каждого $1 \leq j \leq m$ независимо $\Pr[j \in I_i] = 1/2$.

Схемы ограниченной глубины

Доказательство (продолжение). Заметим, что для любого фиксированного i, $1 \le i \le \ell$, сумма $\left(\sum_{j \in I_i} y_j\right)^2$ над полем $GF(3)$ обязательно равна 0, если $y_1 \vee \cdots \vee y_m = 0$, и равна 1 с вероятностью не меньше $\frac{1}{2}$, если $y_1 \vee \cdots \vee y_m = 1$.

Таким образом, если мы вычислим значение ИЛИ от ℓ выражений $\left(\sum_{j \in I_i} y_j\right)^2, 1 \le i \le \ell$, то эта функция равна 0 при $y_1 \vee \cdots \vee y_m = 0$, и равна 1 с вероятностью не меньше $1 - (1/2)^\ell$, если $y_1 \vee \cdots \vee y_m = 1$. Тогда мы вычислим ИЛИ и запишем результат в виде полинома, как это было сделано в формуле (1). Это даёт

$$1 - \prod_{i=1}^{\ell} \left(1 - \left(\sum_{j \in I_i} y_j\right)^2\right). \qquad (2)$$

Схемы ограниченной глубины

Доказательство (продолжение). Следовательно, в нашей новой схеме мы заменим каждый элемент ИЛИ на приближающий полиномиальный элемент вида (2). Получив приближение для элемента ИЛИ, мы можем получить соответствующее приближение и для элемента И, применяя правила де Моргана. Так как $y_1 \wedge \ldots \wedge y_m = \overline{(\bar{y}_1 \vee \cdots \vee \bar{y}_m)}$, мы заменяем каждый элемент И вида $y_1 \wedge \ldots \wedge y_m$ на

$$\prod_{i=1}^{\ell}\left(1-\left(\sum_{j\in I_i}(1-y_j)\right)^2\right). \qquad (3)$$

Заметим, что степени полиномов (2) и (3) не превосходят 2ℓ.

Схемы ограниченной глубины

Доказательство (окончание). В исходной схеме C глубины d и сложности s мы теперь можем заменить все её элементы нашими приближёнными полиномиальными элементами и получить новую схему CP, которая зависит от всех случайных выборов, сделанных при каждой замене каждого элемента И/ИЛИ. Новая схема CP вычисляет полином $P(x_1, \dots, x_n)$ степени не больше $(2\ell)^d$. Более того, для любых фиксированных булевых значений $x_1, \dots, x_n$ вероятность того, что все новые элементы вычисляют то же, что и соответствующие элементы в C, не меньше $1 - s/2^\ell$. Следовательно, ожидаемое число входных значений, на которых $P(x_1, \dots, x_n)$ совпадает с выходными значениями C, не меньше $2^n(1 - s/2^\ell)$ Таким образом, теорема доказана . ■

Схемы ограниченной глубины

Чтобы применить теорему 1 для получения нижних оценок сложности любой схемы описанного выше типа, нам потребуется следующий дополнительный комбинаторный результат.

Лемма 1. Не существует полинома $P = P(x_1, \dots, x_n)$ над полем $GF(3)$ степени не больше $\sqrt{n}$, равного счётчику чётности от $x_1, \dots, x_n$ на множестве S из не менее чем $0.9 \cdot 2^n$ различных булевых векторов $(x_1, \dots, x_n)$.

Доказательство. Предположим, что это не так. Пусть существует полином $P(x_1, \dots, x_n)$, равный $x_1 \oplus \dots \oplus x_n$ для всех $(x_1, \dots, x_n) \in S$, где $S \subset \{0,1\}^n$, $|S| \geq 0.9 \cdot 2^n$, степень которого не больше $\sqrt{n}$.

Доказательство (продолжение).
Определим вспомогательный полином $Q = Q(y_1, \dots, y_n)$ как $Q = Q(y_1, \dots, y_n) = P(y_1 + 2, \dots, y_n + 2) - 2$ и множество T как $T = \{(y_1, \dots, y_n) \in \{-1,1\}^n : (y_1 + 2, \dots, y_n + 2) \in S\}$, где все суммы берутся по модулю 3. Ясно, что степень многочлена Q не превосходит $\sqrt{n}$, и $Q(y_1, \dots, y_n) = \prod_{i=1}^{n} y_i$ для всех $(y_1, \dots, y_n) \in T$. Пусть теперь $G = G(y_1, \dots, y_n) : T \to GF(3)$ есть произвольная функция. Расширим её произвольным образом до функции из $\left(GF(3)\right)^n \to GF(3)$ и запишем эту функцию как полином от n переменных. Ясно, что любая функция из $\left(GF(3)\right)^n \to GF(3)$ является полиномом, так как может быть представлена в виде линейной комбинации функций вида $\prod_{i=1}^{n}(y_i - \varepsilon_i)(y_i - \varepsilon_i - 1)$, где $\varepsilon_i \in GF(3)$.

Схемы ограниченной глубины

Доказательство (окончание). Заменим каждое вхождение y_i^2 в этом полиноме на 1, чтобы получить полилинейный полином $\tilde{G}$, совпадающий с G на T. Теперь заменим каждый одночлен $\prod_{i\in U} y_i$, где $|U| > \frac{n}{2} + \frac{\sqrt{n}}{2}$, на $\prod_{i\in U} y_i \cdot Q(y_1, \dots, y_n)$, и этот новый полином заменим на полилинейный полином $\tilde{\tilde{G}}$, снова заменяя каждое y_i^2 на 1. Так как для $y_i \in \{\pm 1\}$, $\prod_{i\notin U} y_i \cdot \prod_{i=1}^{n} y_i = \prod_{i\in U} y_i$, то $\tilde{\tilde{G}}$ равно G на T, и его степень не превосходит $\frac{n}{2} + \frac{\sqrt{n}}{2}$. Тем не менее, число возможных $\tilde{\tilde{G}}$ равно $3^{\sum_{i=0}^{\left\lfloor \frac{n}{2}+\frac{\sqrt{n}}{2} \right\rfloor} \binom{n}{i}} < 3^{0.88\cdot 2^n}$, в то время как число возможных G равно $3^{|T|} \geq 3^{0.9\cdot 2^n}$. Это невозможно, а значит верно утверждение леммы. ■

Схемы ограниченной глубины

Следствие 1. Не существует схемы глубины d и сложности $s \leq \frac{1}{10} \cdot 2^{\frac{1}{2}n^{1/2d}}$, реализующей счётчик чётности от $x_1, \dots, x_n$, состоящей из элементов И, ИЛИ, НЕ и Mod_3.

Доказательство. Предположим, что это не так, и пусть C – такая схема. Положим $\ell = \frac{1}{2}n^{1/2d}$. По теореме 1 существует полином $P = P(x_1, \dots, x_n)$ над полем $GF(3)$, степень которого не превосходит $(2\ell)^d = \sqrt{n}$, равный счётчику чётности от $x_1, \dots, x_n$ не менее чем на $2^n\left(1 - \frac{s}{2^{\frac{1}{2}n^{1/2d}}}\right) \geq 0.9 \cdot 2^n$ входных значениях.

Это противоречит лемме 1, что и завершает доказательство. ■

Формулы

Под **формулой** мы здесь будем понимать схему, в которой число выходов каждого элемента не превосходит 1. В отличие от случая со схемами, есть сверхлинейные нижние оценки минимальной сложности формул, вычисляющих различные явные NP-функции над полным двоичным базисом. Для булевой функции $f = f(x_1, \dots, x_n)$ обозначим через $L(f)$ минимальное число элементов И и ИЛИ в формуле, использующей элементы И, ИЛИ и НЕ и вычисляющей f. В силу правил де Моргана, мы можем считать, что все элементы НЕ входят в первый уровень этой формулы.

Мы рассмотрим здесь простой результат Субботовской **[4]**, который заключается в том, что $L(f) \geq \Omega(n^{3/2})$ для счётчика чётности $f = x_1 \oplus \dots \oplus x_n$.

Формулы

Эта оценка была позднее улучшена Храпченко **[5]** до $L(f) = n^2 - 1$. Тем не менее, бы представляем здесь лишь более слабую нижнюю оценку $\Omega(n^{3/2})$ не только потому, что это позволит ещё раз продемонстрировать силу относительно простых вероятностных приёмов, но и потому, что модификация этого доказательства позволила Андрееву **[6]** получить нижнюю оценку $\Omega(n^{5/2}/(\log n)^{O(1)})$ на $L(g)$ для другой функции $g = g(x_1, \dots, x_n)$. Хостад **[7]** позднее улучшил и эту нижнюю оценку до $\Omega\left(n^{3-o(1)}\right)$. В настоящее время это лучшая из известных нижних оценок сложности формулы для NP-функции от n переменных над полным базисом.

Метод Субботовской основан на случайных ограничениях, аналогичных использованным ранее.

Формулы

Теорема 3 ([4] Субботовская, 1961). Пусть $f = f(x_1, \dots, x_n)$ – булева функция от переменных, не являющаяся атомом. Тогда существуют i, $1 \le i \le n$, и $\varepsilon \in \{0,1\}$, такие, что для функции $g = f(x_1, \dots, x_{i-1}, \varepsilon, x_{i+1}, \dots, x_n)$ от $n-1$ переменных, полученной из заменой $x_i = \varepsilon$, верно следующее неравенство:

$$(L(g)+1) \le \left(1 - \frac{3}{2n}\right)(L(f)+1) \le \left(1 - \frac{1}{n}\right)^{3/2}(L(f)+1).$$

Доказательство. Зафиксируем формулу F, вычисляющую функцию f, с $l = L(f)$ элементами И и ИЛИ. Формула F может быть представлена как двоичное дерево, каждый из $l+1$ листьев которого помечен атомом x_i или $\overline{x}_i$. Случайно выберем переменную x_i, $1 \le i \le n$, согласно равномерному распределению, и присвоим ей случайное двоичное значение $\varepsilon \in \{0,1\}$.

Формулы

Доказательство (продолжение). Когда мы заменяем значения ε и $1-\varepsilon$ на x_i и $\overline{x}_i$, соответственно, число листьев F уменьшается; математическое ожидание числа листьев, удаляемых таким образом, равно $(l+1)/n$. Однако, может произойти дальнейшее сокращение. В самом деле, предположим, что лист помечен символом x_i и питает, допустим, элемент И $x_i \wedge H$ в F. Мы можем считать, что переменная x_i не входит в подформулу H, так как в противном случае F может быть упрощена заменой $x_i = 1$ в H. Если $x_i = \varepsilon = 0$, то H может быть удалена после того, как мы заменим значение для x_i, тем самым ещё сильнее сокращая число листьев. Так, аналогичный эффект получается если взять элемент ИЛИ вместо И (а также если взять $\overline{x}_i$ вместо x_i), математическое ожидание числа дополнительно удалённых листьев не меньше $(l+1)/2n$.

Формулы

Доказательство (окончание).
Следовательно, математическое ожидание числа оставшихся в упрощённой формуле листьев не превосходит $(l+1)/\left[\frac{3}{2n}\right]$, что и требовалось доказать . ■

Многократно применяя теорему 3, получим

Следствие 2. Если $f = f(x_1, \dots, x_n)$ и $L(f) \leq \left(\frac{n}{k}\right)^{\frac{3}{2}} - 1$, то можно так присвоить значения $n-k$ переменным, что получившаяся функция g будет атомом.

Формулы

Доказательство следствия 2. Применение теоремы 3 $n-k$ раз даёт функцию g, для которой

$$(L(g)+1) \leq \prod_{i=k+1}^{n}\left(1-\frac{1}{i}\right)^{3/2}(L(f)+1) = (k/n)^{3/2}(L(f)+1) \leq 1.$$

Значит, g равно либо x_i, либо $\overline{x}_i$ для некоторого i. ■

Следствие 3. Для счётчика чётности $f = x_1 \oplus \ldots \oplus x_n$ справедливо неравенство

$$L(f) > \left(\frac{n}{2}\right)^{\frac{3}{2}} - 1.$$

Максимальные антицепи

Определение. Семейство $\mathcal{F}$ подмножеств множества $\{1, \dots, n\}$ называется **антицепью**, если ни одно множество из $\mathcal{F}$ не содержится в другом.

Теорема 4. Пусть $\mathcal{F}$ – антицепь на множестве $\{1, \dots, n\}$. Тогда

$$\sum_{A \in \mathcal{F}} \left[1 / \binom{n}{|A|}\right] \leq 1.$$

Доказательство. Пусть σ – равновероятно выбранная перестановка на множестве $\{1, \dots, n\}$. Положим

$$\mathcal{C}_\sigma = \{\{\sigma(j) : 1 \leq j \leq i\} : 0 \leq i \leq n\}.$$

(В случаях $i = 0$ и $i = n$ мы получим $\emptyset$, $\{1, \dots, n\} \in \mathcal{C}_\sigma$, соответственно.)

Максимальные антицепи

Доказательство (продолжение). Введём случайную величину

$$X = |\mathcal{F} \cap \mathcal{C}_\sigma|.$$

Рассмотрим разложение

$$X = \sum_{A \in \mathcal{F}} X_A\,,$$

где X_A – индикатор события «$A \in \mathcal{C}_\sigma$». Тогда

$$\mathbf{E}[X_A] = \Pr[A \in \mathcal{C}_\sigma] = 1/\binom{n}{|A|},$$

так как $\mathcal{C}_\sigma$ содержит ровно одно множество размера $|A|$, которое выбирается равновероятно среди всех множеств размера $|A|$.

Максимальные антицепи

Доказательство (окончание). Из линейности математического ожидания следует, что

$$\mathbf{E}[X] = \sum_{A \in \mathcal{F}} \left[1 / \binom{n}{|A|} \right].$$

$\mathcal{C}_\sigma$ образует цепь для *<u>любого</u>* σ, следовательно, каждая пара множеств сравнима. Так как $\mathcal{F}$ – антицепь, *<u>должно</u>* выполняться неравенство $X = |\mathcal{F} \cap \mathcal{C}_\sigma| \leq 1$. Следовательно, $\mathbf{E}[X] \leq 1$. ■

Максимальные антицепи

Следствие 4 (теорема Шпернера). Пусть $\mathcal{F}$ – антицепь на множестве $\{1, \dots, n\}$. Тогда

$$|\mathcal{F}| \le \binom{n}{\lfloor n/2 \rfloor}.$$

Доказательство. Известно, что функция $\binom{n}{x}$ достигает максимума при $x = \lfloor n/2 \rfloor$, так что

$$1 \ge \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \ge \frac{|\mathcal{F}|}{\binom{n}{\lfloor n/2 \rfloor}}. \qquad \blacksquare$$

Литература к лекции

1. Алон Н., Спенсер Дж. Вероятностный метод. М.: БИНОМ. Лаборатория знаний, 2007, с. 207-216, 219-222.
2. Разборов А. А. (1987) Нижние оценки сложности схем ограниченной глубины над полным базисом, содержащим функцию логического сложения // *Математические заметки* **41** (4): с. 598-607.
3. Smolensky R. (1987) Algebraic methods in the theory of lower bounds for boolean circuit complexity // *Proceedings of the 19-th ACM STOC*, ACM Press, New York, pp. 77-82.
4. Субботовская Б. А. (1961) Реализация линейных функций формулами в базисе $\vee$, $\wedge$, $-$ // *Доклады Академии Наук СССР* **136** (3): с. 110-112.

Литература к лекции

5. Храпченко В. М. (1971) Об одном методе получения нижних оценок сложности П-схем // *Математические заметки* **10** (1): с. 83-92.
6. Андреев А. Е. (1987) О методе получения более чем квадратичных эффективных нижних оценок сложности π –схем // *Вестник Московского Университета, Серия 1, Математика, Механика,* (1): с. 70-73.
7. Hástad J. (1998) The shrinkage exponent of De Morgan formulas is 2 // *SIAM J. Comput.* **27** (1): pp. 48-64.

СПАСИБО ЗА ВНИМАНИЕ!