Семинар по сложности булевых функций

Лекция 7: Монотонные формулы

Е. Деменков

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

06.11.2011

План лекции

1. Введение
2. Нижняя оценка для квадратичных функций
3. Суперполиномиальная нижняя оценка

План лекции

1. Введение
2. Нижняя оценка для квадратичных функций
3. Суперполиномиальная нижняя оценка

Введение

Определение

Покрывающее число $\chi(f)(\chi_+(f))$ это минимальное количество монохроматических(положительных) прямоугольников (попарно не пересекающихся), покрывающих все ребра $S_f = f^{-1}(1) \times f^{-1}(0)$.

Введение

Определение

Покрывающее число $\chi(f)(\chi_+(f))$ это минимальное количество монохроматических(положительных) прямоугольников (попарно не пересекающихся), покрывающих все ребра $S_f = f^{-1}(1) \times f^{-1}(0)$.

Определение

Прямоугольник $A \times B$ монохроматический, если есть литерал z такой, что $z(a) = 1$ для всех $a \in A$ и $z(b) = 0$ для всех $b \in B$.

Введение

Определение

Покрывающее число $\chi(f)(\chi_+(f))$ это минимальное количество монохроматических(положительных) прямоугольников (попарно не пересекающихся), покрывающих все ребра $S_f = f^{-1}(1) \times f^{-1}(0)$.

Определение

Прямоугольник $A \times B$ монохроматический, если есть литерал z такой, что $z(a) = 1$ для всех $a \in A$ и $z(b) = 0$ для всех $b \in B$.
Положительно монохроматический, если $z = x_i$ для некоторого i.

Введение

Определение

Покрывающее число $\chi(f)(\chi_+(f))$ это минимальное количество монохроматических(положительных) прямоугольников (попарно не пересекающихся), покрывающих все ребра $S_f = f^{-1}(1) \times f^{-1}(0)$.

Определение

Прямоугольник $A \times B$ монохроматический, если есть литерал z такой, что $z(a) = 1$ для всех $a \in A$ и $z(b) = 0$ для всех $b \in B$.
Положительно монохроматический, если $z = x_i$ для некоторого i.

Замечание

Храпченко и Рычков доказали, что

$$L_+(f) \geq \chi_+(f).$$

И что с этим можно сделать?

И что с этим можно сделать?

Замечание

Рассмотрим матрицу $M : A \times B \to \mathbb{F}$, которая имеет большой ранг. Предположим, что любой минор M_R, образованный положительным монохроматическим прямоугольником R, имеет ранг не более, чем r. Тогда

И что с этим можно сделать?

Замечание

Рассмотрим матрицу $M : A \times B \to \mathbb{F}$, которая имеет большой ранг. Предположим, что любой минор M_R, образованный положительным монохроматическим прямоугольником R, имеет ранг не более, чем r. Тогда

$$L_+(f) \geq \chi_+(f) \geq \frac{rk(M)}{r}.$$

План лекции

Квадратичная функция графа

Определение

Пусть $G = ([n], E)$ – граф. Для него можно определить следующую монотонную(квадратическую) функцию

$$f_G(x_1, \ldots, x_n) = \bigvee_{\{i,j\} \in E} x_i x_j.$$

Квадратичная функция графа

Определение

Пусть $G = ([n], E)$ – граф. Для него можно определить следующую монотонную(квадратическую) функцию

$$f_G(x_1, \ldots, x_n) = \bigvee_{\{i,j\} \in E} x_i x_j.$$

Пример

Пусть $G = ([n], E)$ полный двудольный граф. $E = S \times T$, $S \cap T = \emptyset$ и $|S| = |T| = n/2$. При этом $|E| = n^2/4$ и f_G может быть вычислена, как монотонная формула линейного размера следующим образом:

$$F(x_1, \ldots, x_n) = \left(\bigvee_{i \in S} x_i\right) \wedge \left(\bigvee_{i \in T} x_i\right)$$

Теорема (Jukna 2008)

$G = (V, E)$ – граф без треугольников и квадратов. Тогда

$$L_+(f_G) \geq |E|.$$

Теорема (Jukna 2008)

$G = (V, E)$ – граф без треугольников и квадратов. Тогда

$$L_+(f_G) \geq |E|.$$

Пример

Рассмотрим проективное пространство $PG(2, q)$. В нем $q^2 + q + 1$ точка, $q + 1$ линия, каждая линия содержит $q + 1$ точку, любые две точки лежат на одной прямой, любые две прямые пересекаются в единственной точке.

Теорема (Jukna 2008)

$G = (V, E)$ – граф без треугольников и квадратов. Тогда

$$L_+(f_G) \geq |E|.$$

Пример

Рассмотрим проективное пространство $PG(2, q)$. В нем $q^2 + q + 1$ точка, $q + 1$ линия, каждая линия содержит $q + 1$ точку, любые две точки лежат на одной прямой, любые две прямые пересекаются в единственной точке. Рассмотрим двудольный граф, в котором в одной доле линии, во второй точки. Ребро соответствует тому, что точка принадлежит прямой.

Теорема (Jukna 2008)

$G = (V, E)$ – граф без треугольников и квадратов. Тогда

$$L_+(f_G) \geq |E|.$$

Пример

Рассмотрим проективное пространство $PG(2, q)$. В нем $q^2 + q + 1$ точка, $q + 1$ линия, каждая линия содержит $q + 1$ точку, любые две точки лежат на одной прямой, любые две прямые пересекаются в единственной точке. Рассмотрим двудольный граф, в котором в одной доле линии, во второй точки. Ребро соответствует тому, что точка принадлежит прямой. В этом графе $n = \Theta(q^2)$ вершин и $\Theta(q^3) = \Theta(n^{3/2})$ ребер.

Теорема (Jukna 2008)

$G = (V, E)$ – граф без треугольников и квадратов. Тогда

$$L_+(f_G) \geq |E|.$$

Пример

Рассмотрим проективное пространство $PG(2, q)$. В нем $q^2 + q + 1$ точка, $q + 1$ линия, каждая линия содержит $q + 1$ точку, любые две точки лежат на одной прямой, любые две прямые пересекаются в единственной точке. Рассмотрим двудольный граф, в котором в одной доле линии, во второй точки. Ребро соответствует тому, что точка принадлежит прямой. В этом графе $n = \Theta(q^2)$ вершин и $\Theta(q^3) = \Theta(n^{3/2})$ ребер. И в этом графе нет ни треугольников, ни квадратов.

План лекции

И еще немного определений

Определение

Пусть $A \subset 2^{[n]}$ - семейство 1-термов, а $B \subset 2^{[n]}$ - семейство 0-термов ($f(a) = 1$ для $a \in A$ и $f(\bar{b}) = 0$ для $b \in B$, где $\bar{b} = [n] \setminus b$). A, B кросс пересекающиеся, если $a \cap b \neq \emptyset$ для всех $a \in A$, $b \in B$.

И еще немного определений

Определение

Пусть $A \subset 2^{[n]}$ - семейство 1-термов, а $B \subset 2^{[n]}$ - семейство 0-термов ($f(a) = 1$ для $a \in A$ и $f(\bar{b}) = 0$ для $b \in B$, где $\bar{b} = [n] \setminus b$). A, B кросс пересекающиеся, если $a \cap b \neq \emptyset$ для всех $a \in A$, $b \in B$.

Определение

Пусть A, B – локально пересекающиеся, если для любого $b \in B$ может быть разделено на две не пустых части $b = b_0 \cup b_1$, что любое $a \in A$ пересекается только с одной частью.

И еще немного определений

Определение

Пусть $A \subset 2^{[n]}$ - семейство 1-термов, а $B \subset 2^{[n]}$ - семейство 0-термов ($f(a) = 1$ для $a \in A$ и $f(\bar{b}) = 0$ для $b \in B$, где $\bar{b} = [n] \setminus b$). A, B кросс пересекающиеся, если $a \cap b \neq \emptyset$ для всех $a \in A$, $b \in B$.

Определение

Пусть A, B – локально пересекающиеся, если для любого $b \in B$ может быть разделено на две не пустых части $b = b_0 \cup b_1$, что любое $a \in A$ пересекается только с одной частью.

Определение

Для любых локально пересекающихся A, B можно определить следующую(ортогональную) матрицу $D_{A,B}$:

$$D[a, b] = \begin{cases} 0 & \text{if } a \cap b_0 \neq \emptyset \\ 1 & \text{if } a \cap b_1 \neq \emptyset \end{cases}.$$

Лемма Gal-Pudlak

Лемма (Gal-Pudak 2003)

Пусть A множество 1-термов, B множество 0-термов. Если A, B локально пересекающиеся, тогда

$$L_+(f) \geq rk(D_{A,B}).$$

Доказательство

Для этого достаточно доказать, что $rk(M_R) \leq 1$, для любого монохроматического подпрямоугольника $R = A' \times B'$ прямоугольника $A \times B$.

Доказательство

Для этого достаточно доказать, что $rk(M_R) \leq 1$, для любого монохроматического подпрямоугольника $R = A' \times B'$ прямоугольника $A \times B$.

Мы знаем, что $f(a) = 1$ для всех $a \in A'$ и $f(\bar{b}) = 1$ для всех $b \in B'$. R монохроматический. Так что есть $i \in [n]$, что

$$i \in a \setminus \bar{b}, \text{ для всех } a \in A', b \in B'.$$

Доказательство

Для этого достаточно доказать, что $rk(M_R) \leq 1$, для любого монохроматического подпрямоугольника $R = A' \times B'$ прямоугольника $A \times B$.
Мы знаем, что $f(a) = 1$ для всех $a \in A'$ и $f(\bar{b}) = 1$ для всех $b \in B'$. R монохроматический. Так что есть $i \in [n]$, что

$$i \in a \setminus \bar{b}, \text{ для всех } a \in A', b \in B'.$$

Поскольку, A', B' локально пересекающиеся, любое $b \in B'$ можно разделить на две части, $b = b_0 \cup b_1$, что любое $a \in A'$ пересекается только с одной частью.

Доказательство

Для этого достаточно доказать, что $rk(M_R) \leq 1$, для любого монохроматического подпрямоугольника $R = A' \times B'$ прямоугольника $A \times B$.

Мы знаем, что $f(a) = 1$ для всех $a \in A'$ и $f(\bar{b}) = 1$ для всех $b \in B'$. R монохроматический. Так что есть $i \in [n]$, что

$$i \in a \setminus \bar{b}, \text{ для всех } a \in A', b \in B'.$$

Поскольку, A', B' локально пересекающиеся, любое $b \in B'$ можно разделить на две части, $b = b_0 \cup b_1$, что любое $a \in A'$ пересекается только с одной частью. Тогда B' можно разделить на 2 части $B_0 = \{b \in B' | i \in b_0\}$ и $B_1 = \{b \in B' | i \in b_1\}$ $A' \times B_0$ – 0-матрица, а $A' \times B_1$ – 1-матрица.

Доказательство

Для этого достаточно доказать, что $rk(M_R) \leq 1$, для любого монохроматического подпрямоугольника $R = A' \times B'$ прямоугольника $A \times B$.

Мы знаем, что $f(a) = 1$ для всех $a \in A'$ и $f(\bar{b}) = 1$ для всех $b \in B'$. R монохроматический. Так что есть $i \in [n]$, что

$$i \in a \setminus \bar{b}, \text{ для всех } a \in A', b \in B'.$$

Поскольку, A', B' локально пересекающиеся, любое $b \in B'$ можно разделить на две части, $b = b_0 \cup b_1$, что любое $a \in A'$ пересекается только с одной частью. Тогда B' можно разделить на 2 части $B_0 = \{b \in B' | i \in b_0\}$ и $B_1 = \{b \in B' | i \in b_1\}$ $A' \times B_0$ – 0-матрица, а $A' \times B_1$ – 1-матрица. А значит ранг исходной матрицы $A \times B$ не превосходит 1. $\square$

Ортогональная матрица

Определение

Пусть $A \subset 2^{[n]}$ и $T : A \to 2^{[n]}$ некое отображение. T контрактор если для любого $a \in A$ $T(a) \subset a$ и для любого другого $a' \in A$, $a \neq a'$ $T(a) \not\subseteq a'$. Если такое T существует, то A называют антицепью.

Ортогональная матрица

Определение

Пусть $A \subset 2^{[n]}$ и $T : A \to 2^{[n]}$ некое отображение. T контрактор если для любого $a \in A$ $T(a) \subset a$ и для любого другого $a' \in A$, $a \neq a'$ $T(a) \not\subseteq a'$. Если такое T существует, то A называют антицепью.

Определение

Пусть A –антицепь, а T – контрактор. Ортогональная матрица(D_A) множества A это булева матрица, в которой столбцы– элементы A, а строки это все $b \subset T(a)$ для всех $a \in A$. $D_A[a, b] = 1$ тогда и только тогда $a \cap b = \emptyset$.

Лемма

Для любой антицепи A и ее ортогональной матрицы D_A, $rk(D_A) = |A|$.

Лемма

Для любой антицепи A и ее ортогональной матрицы D_A, $rk(D_A) = |A|$.

Доказательство

Основная ортогональная матрица D_m это булева матрица размера $2^m \times 2^m$, у которой строки и столбцы отмечены всеми подмножествами m-элементного множества. Эта матрица имеет полный ранг 2^m(это легко доказывается по индукции).

Лемма

Для любой антицепи A и ее ортогональной матрицы D_A, $rk(D_A) = |A|$.

Доказательство

Основная ортогональная матрица D_m это булева матрица размера $2^m \times 2^m$, у которой строки и столбцы отмечены всеми подмножествами m-элементного множества. Эта матрица имеет полный ранг 2^m(это легко доказывается по индукции).
Достаточно показать, что все строки в нашей исходной матрице линейно независимы.

Лемма

Для любой антицепи A и ее ортогональной матрицы D_A, $rk(D_A) = |A|$.

Доказательство

Основная ортогональная матрица D_m это булева матрица размера $2^m \times 2^m$, у которой строки и столбцы отмечены всеми подмножествами m-элементного множества. Эта матрица имеет полный ранг 2^m(это легко доказывается по индукции).

Достаточно показать, что все строки в нашей исходной матрице линейно независимы. Зафиксируем $a \in A$. Пусть D_a матрица индуцированная $b \in T(a)$ и все $a' \in A$ заменяются на $a' \cap T(a)$.

Лемма

Для любой антицепи A и ее ортогональной матрицы D_A, $rk(D_A) = |A|$.

Доказательство

Основная ортогональная матрица D_m это булева матрица размера $2^m \times 2^m$, у которой строки и столбцы отмечены всеми подмножествами m-элементного множества. Эта матрица имеет полный ранг 2^m(это легко доказывается по индукции).
Достаточно показать, что все строки в нашей исходной матрице линейно независимы. Зафиксируем $a \in A$. Пусть D_a матрица индуцированная $b \in T(a)$ и все $a' \in A$ заменяются на $a' \cap T(a)$.
Поскольку D_m имеет полный ранг, то D_a также имеет полный ранг. $\square$

k-разделяемый граф

Определение

Пусть $G = (U \cup V, E)$ – двудольный граф. Он *k-разделяем*, если для любых двух не пересекающихся подмножеств X, Y множества U, размера не более k, есть вершина $v \in V$, которая соединена со всеми вершинами из X и не с одной вершиной из Y.

k-разделяемый граф

Определение

Пусть $G = (U \cup V, E)$ – двудольный граф. Он k-разделяем, если для любых двух не пересекающихся подмножеств X, Y множества U, размера не более k, есть вершина $v \in V$, которая соединена со всеми вершинами из X и не с одной вершиной из Y.

Определение

Для k-разделяемого графа определим A как множество $a \subseteq U \cup V$ таких, что $|a \cap U| = k$ и $a \cap V$ все вершины из V соединенными со всеми вершинами из $a \cap U$.

Функция Палей

Определение

Для k-разделяемого графа G, определим

$$f_{G,k} = \bigvee_{a \in A} \bigwedge_{i \in a} x_i.$$

Функция Палей

Определение

Для k-разделяемого графа G, определим

$$f_{G,k} = \bigvee_{a \in A} \bigwedge_{i \in a} x_i.$$

Замечание

Для любого графа G на $2n$ вершинах и для любого $1 \le k \le n$

$$L_+(f_{G,k}) \le 2n \binom{n}{k}.$$

Теорема

Если граф G k-разделим, тогда

$$L_+(f_{G,k}) \geq \binom{n}{k}.$$

Теорема

Если граф G k-разделим, тогда

$$L_+(f_{G,k}) \geq \binom{n}{k}.$$

Доказательство

Определим B, как семейство множеств $b = b_0 \cup b_1$, таких что $b_0 \subset U, |b_0| \geq k$, а b_1 множество вершин из V, у которых нет соседей в b_0.

Теорема

Если граф G k-разделим, тогда

$$L_+(f_{G,k}) \geq \binom{n}{k}.$$

Доказательство

Определим B, как семейство множеств $b = b_0 \cup b_1$, таких что $b_0 \subset U, |b_0| \geq k$, а b_1 множество вершин из V, у которых нет соседей в b_0. Поскольку граф k-разделяем, то $b_0 \cap a = \emptyset$ тогда и только тогда, когда $b_1 \cap a \neq \emptyset$, для $a \in A$.

Теорема

Если граф G k-разделим, тогда

$$L_+(f_{G,k}) \geq \binom{n}{k}.$$

Доказательство

Определим B, как семейство множеств $b = b_0 \cup b_1$, таких что $b_0 \subset U, |b_0| \geq k$, а b_1 множество вершин из V, у которых нет соседей в b_0. Поскольку граф k-разделяем, то $b_0 \cap a = \emptyset$ тогда и только тогда, когда $b_1 \cap a \neq \emptyset$, для $a \in A$. Тогда A, B локально пересекающиеся, и разделимы $f = f_{G,k}$, то размер формулы, вычисляющей f как минимум $rk(D_{A,B})$.

Теорема

Если граф G k-разделим, тогда

$$L_+(f_{G,k}) \geq \binom{n}{k}.$$

Доказательство

Определим B, как семейство множеств $b = b_0 \cup b_1$, таких что $b_0 \subset U, |b_0| \geq k$, а b_1 множество вершин из V, у которых нет соседей в b_0. Поскольку граф k-разделяем, то $b_0 \cap a = \emptyset$ тогда и только тогда, когда $b_1 \cap a \neq \emptyset$, для $a \in A$. Тогда A, B локально пересекающиеся, и разделимы $f = f_{G,k}$, то размер формулы, вычисляющей f как минимум $rk(D_{A,B})$. Переобозначим строки a на $a' = a \cap U$ и столбцы b на $b' = b \cap U$. Получим матрицу M, она будет ортогональной для $A' = \{a \cap U \mid a \in A\}$ (с тривиальным контрактором).

Теорема

Если граф G k-разделим, тогда

$$L_+(f_{G,k}) \geq \binom{n}{k}.$$

Доказательство

Определим B, как семейство множеств $b = b_0 \cup b_1$, таких что $b_0 \subset U, |b_0| \geq k$, а b_1 множество вершин из V, у которых нет соседей в b_0. Поскольку граф k-разделяем, то $b_0 \cap a = \emptyset$ тогда и только тогда, когда $b_1 \cap a \neq \emptyset$, для $a \in A$. Тогда A, B локально пересекающиеся, и разделимы $f = f_{G,k}$, то размер формулы, вычисляющей f как минимум $rk(D_{A,B})$. Переобозначим строки a на $a' = a \cap U$ и столбцы b на $b' = b \cap U$. Получим матрицу M, она будет ортогональной для $A' = \{a \cap U \mid a \in A\}$ (с тривиальным контрактором). Тогда

$$rk(D_{A,B}) = rk(D_{A'}) = |A'| = \binom{n}{k}$$

Функция Палей

Определение

Пусть p простое число, сравнимое с 1 по модулю 4. Граф Палей это двудольный граф $G = (U \cup V, E)$, где $U = V = GF(n)$. И ребро между $u \in U$ и $v \in V$, если и только если, $u - v$ ненулевой квадрат в $GF(n)$.

Функция Палей

Определение

Пусть p простое число, сравнимое с 1 по модулю 4. Граф Палей это двудольный граф $G = (U \cup V, E)$, где $U = V = GF(n)$. И ребро между $u \in U$ и $v \in V$, если и только если, $u - v$ ненулевой квадрат в $GF(n)$.

Замечание

-1 корень в $GF(n)$.

Функция Палей

Определение

Пусть p простое число, сравнимое с 1 по модулю 4. Граф Палей это двудольный граф $G = (U \cup V, E)$, где $U = V = GF(n)$. И ребро между $u \in U$ и $v \in V$, если и только если, $u - v$ ненулевой квадрат в $GF(n)$.

Замечание

-1 корень в $GF(n)$.

Определение

Функция Палей

$$Paley_n(x) = f_{G,k}(x), \text{где } k = \lfloor (\log n)/3 \rfloor.$$

Суперполиномиальная оценка

Суперполиномиальная оценка

Теорема

$$L_+(Paley_n) = n^{\Theta(\log n)}.$$

Суперполиномиальная оценка

Теорема

$$L_+(Paley_n) = n^{\Theta(\log n)}.$$

Доказательство

Пусть $G = (U \cup V, E)$ двудольный $n \times n$ граф Палей.

Суперполиномиальная оценка

Теорема

$$L_+(Paley_n) = n^{\Theta(\log n)}.$$

Доказательство

Пусть $G = (U \cup V, E)$ двудольный $n \times n$ граф Палей. Пусть A, B – два непересекающихся подмножества U размера k. Обозначим через $v(A, B)$ количество вершин в V, соединенных с A и не соединенных с B.

Суперполиномиальная оценка

Теорема

$$L_+(Paley_n) = n^{\Theta(\log n)}.$$

Доказательство

Пусть $G = (U \cup V, E)$ двудольный $n \times n$ граф Палей. Пусть A, B – два непересекающихся подмножества U размера k. Обозначим через $v(A, B)$ количество вершин в V, соединенных с A и не соединенных с B. Тогда теоремы Weil(1948), Graham и Spencer(1971) и Bollobas и Thomason(1981) доказывают:

$$|v(A, B) - 2^{-k} n| \leq k\sqrt{n}$$

Суперполиномиальная оценка

Теорема

$$L_+(Paley_n) = n^{\Theta(\log n)}.$$

Доказательство

Пусть $G = (U \cup V, E)$ двудольный $n \times n$ граф Палей. Пусть A, B – два непересекающихся подмножества U размера k. Обозначим через $v(A, B)$ количество вершин в V, соединенных с A и не соединенных с B. Тогда теоремы Weil(1948), Graham и Spencer(1971) и Bollobas и Thomason(1981) доказывают:

$$|v(A, B) - 2^{-k}n| \leq k\sqrt{n}$$

Так что $v(A, B) > 0$ как только $k2^k \leq \sqrt{n}$. G k-разделим, для $k = \lfloor (\log n)/3 \rfloor$. □

Верхняя оценка

Теорема

Пусть $A, B \subset 2^{[n]}$ *локально непересекающиеся. Тогда ранг ортогональной матрицы* $D_{A,B}$ *не превосходит* $n^{O(\log n)}$.

Спасибо за внимание!