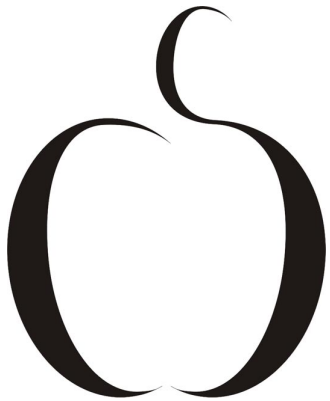
Семинар по сложности булевых функций

Лекция 11: Методы получения нижних оценок на размеры схем ограниченной глубины

П. Колганов

Computer Science клуб при ПОМИ
http://compsciclub.ru

11.12.2011



План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Чередующиеся схемы фиксированной глубины

С чем мы имеем дело?

- Мы рассматриваем схемы, состоящие из чередующихся уровней *AND* и *OR* гейтов с неограниченным числом входов (AC-схемы).
- На входе схемы — переменные и их отрицания.
- Глубина схемы ограничена какой-либо функцией от числа входных переменных, размер же может быть произвольным.

Чередующиеся схемы фиксированной глубины

С чем мы имеем дело?

- Мы рассматриваем схемы, состоящие из чередующихся уровней *AND* и *OR* гейтов с неограниченным числом входов (AC-схемы).
- На входе схемы — переменные и их отрицания.
- Глубина схемы ограничена какой-либо функцией от числа входных переменных, размер же может быть произвольным.

Как получать нижние оценки?

- Метод сокращения глубины схемы.
- Версия метода аппроксимаций Разборова.

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Лемма о переключении: общая идея

- Ключевой инструмент для сокращения глубины — лемма о переключении (Håstad's Switching Lemma).
- Она позволяет заменить КНФ на ДНФ и наоборот.

Лемма о переключении: общая идея

- Ключевой инструмент для сокращения глубины — лемма о переключении (Håstad's Switching Lemma).
- Она позволяет заменить КНФ на ДНФ и наоборот.
- Более того, лемма гарантирует ограниченность длины конъюнктов (дизъюнктов) получаемой формулы. В то же время она требует, чтобы дизъюнкты (конъюнкты) входной формулы так же были ограниченной длины.

Лемма о переключении: общая идея

- Ключевой инструмент для сокращения глубины — лемма о переключении (Håstad's Switching Lemma).
- Она позволяет заменить КНФ на ДНФ и наоборот.
- Более того, лемма гарантирует ограниченность длины конъюнктов (дизъюнктов) получаемой формулы. В то же время она требует, чтобы дизъюнкты (конъюнкты) входной формулы так же были ограниченной длины.
- Замена достигается не бесплатно, но засчет подстановки константных значений некоторым входным переменным.

Общая идея использования леммы

- Переключение позволит поменять типы гейтов на первых двух уровнях (следующих после входных переменных), затем по ассоциативности операций *AND* и *OR* можно будет объединить второй и третий уровни в один, уменьшив этим на один глубину схемы.

Общая идея использования леммы

- Переключение позволит поменять типы гейтов на первых двух уровнях (следующих после входных переменных), затем по ассоциативности операций *AND* и *OR* можно будет объединить второй и третий уровни в один, уменьшив этим на один глубину схемы.
- Эту операцию можно повторять до тех пор, пока глубина схемы не станет равна двум.

Общая идея использования леммы

- Переключение позволит поменять типы гейтов на первых двух уровнях (следующих после входных переменных), затем по ассоциативности операций *AND* и *OR* можно будет объединить второй и третий уровни в один, уменьшив этим на один глубину схемы.
- Эту операцию можно повторять до тех пор, пока глубина схемы не станет равна двум.
- Если число подставляемых переменных определенным образом зависит от размера схемы, то для маленькой схемы может получиться, что она превратится в схему глубины 2 малого размера после подстановки малого числа переменных по сравнениию их с общим числом. После чего подстановкой еще небольшого числа переменных она обратится в константу.

Общая идея использования леммы

- Переключение позволит поменять типы гейтов на первых двух уровнях (следующих после входных переменных), затем по ассоциативности операций *AND* и *OR* можно будет объединить второй и третий уровни в один, уменьшив этим на один глубину схемы.
- Эту операцию можно повторять до тех пор, пока глубина схемы не станет равна двум.
- Если число подставляемых переменных определенным образом зависит от размера схемы, то для маленькой схемы может получиться, что она превратится в схему глубины 2 малого размера после подстановки малого числа переменных по сравнениию их с общим числом. После чего подстановкой еще небольшого числа переменных она обратится в константу.
- Некоторые функции, например, $Parity_n$, нельзя обратить в константу подстановкой малого числа переменных, для них и получаем большие нижние оценки.

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Минтермы и макстермы

Определение

1-терм (0-терм) булевой функции — подмножество ее переменных, таких, что эта функция может быть обращена в тождественную единицу (ноль) подстановкой этим переменным некоторых значений.

Определение

Минтерм (макстерм) — минимальный по включению 1-терм (0-терм).

Определение

Обозначим как $\min(f)$ ($\max(f)$) размер максимального минтерма (макстерма).

t-КНФ и s-ДНФ

Определение

t-КНФ — формула, записанная в КНФ, каждый дизъюнкт которой содержит не более t литералов.

Определение

s-ДНФ — формула, записанная в ДНФ, каждый конъюнкт которой содержит не более s литералов.

t-КНФ и s-ДНФ

Определение

t-КНФ — формула, записанная в КНФ, каждый дизъюнкт которой содержит не более t литералов.

Определение

s-ДНФ — формула, записанная в ДНФ, каждый конъюнкт которой содержит не более s литералов.

Замечание

Функция f представима как s-ДНФ $\Leftrightarrow \min(f) \leq s$.
Функция f представима как t-КНФ $\Leftrightarrow \max(f) \leq t$.

Подстановки

Определение

p-случайная подстановка ρ, примененная к n переменным — присвоение части переменных константного значения так, что np случайно выбранных переменных остаются неприсвоенными, остальные $n(1-p)$ равновероятно присваиваются нулю или единице.

Определение

Обозначим как f_ρ подфункцию f, получаемую из f после применениея к ее аргументам подстановки ρ.

Подстановки

Определение

p-случайная подстановка ρ, примененная к n переменным — присвоение части переменных константного значения так, что np случайно выбранных переменных остаются неприсвоенными, остальные $n(1-p)$ равновероятно присваиваются нулю или единице.

Определение

Обозначим как f_ρ подфункцию f, получаемую из f после применениея к ее аргументам подстановки ρ.

Замечание

Далее мы будем отождествлять подстановку и множество переменных, которые она присваивает, напрмер, называть минтермом подстановку, присваивающую минимальное количество переменных и обращающую функцию в единицу.

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Лемма о переключении

Лемма (о переключении, Håstad, 86)

Пусть f представима как t-КНФ, ρ — p-случайная подстановка. Тогда

$$\Pr[\min(f_\rho) > s] \leq (8pt)^s.$$

Лемма о переключении

Лемма (о переключении, Håstad, 86)

Пусть f представима как t-КНФ, ρ — p-случайная подстановка. Тогда

$$\Pr[\min(f_\rho) > s] \leq (8pt)^s.$$

Замечание

Верно и симметричное утверждение, позволяющего переключать t-ДНФ на s-КНФ.

Использование леммы о переключении

- f представима как s-ДНФ с вероятностью не менее $1 - (8pt)^s$.

Использование леммы о переключении

- f представима как s-ДНФ с вероятностью не менее $1 - (8pt)^s$.
- Возникает вопрос: как нам могут помочь вероятностные оценки?

Использование леммы о переключении

- f представима как s-ДНФ с вероятностью не менее $1 - (8pt)^s$.
- Возникает вопрос: как нам могут помочь вероятностные оценки?
- Достаточно большая оценка на вероятность показывает, что существует такая подстановка ρ, что f_ρ представима как s-ДНФ.

Использование леммы о переключении

- f представима как s-ДНФ с вероятностью не менее $1 - (8pt)^s$.
- Возникает вопрос: как нам могут помочь вероятностные оценки?
- Достаточно большая оценка на вероятность показывает, что существует такая подстановка ρ, что f_ρ представима как s-ДНФ.
- В частности, если оценка на вероятность успеха превосходит $1/2$, то искомая подстановка существует.

Использование леммы о переключении

- f представима как s-ДНФ с вероятностью не менее $1 - (8pt)^s$.
- Возникает вопрос: как нам могут помочь вероятностные оценки?
- Достаточно большая оценка на вероятность показывает, что существует такая подстановка ρ, что f_ρ представима как s-ДНФ.
- В частности, если оценка на вероятность успеха превосходит $1/2$, то искомая подстановка существует.
- Можно применять лемму одновременно к нескольким функциям.

Лемма Разборова

Определение

Обозначим как $\mathcal{R}^\ell$ множество всех подстановок, оставляющих неприсвоенными ровно ℓ переменных (при фиксированном общем числе переменных n).

Определение

Обозначим как $Bad_f(\ell, s)$ множество $\{\rho \in \mathcal{R}^\ell \mid \min(f_\rho) > s\}$.

Лемма Разборова

Определение

Обозначим как $\mathcal{R}^\ell$ множество всех подстановок, оставляющих неприсвоенными ровно ℓ переменных (при фиксированном общем числе переменных n).

Определение

Обозначим как $Bad_f(\ell, s)$ множество $\{\rho \in \mathcal{R}^\ell \mid \min(f_\rho) > s\}$.

Замечание

$$|\mathcal{R}^\ell| = \binom{n}{\ell} 2^{n-\ell}.$$

Лемма Разборова

Определение

Обозначим как $\mathcal{R}^\ell$ множество всех подстановок, оставляющих неприсвоенными ровно ℓ переменных (при фиксированном общем числе переменных n).

Определение

Обозначим как $Bad_f(\ell, s)$ множество $\{\rho \in \mathcal{R}^\ell \mid \min(f_\rho) > s\}$.

Замечание

$$|\mathcal{R}^\ell| = \binom{n}{\ell} 2^{n-\ell}.$$

Лемма (Разборов, 95)

f представима как t-КНФ $\Rightarrow |Bad_f(\ell, s)| \leq |\mathcal{R}^{\ell-s}| \cdot (2t)^s$.

Доказательство леммы о переключении

Доказательство

Положим $\ell = np$. Тогда

$$\Pr[\min(f_\rho) > s] = \frac{|Bad_f(\ell, s)|}{|\mathcal{R}^\ell|}.$$

Доказательство леммы о переключении

Доказательство

Положим $\ell = np$. Тогда

$$\Pr[\min(f_\rho) > s] = \frac{|Bad_f(\ell, s)|}{|\mathcal{R}^\ell|}.$$

По лемме Разборова это не превосходит

$$\frac{\binom{n}{\ell-s}2^{n-\ell+s}(2t)^s}{\binom{n}{\ell}2^{n-\ell}} \leq \left(\frac{\ell}{n-\ell}\right)^s (4t)^s = \left(\frac{4tp}{1-p}\right)^s.$$

Доказательство леммы о переключении

Доказательство

Положим $\ell = np$. Тогда

$$\Pr[\min(f_\rho) > s] = \frac{|Bad_f(\ell, s)|}{|\mathcal{R}^\ell|}.$$

По лемме Разборова это не превосходит

$$\frac{\binom{n}{\ell-s}2^{n-\ell+s}(2t)^s}{\binom{n}{\ell}2^{n-\ell}} \leq \left(\frac{\ell}{n-\ell}\right)^s (4t)^s = \left(\frac{4tp}{1-p}\right)^s.$$

При $p \leq 1/2$, получаем требуемое, то есть верхнюю оценку $(8pt)^s$.

Доказательство леммы о переключении

Доказательство

Положим $\ell = np$. Тогда

$$\Pr[\min(f_\rho) > s] = \frac{|Bad_f(\ell, s)|}{|\mathcal{R}^\ell|}.$$

По лемме Разборова это не превосходит

$$\frac{\binom{n}{\ell-s}2^{n-\ell+s}(2t)^s}{\binom{n}{\ell}2^{n-\ell}} \le \left(\frac{\ell}{n-\ell}\right)^s (4t)^s = \left(\frac{4tp}{1-p}\right)^s.$$

При $p \le 1/2$, получаем требуемое, то есть верхнюю оценку $(8pt)^s$.
Ясно, что из этого следует истинность леммы при любом p. □

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Идея доказательства леммы Разборова

1. Построим кодирование $Code : Bad_f(\ell, s) \to C$.

Идея доказательства леммы Разборова

1. Построим кодирование $Code : Bad_f(\ell, s) \to C$.
2. Предъявим способ получения подстановки ρ по ее коду $Code(\rho)$ единственным образом, показав этим инъективность кода.

Идея доказательства леммы Разборова

1. Построим кодирование $Code : Bad_f(\ell, s) \to C$.
2. Предъявим способ получения подстановки ρ по ее коду $Code(\rho)$ единственным образом, показав этим инъективность кода.
3. Покажем, что $|C| \leq |\mathcal{R}^{\ell-s}| \cdot (2t)^s$.

Построение кода: инициализация

1. Зафиксируем формулу F, являющуюся представлением функции f в виде t-КНФ. Зафиксируем в ней порядок дизъюнктов и литералов внутри каждого дизъюнкта.

Построение кода: инициализация

1. Зафиксируем формулу F, являющуюся представлением функции f в виде t-КНФ. Зафиксируем в ней порядок дизъюнктов и литералов внутри каждого дизъюнкта.
2. Рассмотрим «плохую» подстановку $\rho \in Bad_f(\ell, s)$. После ее применения в формуле F может быть обращена в единицу и выкинута часть дизъюнктов, но не все.

Построение кода: инициализация

1. Зафиксируем формулу F, являющуюся представлением функции f в виде t-КНФ. Зафиксируем в ней порядок дизъюнктов и литералов внутри каждого дизъюнкта.
2. Рассмотрим «плохую» подстановку $\rho \in Bad_f(\ell, s)$. После ее применения в формуле F может быть обращена в единицу и выкинута часть дизъюнктов, но не все.
3. f_ρ имеет минтерм π' размера больше s. Выберем из него первые s переменных в порядке первого дизънкта, который они обращают в единицу. Полученное подмножество обозначим как π.

Построение кода: первый шаг

1. Пусть C_1 — первый дизъюнкт, не обращенный в единицу ρ, но обращенный в единицу $\rho\pi$.

Построение кода: первый шаг

1. Пусть C_1 — первый дизъюнкт, не обращенный в единицу ρ, но обращенный в единицу $\rho\pi$.
2. Пусть $\pi_1 \subseteq \pi$ — множество переменных, содержахихся в C_1.

Построение кода: первый шаг

1. Пусть C_1 — первый дизъюнкт, не обращенный в единицу ρ, но обращенный в единицу $\rho\pi$.
2. Пусть $\pi_1 \subseteq \pi$ — множество переменных, содержахихся в C_1.
3. Пусть $\overline{\pi}_1$ — подстановка, содержащая те же переменные, что и π_1, но НЕ обращающая в единицу C_1.

Построение кода: первый шаг

1. Пусть C_1 — первый дизъюнкт, не обращенный в единицу ρ, но обращенный в единицу $\rho\pi$.
2. Пусть $\pi_1 \subseteq \pi$ — множество переменных, содержахихся в C_1.
3. Пусть $\overline{\pi}_1$ — подстановка, содержащая те же переменные, что и π_1, но НЕ обращающая в единицу C_1.
4. Пусть $\vec{a}_1 \in \{0,1\}^t$ — бинарная строка, в которой единицами отмечены позиции литералов C_1, затронутых π_1.

Построение кода: первый шаг

1. Пусть C_1 — первый дизъюнкт, не обращенный в единицу ρ, но обращенный в единицу $\rho\pi$.
2. Пусть $\pi_1 \subseteq \pi$ — множество переменных, содержахихся в C_1.
3. Пусть $\overline{\pi}_1$ — подстановка, содержащая те же переменные, что и π_1, но НЕ обращающая в единицу C_1.
4. Пусть $\vec{a}_1 \in \{0,1\}^t$ — бинарная строка, в которой единицами отмечены позиции литералов C_1, затронутых π_1.

Пример

$$
\begin{array}{lcccccccccc}
C_1 & = & x_3 & \vee & \neg x_4 & \vee & x_6 & \vee & x_7 & \vee & x_{12} \\
\pi_1 & = & * & & 0 & & * & & 1 & & 0 \\
\overline{\pi}_1 & = & * & & 1 & & * & & 0 & & 0 \\
\vec{a}_1 & = & 0 & & 1 & & 0 & & 1 & & 1
\end{array}
$$

Построение кода: последующие шаги

1. Теперь положим $\rho = \rho\pi_1$, $\pi = \pi \setminus \pi_1$.

Построение кода: последующие шаги

1. Теперь положим $\rho = \rho\pi_1$, $\pi = \pi \setminus \pi_1$.
2. Аналогичным первому шагу образом получим C_2, π_2, $\overline{\pi}_2$, $\vec{a}_2$.

Построение кода: последующие шаги

1. Теперь положим $\rho = \rho\pi_1$, $\pi = \pi \setminus \pi_1$.
2. Аналогичным первому шагу образом получим C_2, π_2, $\overline{\pi}_2$, $\vec{a}_2$.
3. Продолжаем процесс, пока π не пусто.

Построение кода: последующие шаги

1. Теперь положим $\rho = \rho\pi_1$, $\pi = \pi \setminus \pi_1$.
2. Аналогичным первому шагу образом получим C_2, π_2, $\overline{\pi}_2$, $\vec{a}_2$.
3. Продолжаем процесс, пока π не пусто.
4. Получим последовательности $\pi_1, \ldots, \pi_m$, $\overline{\pi}_1, \ldots, \overline{\pi}_m$, $\vec{a}_1, \ldots, \vec{a}_m$.

Построение кода: получение результата

1. Положим $\vec{b} \in \{0,1\}^s$ равным бинарной строке, в которой единицами отмечены совпадающие позиции подстановок π и $\overline{\pi} = \overline{\pi}_1 \dots \overline{\pi}_m$, нулем, соответственно, различающиеся. Переменные при этом упорядочим в порядке их повления в C_1, затем в C_2 и так далее.

Построение кода: получение результата

1. Положим $\vec{b} \in \{0,1\}^s$ равным бинарной строке, в которой единицами отмечены совпадающие позиции подстановок π и $\overline{\pi} = \overline{\pi}_1 \dots \overline{\pi}_m$, нулем, соответственно, различающиеся. Переменные при этом упорядочим в порядке их повления в C_1, затем в C_2 и так далее.

Пример

$$\begin{array}{cccccccc} \pi & = & * & 0 & * & 1 & 0 \\ \overline{\pi} & = & * & 1 & * & 0 & 0 \\ \vec{b} & = & & 0 & & 0 & 1 \end{array}$$

Построение кода: получение результата

1. Положим $\vec{b} \in \{0,1\}^s$ равным бинарной строке, в которой единицами отмечены совпадающие позиции подстановок π и $\overline{\pi} = \overline{\pi}_1 \dots \overline{\pi}_m$, нулем, соответственно, различающиеся. Переменные при этом упорядочим в порядке их повления в C_1, затем в C_2 и так далее.

Пример

$$\begin{array}{cccccccc} \pi & = & * & 0 & * & 1 & 0 \\ \overline{\pi} & = & * & 1 & * & 0 & 0 \\ \vec{b} & = & & 0 & & 0 & 1 \end{array}$$

2. В результате положим

$$Code(\rho) = \left\langle \rho\overline{\pi}_1 \dots \overline{\pi}_m,\ \vec{a}_1, \dots, \vec{a}_m,\ \vec{b} \right\rangle .$$

Декодирование

1. Рассмотрим первый дизъюнкт F, который не обращается в единицу подстановкой $\rho\overline{\pi}_1 \ldots \overline{\pi}_m$. Им будет C_1.

Декодирование

1. Рассмотрим первый дизъюнкт F, который не обращается в единицу подстановкой $\rho\overline{\pi}_1 \dots \overline{\pi}_m$. Им будет C_1. Это видно из того, что $\overline{\pi}_2 \dots \overline{\pi}_m$ не содержит переменных из C_1 в силу выбора π_1.

Декодирование

1. Рассмотрим первый дизъюнкт F, который не обращается в единицу подстановкой $\rho\overline{\pi}_1 \dots \overline{\pi}_m$. Им будет C_1. Это видно из того, что $\overline{\pi}_2 \dots \overline{\pi}_m$ не содержит переменных из C_1 в силу выбора π_1.
2. Имея C_1, $\vec{a}_1$ и $\vec{b}$ восстановим π_1.

Декодирование

1. Рассмотрим первый дизъюнкт F, который не обращается в единицу подстановкой $\rho\overline{\pi}_1 \dots \overline{\pi}_m$. Им будет C_1. Это видно из того, что $\overline{\pi}_2 \dots \overline{\pi}_m$ не содержит переменных из C_1 в силу выбора π_1.
2. Имея C_1, $\vec{a}_1$ и $\vec{b}$ восстановим π_1.
3. Теперь рассмотрим $\rho\pi_1\overline{\pi}_2 \dots \overline{\pi}_m$. Аналогично получим π_2.

Декодирование

1. Рассмотрим первый дизъюнкт F, который не обращается в единицу подстановкой $\rho\overline{\pi}_1 \dots \overline{\pi}_m$. Им будет C_1. Это видно из того, что $\overline{\pi}_2 \dots \overline{\pi}_m$ не содержит переменных из C_1 в силу выбора π_1.
2. Имея C_1, $\vec{a}_1$ и $\vec{b}$ восстановим π_1.
3. Теперь рассмотрим $\rho\pi_1\overline{\pi}_2 \dots \overline{\pi}_m$. Аналогично получим π_2.
4. Повторяя процесс, в итоге получаем $\pi = \pi_1 \dots \pi_m$.

Декодирование

1. Рассмотрим первый дизъюнкт F, который не обращается в единицу подстановкой $\rho\overline{\pi}_1 \dots \overline{\pi}_m$. Им будет C_1. Это видно из того, что $\overline{\pi}_2 \dots \overline{\pi}_m$ не содержит переменных из C_1 в силу выбора π_1.
2. Имея C_1, $\vec{a}_1$ и $\vec{b}$ восстановим π_1.
3. Теперь рассмотрим $\rho\pi_1\overline{\pi}_2 \dots \overline{\pi}_m$. Аналогично получим π_2.
4. Повторяя процесс, в итоге получаем $\pi = \pi_1 \dots \pi_m$.
5. Наконец, получаем $\rho = \rho\pi \setminus \pi$.

Оценка размера

1. $\rho\overline{\pi}_1 \dots \overline{\pi}_m \in \mathcal{R}^{\ell-s}$, число таких подстановок не превосходит $\left|\mathcal{R}^{\ell-s}\right|$.

Оценка размера

1. $\rho\overline{\pi}_1 \dots \overline{\pi}_m \in \mathcal{R}^{\ell-s}$, число таких подстановок не превосходит $|\mathcal{R}^{\ell-s}|$.
2. Число возможных строк $\vec{b}$ равно $|\{0,1\}^s| = 2^s$.

Оценка размера

1. $\rho\overline{\pi}_1 \dots \overline{\pi}_m \in \mathcal{R}^{\ell-s}$, число таких подстановок не превосходит $|\mathcal{R}^{\ell-s}|$.
2. Число возможных строк $\vec{b}$ равно $|\{0,1\}^s| = 2^s$.
3. Число возможных строк $\vec{a}$ — это число разбиений s-элементного множетва на подмножества размера от 1 до t.

Оценка размера

1. $\rho\overline{\pi}_1 \dots \overline{\pi}_m \in \mathcal{R}^{\ell-s}$, число таких подстановок не превосходит $|\mathcal{R}^{\ell-s}|$.
2. Число возможных строк $\vec{b}$ равно $|\{0,1\}^s| = 2^s$.
3. Число возможных строк $\vec{a}$ — это число разбиений s-элементного множетва на подмножества размера от 1 до t. Индукцией по s можно покзать, что это не превосходит t^s.

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Оценка на $R(f)$

Определение

Обозначим как $R(f)$ минимальное число переменных, подстановка которых обращает f в константу.

Оценка на $R(f)$

Определение

Обозначим как $R(f)$ минимальное число переменных, подстановка которых обращает f в константу.

Пример

$R(Parity_n) = n$.
$R(Maj_n) = n/2$.

Оценка на $R(f)$

Определение

Обозначим как $R(f)$ минимальное число переменных, подстановка которых обращает f в константу.

Пример

$R(Parity_n) = n$.
$R(Maj_n) = n/2$.

Теорема

Пусть булева функция f от n переменных может быть вычислена AC-схемой глубины $(d+1)$ размера S. Тогда

$$R(f) \leq n - \frac{n}{c_d(\log S)^{d-1}} + 2\log S,$$

где c_d зависит только от глубины схемы.

Доказательство оценки на $R(f)$: ограничение входной степени

- Пусть на первом уровне расположены *OR* гейты (случай *AND* гейтов разбирается аналогично).

Доказательство оценки на $R(f)$: ограничение входной степени

- Пусть на первом уровне расположены *OR* гейты (случай *AND* гейтов разбирается аналогично).
- Каждый такой гейт представляет собой 1-ДНФ.

Доказательство оценки на $R(f)$: ограничение входной степени

- Пусть на первом уровне расположены *OR* гейты (случай *AND* гейтов разбирается аналогично).
- Каждый такой гейт представляет собой 1-ДНФ.
- Применим лемму о переключении с параметрами $t = 1$, $s = 2 \log S$, $p = 1/16$.

Доказательство оценки на $R(f)$: ограничение входной степени

- Пусть на первом уровне расположены *OR* гейты (случай *AND* гейтов разбирается аналогично).
- Каждый такой гейт представляет собой 1-ДНФ.
- Применим лемму о переключении с параметрами $t = 1$, $s = 2 \log S$, $p = 1/16$.
- $1 - (8pt)^s = 1 - \left(\frac{8}{16}\right)^{2 \log S} = 1 - S^{-2}$.

Доказательство оценки на $R(f)$: ограничение входной степени

- Пусть на первом уровне расположены *OR* гейты (случай *AND* гейтов разбирается аналогично).
- Каждый такой гейт представляет собой 1-ДНФ.
- Применим лемму о переключении с параметрами $t = 1$, $s = 2 \log S$, $p = 1/16$.
- $1 - (8pt)^s = 1 - \left(\frac{8}{16}\right)^{2 \log S} = 1 - S^{-2}$.
- Гейтов на первом уровне не более S, вероятность заменить их все сразу не менее $(1 - S^{-2})^S \geq 1/2$. Значит, нужная подстановка существует.

Доказательство оценки на $R(f)$: ограничение входной степени

- Пусть на первом уровне расположены *OR* гейты (случай *AND* гейтов разбирается аналогично).
- Каждый такой гейт представляет собой 1-ДНФ.
- Применим лемму о переключении с параметрами $t = 1$, $s = 2\log S$, $p = 1/16$.
- $1 - (8pt)^s = 1 - \left(\frac{8}{16}\right)^{2\log S} = 1 - S^{-2}$.
- Гейтов на первом уровне не более S, вероятность заменить их все сразу не менее $(1 - S^{-2})^S \geq 1/2$. Значит, нужная подстановка существует.
- Полученные КНФ будут содержать ровно один дизъюнкт. Иными словами, такая подстановка ограничит входную степень гейтов на первом уровне до $2\log S$.

Доказательство оценки на $R(f)$: сокращение глубины

- Применим лемму о переключении к гейтам на втором уровне с параметрами $t = 2\log S$, $s = 2\log S$, $p = \frac{1}{32\log S}$.

Доказательство оценки на $R(f)$: сокращение глубины

- Применим лемму о переключении к гейтам на втором уровне с параметрами $t = 2\log S$, $s = 2\log S$, $p = \frac{1}{32\log S}$.
- $1 - (8pt)^s = 1 - \left(\frac{16\log S}{32\log S}\right)^{2\log S} = 1 - S^{-2}$.

Доказательство оценки на $R(f)$: сокращение глубины

- Применим лемму о переключении к гейтам на втором уровне с параметрами $t = 2\log S$, $s = 2\log S$, $p = \frac{1}{32\log S}$.
- $1 - (8pt)^s = 1 - \left(\frac{16\log S}{32\log S}\right)^{2\log S} = 1 - S^{-2}$.
- Аналогично предыдущему шагу, искомая подстановка существует.

Доказательство оценки на $R(f)$: сокращение глубины

- Применим лемму о переключении к гейтам на втором уровне с параметрами $t = 2\log S$, $s = 2\log S$, $p = \frac{1}{32\log S}$.
- $1 - (8pt)^s = 1 - \left(\frac{16\log S}{32\log S}\right)^{2\log S} = 1 - S^{-2}$.
- Аналогично предыдущему шагу, искомая подстановка существует.
- Заменили типы гейтов на первых двух уровнях, объединяем второй и третий уровни.

Доказательство оценки на $R(f)$: сокращение глубины

- Применим лемму о переключении к гейтам на втором уровне с параметрами $t = 2\log S$, $s = 2\log S$, $p = \frac{1}{32\log S}$.
- $1 - (8pt)^s = 1 - \left(\frac{16\log S}{32\log S}\right)^{2\log S} = 1 - S^{-2}$.
- Аналогично предыдущему шагу, искомая подстановка существует.
- Заменили типы гейтов на первых двух уровнях, объединяем второй и третий уровни.
- Повторим $(d-1)$ раз, получим схему глубины 2, представляющую собой $(2\log S)$-КНФ или $(2\log S)$-ДНФ.

Доказательство оценки на $R(f)$: сокращение глубины

- Применим лемму о переключении к гейтам на втором уровне с параметрами $t = 2\log S$, $s = 2\log S$, $p = \frac{1}{32\log S}$.
- $1 - (8pt)^s = 1 - \left(\frac{16\log S}{32\log S}\right)^{2\log S} = 1 - S^{-2}$.
- Аналогично предыдущему шагу, искомая подстановка существует.
- Заменили типы гейтов на первых двух уровнях, объединяем второй и третий уровни.
- Повторим $(d-1)$ раз, получим схему глубины 2, представляющую собой $(2\log S)$-КНФ или $(2\log S)$-ДНФ.
- У нас уже подставлено $n - \frac{n}{16(32\log S)^{d-1}}$ переменных. Из оставшихся достаточно подставить $2\log S$, чтобы обратить схему в константу. Таким образом, теорема доказана.

Следствия из оценки на $R(f)$

Теорема (Håstad, 86)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/d})}$.

Следствия из оценки на $R(f)$

Теорема (Håstad, 86)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/d})}$.

Определение

AC^k - класс булевых функций, вычислимых AC-схемами глубины $\mathcal{O}(log^k n)$ полиномиального размера.

Следствия из оценки на $R(f)$

Теорема (Håstad, 86)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/d})}$.

Определение

AC^k - класс булевых функций, вычислимых AC-схемами глубины $\mathcal{O}(log^k n)$ полиномиального размера.

Утверждение

$f \in AC^0 \Rightarrow R(f) \leq n - \frac{n}{polylog(n)}$.

Оценка для Maj_n

Утверждение

Любая AC-схема глубины d, вычисляющая Maj_n, имеет размер не менее $2^{\Omega(n^{1/d})}$.

Оценка для Maj_n

Утверждение

Любая AC-схема глубины d, вычисляющая Maj_n, имеет размер не менее $2^{\Omega(n^{1/d})}$.

Доказательство

- Прямое использование оценки на $R(f)$ не поможет: $R(Maj_n) = n/2$.

Оценка для Maj_n

Утверждение

Любая AC-схема глубины d, вычисляющая Maj_n, имеет размер не менее $2^{\Omega(n^{1/d})}$.

Доказательство

- Прямое использование оценки на $R(f)$ не поможет: $R(Maj_n) = n/2$.
- $E_k^{n/2}(x) = Th_k^{n/2}(x) \wedge \neg Th_{k+1}^{n/2}(x) = Th_k^{n/2}(x) \wedge Th_{n/2-k-1}^{n/2}(\neg x)$.

Оценка для Maj_n

Утверждение

Любая AC-схема глубины d, вычисляющая Maj_n, имеет размер не менее $2^{\Omega(n^{1/d})}$.

Доказательство

- Прямое использование оценки на $R(f)$ не поможет: $R(Maj_n) = n/2$.
- $E_k^{n/2}(x) = Th_k^{n/2}(x) \wedge \neg Th_{k+1}^{n/2}(x) = Th_k^{n/2}(x) \wedge Th_{n/2-k-1}^{n/2}(\neg x)$.
- $Th_k^{n/2}(x) = Maj_n(x \underbrace{1 \ldots 1}_{n/2-k} \underbrace{0 \ldots 0}_{k})$

Оценка для Maj_n

Утверждение

Любая AC-схема глубины d, вычисляющая Maj_n, имеет размер не менее $2^{\Omega(n^{1/d})}$.

Доказательство

- Прямое использование оценки на $R(f)$ не поможет: $R(Maj_n) = n/2$.
- $E_k^{n/2}(x) = Th_k^{n/2}(x) \wedge \neg Th_{k+1}^{n/2}(x) = Th_k^{n/2}(x) \wedge Th_{n/2-k-1}^{n/2}(\neg x)$.
- $Th_k^{n/2}(x) = Maj_n(x \underbrace{1 \ldots 1}_{n/2-k} \underbrace{0 \ldots 0}_{k})$
- $Parity_n = \bigvee_{k \le n/2,\, k \equiv 1 \bmod 2} E_k^{n/2} = \bigwedge_{k \le n/2,\, k \equiv 0 \bmod 2} \neg E_k^{n/2}$.

Оценка для Maj_n

Утверждение

Любая AC-схема глубины d, вычисляющая Maj_n, имеет размер не менее $2^{\Omega(n^{1/d})}$.

Доказательство

- Прямое использование оценки на $R(f)$ не поможет: $R(Maj_n) = n/2$.
- $E_k^{n/2}(x) = Th_k^{n/2}(x) \wedge \neg Th_{k+1}^{n/2}(x) = Th_k^{n/2}(x) \wedge Th_{n/2-k-1}^{n/2}(\neg x)$.
- $Th_k^{n/2}(x) = Maj_n(x \underbrace{1 \ldots 1}_{n/2-k} \underbrace{0 \ldots 0}_{k})$
- $Parity_n = \bigvee_{k \le n/2,\, k \equiv 1 \bmod 2} E_k^{n/2} = \bigwedge_{k \le n/2,\, k \equiv 0 \bmod 2} \neg E_k^{n/2}$.
- Можно вычислить $Parity_{n/2}$ схемой глубины $(d+1)$ размера $\mathcal{O}(nS)$, получаем требуемое. □

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Идея метода аппроксимаций

1. Аппроксимация схем: покажем, что функции, вычисляемые маленькими схемами из определенного класса, могут быть аппроксимированы полиномами маленькой степени.

Идея метода аппроксимаций

1. Аппроксимация схем: покажем, что функции, вычисляемые маленькими схемами из определенного класса, могут быть аппроксимированы полиномами маленькой степени.
2. Аппроксимация функций: покажем, что какие-то функции не могут быть аппроксимирована таким образом, в итоге получим для них нижнюю оценку.

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Аппроксимация OR_n

Лемма (Aspnes, Beigel, Furst, Rudich, 94)

Для любого целого $r > 0$ существует полином p с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}(r \log n)$, такой, что $\Pr[p(x) \neq OR_n(x)] \leq 2^{-r}$ при любом вероятностном распределении x.

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

$$q_k(x) := \sum_{i \in S_k} x_i.$$

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

$$q_k(x) := \sum_{i \in S_k} x_i.$$

$$q(x) := 1 - \prod_{k=0}^{\lceil \log n \rceil} (1 - q_k(x)).$$

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

$$q_k(x) := \sum_{i \in S_k} x_i.$$

$$q(x) := 1 - \prod_{k=0}^{\lceil \log n \rceil} (1 - q_k(x)).$$

$$\Pr[q(x) = 1] \quad \geq \quad \Pr_{2^{k-1} \leq |x|_1 < 2^k}[q_k(x) = 1]$$

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

$$q_k(x) := \sum_{i \in S_k} x_i.$$

$$q(x) := 1 - \prod_{k=0}^{\lceil \log n \rceil} (1 - q_k(x)).$$

$$\begin{aligned} \Pr[q(x) = 1] &\geq \Pr_{2^{k-1} \leq |x|_1 < 2^k}[q_k(x) = 1] \\ &= |x|_1 2^{-k} (1 - 2^{-k})^{|x|_1 - 1} \end{aligned}$$

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

$$q_k(x) := \sum_{i \in S_k} x_i.$$

$$q(x) := 1 - \prod_{k=0}^{\lceil \log n \rceil} (1 - q_k(x)).$$

$$\begin{aligned} \Pr[q(x) = 1] &\geq \Pr_{2^{k-1} \leq |x|_1 < 2^k}[q_k(x) = 1] \\ &= |x|_1 2^{-k} (1 - 2^{-k})^{|x|_1 - 1} \\ &\geq \tfrac{1}{2}(1 - 2^{-k})^{2^k - 1} \end{aligned}$$

Доказательство 1/6-аппроксимации

Доказательство

$$S_0, \ldots, S_{\lceil \log n \rceil} \subseteq \{1, \ldots, n\} : \Pr[j \in S_k] = 2^{-k}.$$

$$q_k(x) := \sum_{i \in S_k} x_i.$$

$$q(x) := 1 - \prod_{k=0}^{\lceil \log n \rceil} (1 - q_k(x)).$$

$$\begin{aligned} \Pr[q(x) = 1] &\geq \Pr_{2^{k-1} \leq |x|_1 < 2^k}[q_k(x) = 1] \\ &= |x|_1 2^{-k} (1 - 2^{-k})^{|x|_1 - 1} \\ &\geq \frac{1}{2}(1 - 2^{-k})^{2^k - 1} \\ &\geq \frac{1}{6}. \end{aligned}$$

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

$$p(x) := 1 - \prod_{i=1}^{4r}(1 - p_i(x)).$$

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

$$p(x) := 1 - \prod_{i=1}^{4r}(1 - p_i(x)).$$

$$\deg(p) = 4r \cdot \deg(q) = 4r(\lceil \log n \rceil + 1) = \mathcal{O}(r \log n).$$

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

$$p(x) := 1 - \prod_{i=1}^{4r}(1 - p_i(x)).$$

$$\deg(p) = 4r \cdot \deg(q) = 4r(\lceil \log n \rceil + 1) = \mathcal{O}(r \log n).$$

$$\Pr[p(x) = 1] \quad \geq \quad \Pr[\exists i : p_i(x) = 1]$$

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

$$p(x) := 1 - \prod_{i=1}^{4r}(1 - p_i(x)).$$

$$\deg(p) = 4r \cdot \deg(q) = 4r(\lceil \log n \rceil + 1) = \mathcal{O}(r \log n).$$

$$\begin{aligned} \Pr[p(x) = 1] &\geq \Pr[\exists i : p_i(x) = 1] \\ &= 1 - \Pr[q(x) \neq 1]^{r4} \end{aligned}$$

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

$$p(x) := 1 - \prod_{i=1}^{4r}(1 - p_i(x)).$$

$$\deg(p) = 4r \cdot \deg(q) = 4r(\lceil \log n \rceil + 1) = \mathcal{O}(r \log n).$$

$$\begin{aligned} \Pr[p(x) = 1] &\geq \Pr[\exists i : p_i(x) = 1] \\ &= 1 - \Pr[q(x) \neq 1]^{r4} \\ &\geq 1 - \left(\tfrac{5}{6}\right)^{4r} \end{aligned}$$

Доказательство $1 - 2^{-r}$-аппроксимации

Доказательство

$p_1, \ldots, p_{4r}$ строятся, как q (могут отличаться семейством $\{S_k\}_{k=0}^{m}$).

$$p(x) := 1 - \prod_{i=1}^{4r}(1 - p_i(x)).$$

$$\deg(p) = 4r \cdot \deg(q) = 4r(\lceil \log n \rceil + 1) = \mathcal{O}(r \log n).$$

$$\begin{aligned} \Pr[p(x) = 1] &\geq \Pr[\exists i : p_i(x) = 1] \\ &= 1 - \Pr[q(x) \neq 1]^{r4} \\ &\geq 1 - \left(\tfrac{5}{6}\right)^{4r} \\ &\geq 1 - 2^{-r}. \end{aligned}$$

□

Произвольность распеределения x

Замечание

Мы еще не показали, почему эта оценка верна при любом распределении x. В общих чертах:

- мы всегда можем построить полином, ошибающийся не более, чем на 2^{n-r} заданных входных последовательностях;

Произвольность распепределения x

Замечание

Мы еще не показали, почему эта оценка верна при любом распределении x. В общих чертах:

- мы всегда можем построить полином, ошибающийся не более, чем на 2^{n-r} заданных входных последовательностях;
- далее, ясно, что при любом распределении этих входных последовательностей найдутся такие 2^{n-r}, что вероятность появления любой из них не превышает 2^{-r}.

Аппроксимация AC-схемы

Утверждение

Для любого $\epsilon > 0$ и любой функции f, вычислимой AC-схемой глубины d размера S существует полином с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}((\log(S/\epsilon)\log S)^d)$, значения которого не совпадают с f на не более, чем $\epsilon 2^n$ входах.

Аппроксимация AC-схемы

Утверждение

Для любого $\epsilon > 0$ и любой функции f, вычислимой AC-схемой глубины d размера S существует полином с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}((\log(S/\epsilon)\log S)^d)$, значения которого не совпадают с f на не более, чем $\epsilon 2^n$ входах.

Доказательство

- Каждый гейт — OR_k или AND_k, $k \leq S$.

Аппроксимация AC-схемы

Утверждение

Для любого $\epsilon > 0$ и любой функции f, вычислимой AC-схемой глубины d размера S существует полином с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}((\log(S/\epsilon)\log S)^d)$, значения которого не совпадают с f на не более, чем $\epsilon 2^n$ входах.

Доказательство

- Каждый гейт — OR_k или AND_k, $k \leq S$.
- Применим предыдущую лемму с $r = \lfloor(\log(S/\epsilon))\rfloor$ и равномерно распределенной входной последовательностью.

Аппроксимация AC-схемы

Утверждение

Для любого $\epsilon > 0$ и любой функции f, вычислимой AC-схемой глубины d размера S существует полином с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}((\log(S/\epsilon)\log S)^d)$, значения которого не совпадают с f на не более, чем $\epsilon 2^n$ входах.

Доказательство

- Каждый гейт — OR_k или AND_k, $k \leq S$.
- Применим предыдущую лемму с $r = \lfloor(\log(S/\epsilon))\rfloor$ и равномерно распределенной входной последовательностью.
- Композиция полиномов для каждого гейта дает полином, вычисляющий значение выходного гейта.

Аппроксимация AC-схемы

Утверждение

Для любого $\epsilon > 0$ и любой функции f, вычислимой AC-схемой глубины d размера S существует полином с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}((\log(S/\epsilon)\log S)^d)$, значения которого не совпадают с f на не более, чем $\epsilon 2^n$ входах.

Доказательство

- Каждый гейт — OR_k или AND_k, $k \leq S$.
- Применим предыдущую лемму с $r = \lfloor(\log(S/\epsilon))\rfloor$ и равномерно распределенной входной последовательностью.
- Композиция полиномов для каждого гейта дает полином, вычисляющий значение выходного гейта. Его степень не более $\mathcal{O}((r\log S)^d)$.

Аппроксимация AC-схемы

Утверждение

Для любого $\epsilon > 0$ и любой функции f, вычислимой AC-схемой глубины d размера S существует полином с вещестенными коэффициентами от n переменных степени не более $\mathcal{O}((\log(S/\epsilon)\log S)^d)$, значения которого не совпадают с f на не более, чем $\epsilon 2^n$ входах.

Доказательство

- Каждый гейт — OR_k или AND_k, $k \leq S$.
- Применим предыдущую лемму с $r = \lfloor(\log(S/\epsilon))\rfloor$ и равномерно распределенной входной последовательностью.
- Композиция полиномов для каждого гейта дает полином, вычисляющий значение выходного гейта. Его степень не более $\mathcal{O}((r\log S)^d)$. Вероятность его ошибки не более $S2^{-r} = \epsilon$. □

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Пространство функций из $\{0,1\}^n$ в $\mathbb{R}$

- Рассмотрим пространство функций из $\{0,1\}^n$ в $\mathbb{R}$.

Пространство функций из $\{0,1\}^n$ в $\mathbb{R}$

- Рассмотрим пространство функций из $\{0,1\}^n$ в $\mathbb{R}$.
- Его размерность равна 2^n.

Пространство функций из $\{0,1\}^n$ в $\mathbb{R}$

- Рассмотрим пространство функций из $\{0,1\}^n$ в $\mathbb{R}$.
- Его размерность равна 2^n.
- Можно определить на нем скалярное произведение $\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x)g(x)$.

Пространство функций из $\{0,1\}^n$ в $\mathbb{R}$

- Рассмотрим пространство функций из $\{0,1\}^n$ в $\mathbb{R}$.
- Его размерность равна 2^n.
- Можно определить на нем скалярное произведение $\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x)g(x)$.
- Функции вида $\chi_S(x) = \prod_{i \in S} (-1)^{x_i} = \prod_{i \in S} (1 - 2x_i)$, где $S \subseteq \{1, \ldots, n\}$, составляют ортонормированный базис.

Слабая степень

Определение

Слабая степень $d_w(f)$ функции f — минимальная возможная степень такого полинома p, что $p \not\equiv 0$ и $p(-1)^f \geq 0$, т. е. знак p соответствует значению f в тех точках, где $p \neq 0$.

Слабая степень

Определение

Слабая степень $d_w(f)$ функции f — минимальная возможная степень такого полинома p, что $p \not\equiv 0$ и $p(-1)^f \geq 0$, т. е. знак p соответствует значению f в тех точках, где $p \neq 0$.

Лемма

$d_w(Parity_n) = n$.

Слабая степень

Определение

Слабая степень $d_w(f)$ функции f — минимальная возможная степень такого полинома p, что $p \not\equiv 0$ и $p(-1)^f \geq 0$, т. е. знак p соответствует значению f в тех точках, где $p \neq 0$.

Лемма

$d_w(Parity_n) = n.$

Доказательство

$p(-1)^{Parity_n} \geq 0, p \not\equiv 0 \Rightarrow \langle p, \chi_{\{1,\ldots,n\}} \rangle > 0 \Rightarrow \deg(p) = n.$ □

Оценка на слабую степень

Лемма

Пусть p — полином степени k, f — булева функция от n переменных, $Error(p, f) = \{x \in \{0,1\}^n \mid p(x)(-1)^{f(x)} \leq 0\}$, $\Delta = \lfloor (d_w(f) - k - 1)/2 \rfloor$. Тогда если $d_w(f) > k$, то

$$|Error(p, f)| \geq \sum_{i=0}^{\Delta} \binom{n}{i}.$$

Оценка на слабую степень

Лемма

Пусть p — полином степени k, f — булева функция от n переменных, $Error(p, f) = \{x \in \{0,1\}^n \mid p(x)(-1)^{f(x)} \leq 0\}$, $\Delta = \lfloor (d_w(f) - k - 1)/2 \rfloor$. Тогда если $d_w(f) > k$, то

$$|Error(p, f)| \geq \sum_{i=0}^{\Delta} \binom{n}{i}.$$

Доказательство

Предположим противное. Тогда найдется невырожденный полином q степени Δ, такой, что $x \in Error(p, f) \Rightarrow q(x) = 0$: его коэффициенты являются решением системы из $|Error(p, f)|$ линейных уравнений от $\sum_{i=0}^{\Delta} \binom{n}{i}$ переменных.

Оценка на слабую степень

Лемма

Пусть p — полином степени k, f — булева функция от n переменных, $Error(p, f) = \{x \in \{0,1\}^n \mid p(x)(-1)^{f(x)} \leq 0\}$, $\Delta = \lfloor (d_w(f) - k - 1)/2 \rfloor$. Тогда если $d_w(f) > k$, то

$$|Error(p, f)| \geq \sum_{i=0}^{\Delta} \binom{n}{i}.$$

Доказательство

Предположим противное. Тогда найдется невырожденный полином q степени Δ, такой, что $x \in Error(p, f) \Rightarrow q(x) = 0$: его коэффициенты являются решением системы из $|Error(p, f)|$ линейных уравнений от $\sum_{i=0}^{\Delta} \binom{n}{i}$ переменных. Тогда $pq^2 \not\equiv 0$ и $pq^2(-1)^f \geq 0$, значит, $d_w(f) \leq \deg(pq^2) \leq d_w(f) - 1$. Получили противоречие. □

Аппроксимация $Parity_n$

Утверждение

Пусть p — полином от n переменных степени не более $\delta\sqrt{n}+1$, где $0 < \delta < 1/2$. Тогда

$$|Error(p, Patity_n)| \geq (1/2 - \delta)2^n.$$

Аппроксимация $Parity_n$

Утверждение

Пусть p — полином от n переменных степени не более $\delta\sqrt{n}+1$, где $0 < \delta < 1/2$. Тогда

$$|Error(p, Patity_n)| \geq (1/2 - \delta)2^n.$$

Доказательство

$$|Error(p, Patity_n)| \quad \geq \quad \sum_{i=0}^{n/2-\delta\sqrt{n}} \binom{n}{i}$$

Аппроксимация $Parity_n$

Утверждение

Пусть p — полином от n переменных степени не более $\delta\sqrt{n}+1$, где $0 < \delta < 1/2$. Тогда

$$|Error(p, Patity_n)| \geq (1/2 - \delta)2^n.$$

Доказательство

$$\begin{aligned} |Error(p, Patity_n)| &\geq \sum_{i=0}^{n/2-\delta\sqrt{n}} \binom{n}{i} \\ &= \sum_{i=0}^{n/2} \binom{n}{i} - \sum_{i=n/2-\delta\sqrt{n}+1}^{n/2} \binom{n}{i} \end{aligned}$$

Аппроксимация $Parity_n$

Утверждение

Пусть p — полином от n переменных степени не более $\delta\sqrt{n}+1$, где $0 < \delta < 1/2$. Тогда

$$|Error(p, Patity_n)| \geq (1/2 - \delta)2^n.$$

Доказательство

$$\begin{aligned} |Error(p, Patity_n)| &\geq \sum_{i=0}^{n/2-\delta\sqrt{n}} \binom{n}{i} \\ &= \sum_{i=0}^{n/2} \binom{n}{i} - \sum_{i=n/2-\delta\sqrt{n}+1}^{n/2} \binom{n}{i} \\ &\geq 2^{n-1} - \delta\sqrt{n}\binom{n}{n/2} \end{aligned}$$

Аппроксимация $Parity_n$

Утверждение

Пусть p — полином от n переменных степени не более $\delta\sqrt{n}+1$, где $0<\delta<1/2$. Тогда

$$|Error(p, Patity_n)| \geq (1/2-\delta)2^n.$$

Доказательство

$$\begin{aligned}
|Error(p, Patity_n)| &\geq \sum_{i=0}^{n/2-\delta\sqrt{n}} \binom{n}{i} \\
&= \sum_{i=0}^{n/2} \binom{n}{i} - \sum_{i=n/2-\delta\sqrt{n}+1}^{n/2} \binom{n}{i} \\
&\geq 2^{n-1} - \delta\sqrt{n}\binom{n}{n/2} \\
&\geq (1/2-\delta)2^n. \qquad \square
\end{aligned}$$

Получение оценки на размер схемы

Теорема ((почти) Aspnes и пр., 94)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/4d})}$.

Получение оценки на размер схемы

Теорема ((почти) Aspnes и пр., 94)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/4d})}$.

Доказательство

- Применим утверждение об аппроксимации схемы с $\epsilon = 1/4$.

Получение оценки на размер схемы

Теорема ((почти) Aspnes и пр., 94)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/4d})}$.

Доказательство

- Применим утверждение об аппроксимации схемы с $\epsilon = 1/4$.
- Можно приблизить $Parity_n$ полиномом p степени не более $\mathcal{O}((\log(4S)\log S)^d) = \mathcal{O}((\log S)^{2d})$, ошибающемся не более, чем на $2^n/4$ входах.

Получение оценки на размер схемы

Теорема ((почти) Aspnes и пр., 94)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/4d})}$.

Доказательство

- Применим утверждение об аппроксимации схемы с $\epsilon = 1/4$.
- Можно приблизить $Parity_n$ полиномом p степени не более $\mathcal{O}((\log(4S)\log S)^d) = \mathcal{O}((\log S)^{2d})$, ошибающемся не более, чем на $2^n/4$ входах.
- Тогда $|Error(1-2p, Patity_n)| \leq 2^n/4$.

Получение оценки на размер схемы

Теорема ((почти) Aspnes и пр., 94)

Любая AC-схема глубины $(d+1)$, *вычисляющая* $Parity_n$, *имеет размер не менее* $2^{\Omega(n^{1/4d})}$.

Доказательство

- Применим утверждение об аппроксимации схемы с $\epsilon = 1/4$.
- Можно приблизить $Parity_n$ полиномом p степени не более $\mathcal{O}((\log(4S)\log S)^d) = \mathcal{O}((\log S)^{2d})$, ошибающемся не более, чем на $2^n/4$ входах.
- Тогда $|Error(1-2p, Patity_n)| \leq 2^n/4$.
- Значит, $\mathcal{O}((\log S)^{2d}) \geq \deg(p) \geq \mathcal{O}(\sqrt{n})$. □

План лекции

1. Метод сокращения глубины: лемма о переключении
   - Общие идеи
   - Вводные определения
   - Лемма о переключении, доказательство через лемму Разборова
   - Доказательство леммы Разборова
   - Получение оценок
2. Метод аппроксимаций
   - Аппроксимация схем
   - Аппроксимация функций
3. Упражнения

Упражнения

1. Покажите, что для любого $d \geq 3$ функция $Parity_n$ может быть вычислена схемой над базисом $\{\wedge, \vee, \neg\}$ глубины $(d+1)$ размера $2^{\Omega(n^{1/d})}$.
2. Пусть $h(x) = \bigwedge\limits_{i \in S} x_i$, где $|S| < n$, и пусть a — 0-1-вектор, содержащий не менее $(d+1)$ единиц. Покажите, что $\bigoplus\limits_{b \leq a} h(b) = 0$.
3. Пусть ρ —p-случайная подстановка, $p = 1/\sqrt{n}$.
   (a) Пусть C — конъюнкт/дизъюнкт. Покажите, что C_ρ зависит от более, чем t переменных, с вероятностью не более $n^{-t/3}$.
   (b) Докажите ослабленную версию леммы о переключении: $\forall t, k \exists s : F$ — t-КНФ $\Rightarrow \Pr[F_\rho$ зависит от $\geq s$ переменных$] \leq n^{-k}$.

Подсказки

1. Расмотреть схему глубины d с гейтами, считающими $Parity_{n^{1/d}}$. Каждый такой гейт заменить на КНФ/ДНФ размера $2^{n^{1/d}}$. При этом глубина увеличится вдвое; для уменьшения использовать ассоциативность AND и OR.
2. Рассмотерть два случая: либо $\forall i \in Sa_i = 1$, либо нет.
3. (a) Если C содержит $> m = t \log n$ литералов, то C_ρ — не константа с вероятностью $\leq ((1+p)/2)^m$; иначе C_ρ содержит хотя бы t переменных с вероятностью $\leq \binom{m}{t} p^t$.
   (b) Индукция по t. База: $s(1,k) = 3k$. Для перехода рассмотреть максимальное множество попарно непересекающихся дизъюнктов F. Пусть Y — объединение множеств переменных этих дизъюнктов. Если $|Y| \geq k2^t \log n$, то F_ρ — константа с вероятностью $\geq 1 - n^{-k}$. Иначе $\forall i$ в Y остается $> i$ неприсвоенных переменных с вероятностью $\leq n^{-i/3}$. Взять $i = 4k$ и установить этим $4k$ переменным из Y константные значения всеми возможноыми способами, чтобы получить $(t-1)$-КНФ и применить предположение индукции.

Спасибо за внимание!