Семинар по сложности булевых функций

Лекция 6: Коммуникационная сложность и глубина схем

А. Головнёв

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

06.11.2011

План лекции

1. Введение
2. Коммуникационная сложность
3. Покрытие прямоугольниками
4. Игры Карчмера-Вигдерсона
5. Задачи

План лекции

1. Введение
2. Коммуникационная сложность
3. Покрытие прямоугольниками
4. Игры Карчмера-Вигдерсона
5. Задачи

История и применения

Коммуникационная сложность

- Введена Яо в 1979 году.
- Служит мерой количества общения для распределённых вычислений.
- Разработка микросхем.
- Оптимизация компьютерных сетей.
- Структуры данных.
- Схемная сложность.

Определение

- Алиса и Боб хотят совместно вычислить значение функции $f : X \times Y \to Z$.
- Алиса знает $x \in X$.
- Боб знает $y \in Y$.
- Алиса и Боб знают функцию f.
- Существует двухсторонний канал связи.
- Цель: вычислить значение функции $f(x, y)$, отправив по каналу минимальное количество битов.

Замечания

- Алиса и Боб дружат!
- Хотя бы один из них должен вычислить значение.
- f можно рассматривать как отношение $f \subseteq X \times Y \times Z$.

Примеры

EQ

$X = \{0,1\}^n$, $Y = \{0,1\}^n$
$f(x, y) = 1 \leftrightarrow x = y$.
Алиса отправляет Бобу все n битов, Боб выдаёт ответ.
Отправили n битов.

Parity

$X = \{0,1\}^n$, $Y = \{0,1\}^n$
$f(x, y) = x_1 \oplus x_2 \oplus \ldots \oplus y_1 \oplus \ldots \oplus y_n$.
Алиса отправляет Бобу $x_1 \oplus x_2 \oplus \ldots \oplus x_n$, Боб выдаёт ответ.
Отправили 1 бит.

Модели коммуникации

- Вероятностные модели.
- Протоколы с несколькими участниками.
- Квантовые модели.
- Недетерминированные модели.
- Коммуникационная сложность в среднем.
- Ассиметрические протоколы.
- Вычисление небулевых функций.
- Вычисление отношений.

Примеры

Лемма
Коммуникационная сложность EQ в вероятностном протоколе с открытым доступом равна единице, в вероятностном протоколе с закрытым доступом — $O(\log n)$.

Лемма
Коммуникационная сложность функции $f(x, y, z) = \oplus Maj(x_i, y_i, z_i)$ в протоколе для троих игроков равна двум.

План лекции

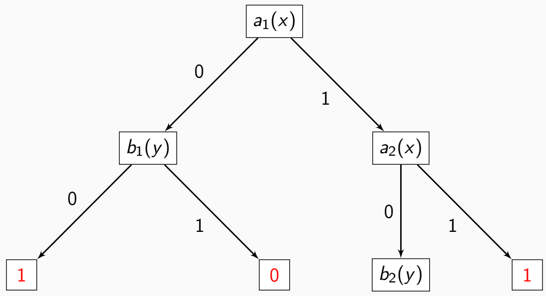
1. Введение
2. Коммуникационная сложность
3. Покрытие прямоугольниками
4. Игры Карчмера-Вигдерсона
5. Задачи

Коммуникационный протокол

Коммуникационным протоколом (деревом) называется бинарное дерево, листья которого помечены элементами Z, а все остальные вершины – функциями $a_i\colon X \to \{0,1\}$ или $b_j\colon Y \to \{0,1\}$.

Вычисление по потоколу происходит следующим образом: начиная от корня движемся по дереву к тому потомку, куда указывает функция, стоящая в вершине. Например, если в вершине функция a_i и её значение 0 — движемся к левому потомку, 1 — к правому (Значение функции a_i вычисляет Алиса, b_j – Боб).
В листе, к которому приводит путь из корня, должно стоять значение функции $f(x, y)$.

Пример коммуникационного протокола



Комбинаторные прямоугольники

Определение
Прямоугольником называется множество $R = R_0 \times R_1$, где $R_0 \subseteq X$ и $R_1 \subseteq Y$.

Определение
Прямоугольником называется множество $R \subseteq X \times Y$, для которого выполняется "cut-and-paste" правило:

$$(x, y), (x', y') \in R \quad \Rightarrow \quad (x, y'), (x', y) \in R.$$

Определение
Пусть задана функция $f\colon X \times Y \to Z$. Прямоугольник R называется одноцветным, если f сохраняет значение на всём прямоугольнике.

Одноцветные прямоугольники

Лемма
Если T — коммуникационное дерево, то для любой вершины v:

$$S_v = \{(x, y) \in X \times Y \,|\, \text{вход } (x, y) \text{ достигает вершину } v\}$$

является прямоугольником.
Более того, если v — лист, то прямоугольник S_v является одноцветным.

Доказательство.
Индукция по глубине v.
Если v — корень, то $S_v = X \times Y$ — прямоугольник.
Иначе, пусть w — отец v. $S_w = A \times B$ — по предположению индукции.

$$S_v = S_w \cap \{(x, y) | a_w(x) = 0\} =$$
$$(A \times B) \cap \{(x, y) | a_w(x) = 0\} = (A \cap \{x | a_w(x) = 0\}) \times B$$

□

Коммуникационная сложность

Определение
Глубина коммуникационного дерева — максимальное количество рёбер на пути от корня до листа.

Определение
Коммуникационная сложность $c(f)$ функции f — это минимальная глубина коммуникационного дерева для функции f.

Коммуникационная сложность EQ

Лемма
$c(EQ) = n$.

Доказательство.
$X = \{0,1\}^n$, $Y = \{0,1\}^n$.
$f(x, y) = 1 \leftrightarrow x = y$.
Мы уже показали, что $c(EQ) \leq n$.
Покажем, что $c(EQ) \geq n$.
Кажый вход (x, x) достигает 1-листа.
Из леммы 3, если v — 1-лист, то S_v — прямоугольник.
Если $(x, x) \in S_v$ и $(y, y) \in S_v$, то $(x, y) \in S_v$ — противоречие $(x \neq y)$.
Значит, листьев хотя бы $|f^{-1}(1)| = 2^n$.
Следовательно, глубина дерева не менее $\log(2^n) = n$. □

Меры сложности

Мы будем рассматривать следующие меры сложности:

- $c(f)$ — наименьшая глубина коммуникационного дерева для функции f.
- $L(f)$ — наименьшее количество листьев коммуникационного дерева для функции f.
- $\chi(f)$ — наименьшее t такое, что $X \times Y$ может быть покрыто с помощью t одноцветных непересекающихся прямоугольников.

Из леммы 3 мы получаем следующее соотношение:

$$c(f) \geq \log L(f) \geq \log \chi(f).$$

План лекции

Балансировка протоколов

Лемма

$$c(f) \leq 2\log_{3/2} L(f).$$

Доказательство

Рассмотрим протокол для функции f, в котором L листьев.
Мы хотим построить протокол, глубина которого не больше $2\log_{3/2} L$.
Индукция по количеству листьев L.
$L = 1$ — тривиальный случай.
Выбираем вершину v так, чтобы количество листьев $|T_v|$ в поддереве удовлетворяло следующему соотношению:

$$L/3 \leq |T_v| \leq 2L/3.$$

Оба игрока знают дерево T, поддерево T_v.

Продолжение доказательства

Доказательство.

Отправив друг другу по одному биту, Алиса и Боб узнают: $(x, y) \in S_v$ или $(x, y) \notin S_v$.

$$c(L) \leq 2 + c(2L/3) \leq 2\log_{3/2} L.$$

□

Получаем:

$$c(f) = \Theta(\log L(f)).$$

Таким образом, оценивая минимальную глубину коммуникационного протокола, мы оцениваем и минимальное количество листьев в коммуникационном протоколе.

Игра "Найди прямоугольник"

Теперь мы хотим показать, что $c(f) = O(\log^2 \chi(f))$.
Пусть у нас есть набор прямоугольников R (не обязательно непересекающихся), которые покрывают $X \times Y$.
Каждый прямоугольник имеет метку.
Мы вводим одно требование: если два прямоугольника R_1 и R_2 имеют различные метки, то $R_1 \cap R_2 = \emptyset$.

Игра "Найди прямоугольник":

Алиса знает x, Боб знает y.
Общая цель Алисы и Боба — найти метку прямоугольника, покрывающего (x, y).

Лемма о пересечении прямоугольников

Лемма

Ни один прямоугольник в R не может пересекать одновременно больше половины иначе покрашенных прямоугольников по строкам и более половины иначе покрашенных прямоугольников по столбцам.

Доказательство.

Пусть такой прямоугольник R существует. Тогда существует прямоугольник T, метка которого отличается от метки R, пересекающий R по строкам и столбцам. Это нарушает правило расстановки меток. □

Коммуникационная сложность игры

Пусть R — покрытие помеченными прямоугольниками множества $X \times Y$.
Пусть $c(f)$ — коммуникационная сложность игры "Найди прямоугльник". Тогда справедлива следующая лемма:

Лемма

$$c(R) \leq 2(\log |R|)^2.$$

Прямоугольник $S = S_0 \times S_1$ назовём Алисиным, если $x \in S_0$.
Положим $r = \lceil \log |R| \rceil$.
Для доказательства леммы построим протокол с r раундами и $r + 1$ битом в каждом раунде.
На каждой итерации алгоритм будет уменьшать количество рассматриваемых прямоугольников в 2 раза.

Доказательство леммы

Доказательство.

Каждая итерация алгоритма выглядит следующим образом:

1. Если все прямоугольники Алисы имеют одинаковую метку, то Алиса сообщает ответ.
2. Алиса пытается найти среди своих прямоугольников такой прямоугольник S, который пересекает по строкам не более половины иначе раскрашенных прямоугольников. Если такой прямоугольник найден, то Алиса отправляет его номер Бобу. Теперь оба игрока оставляют лишь те прямоугольники, которые пересекаются с S по строкам.
3. Если Алисе не удалось найти такой прямоугольник, то она сообщает об этом Бобу, используя один бит.
4. Тогда по лемме 6, Боб может найти свой прямоугольник, который пересекается не более, чем с половиной иначе раскрашенных прямоугольников по столбцам.

□

Оценка сверху

Лемма

Для любой функции $f: X \times Y \to Z, \quad c(f) \le 2(\log \chi(f))^2$.

Доказательство.

Пусть R — оптимальное покрытие $X \times Y$ непересекающимися одноцветными прямоугольниками. $|R| = \chi(f)$. Применив лемму 7, мы получим:

$$c(f) \le 2(\log \chi(f))^2.$$

□

Покрытие матрицы

Лемма

Пусть матрица A может быть покрыта при помощи t (не обязательно непересекающихся) одноцветных подматриц. Тогда A может быть покрыта $t^{2\log t}$ непересекающимися одноцветными подматрицами.

Доказательство.

По лемме 7, коммуникационная сложность игры "Найди прямоугольник" $c(f) \le 2(\log t)^2$.
Каждый лист коммуникационного протокола будет соответствовать одноцветной подматрице.
Следовательно, мы получаем покрытие с не более, чем $2^c = t^{2\log t}$ непересекаюшимися одноцветными прямоугольниками.

□

Связь с рангом матрицы

Лемма

Рангом матрицы M называется наименьшее число l, что матрица M может быть представлена следующим видом:

$$M = \sum_{i=1}^{l} B_i,$$

где B_i — $n \times n$ матрица ранга 1.

Теорема

Для любой функции f:

$$\chi(f) \ge rank(M(f)).$$

Лемма

$$c(EQ) = n.$$

Резюме

$$2\log_{3/2} L(f) \ge c(f) \ge \log L(f).$$

$$2(\log \chi(f))^2 \ge c(f) \ge \log \chi(f).$$

$$\chi(f) \ge rank(M(f)).$$

План лекции

Игры Карчмера-Вигдерсона

Определение

Пусть $S = X \times Y, \quad X, Y \subseteq \{0,1\}^n$ и $X \cap Y = \emptyset$.
Например, $S = f^{-1}(1) \times f^{-1}(0)$.
Игра Карчмера-Вигдерсона заключается в следующем:

- Алиса получает $x \in X$.
- Боб получает $y \in Y$.
- Цель: и Алиса и Боб должны узнать i, что $x_i \ne y_i$.

Нам известно, что:

$$\log \chi(S) \le c(S) \le 2(\log \chi(S))^2.$$

Пример

Лемма

$$\chi(\oplus_n) \le 4n^2, \quad c(\oplus_n) \le 2\log n + 2.$$

Доказательство.

Докажем, что $\chi(\oplus_n) \le n^2$ для случая, когда n является степенью двойки. В остальных случаях дополним строку нулями.
Алиса и Боб высылают чётность первой половины битов.
Далее игра продолжается на той половине входной строки, в которой чётность не совпадает.
Так мы получаем протокол с $2\log n$ битами.
Следовательно, разложение в непересекающиеся прямоугольники содержит не более $2^{2\log n} = n^2$ прямоугольников.

□

Теорема Карчмера-Вигдерсона

Обозначим через $D(f)$ минимальную глубину схемы де Моргана, вычисляющей функцию f.
Пусть $c(f)$ — коммуникационная сложность игры Карчмера-Вигдерсона на прямоугольнике $f^{-1}(1) \times f^{-1}(0)$.

Теорема

$$D(f) = c(f).$$

Отдельно докажем верхнюю и нижнюю оценки на $D(f)$.

От схемы к протоколу

Лемма

$$c(f) \leq D(f).$$

Доказательство.

- У Алисы x, что $f(x) = 1$.
- у Боба y, что $f(y) = 0$.
- Алиса и Боб имеют схему для функции f глубины D.
- Начиная от корня движемся по схеме.
- Если гейт AND, $f = f_0 \wedge f_1$, то Боб высылает i, что $f_i(y) = 0$.
- Если гейт OR, $f = f_0 \vee f_1$, то Алиса высылает i, что $f_i(x) = 1$.
- Таким образом, не более, чем за D шагов, они придут к переменной z_i или её отрицанию.
- Ответ: $x_i \neq y_i$.

□

Замечание

Последний результат можно обобщить на схемы входной степени больше двух.

Лемма

$c(f) = O(d \log S)$, где S — наибольшая входная степень гейта.

Доказательство изменится лишь в том, что для передачи i нам потребуется не 1, а $\log S$ битов.

От протокола к схеме

Лемма

$$D(f) \leq c(f).$$

Доказательство

Для каждого прямоугольника
$S = A \times B, \quad A \subseteq f^{-1}(1), \quad B \subseteq f^{-1}(0)$:

$$D(f) \leq c(S).$$

Индукция по $c(S)$.
Если $c = 0$, то существует i, что $x_i \neq y_i$ для всех $(x, y) \in S$.

Продолжение доказательства

Доказательство.

Шаг индукции:
Пусть первый ход делает Алиса. Тогда существует такое разбиение $A = A_0 \cup A_1, A_0 \cap A_1 = \emptyset$, что для $x \in A_0$ Алиса отправляет ноль, для $x \in A_1$ Алиса отправляет единицу.
По предположению индукции, существует f_0, что:

$$f_0(A_0) = 1 \quad f_0(B) = 0 \quad D(f_0) \leq c - 1,$$

$$f_1(A_1) = 1 \quad f_1(B) = 0 \quad D(f_1) \leq c - 1.$$

Теперь определим $f = f_0 \vee f_1$. Тогда, $f(A) = 1, f(B) = 0$,

$$D(f) \leq 1 + \max(D(f_0), D(f_1)) \leq c.$$

□

Минтермы и макстермы

Определение

Минтерм (макстерм) монотонной булевой функции f — это минимальное по включению множество переменных, означив которые единицей (нулём), мы гарантируем, что значение f будет единицей (нулём).

Каждый макстерм пересекает каждый минтерм.
$Min(f)$ — множество всех минтермов монотонной функции f.
$Max(f)$ — множество всех макстермов монотонной функции f.

Монотонная глубина схем

- Алиса получает $m \in Min$.
- Боб получает $M \in Max$.
- Цель: найти общий элемент в $m \cap M$.

$c_+(f)$ — коммуникационная сложность этой игры.
$D_+(f)$ — минимальная глубина монотонной схемы де Моргана, вычисляющей f.

Теорема

Для любой монотонной функции f:

$$D_+(f) = c_+(f).$$

План лекции

Упражнения

- Пусть f — k-КНФ формула с m клозами. Показать, что для функции f существует протокол игры Карчмера-Вигдерсона с одним раундом, в котором Боб отправляет $\log m$ битов, Алиса отправляет $\log k$ битов.
- Показать, что для любой функции f существует протокол игры Карчмера-Вигдерсона, в котором на каждом раунде Боб отправляет 2^a битов, Алиса отправляет a битов, количество раундов $r \leq D(f)/a$.
  Подсказка: взять лучшую схему для f, разделить её на уровни глубины a. Каждый уровень может быть представлен как 2^a-КНФ с 2^{2^a} клозами. Теперь надо воспользоваться предыдущей задачей.

Ещё одно упражнение

- (Бродал, Хасфилд, 1996) Доказать, что для любой симметрической булевой функции n аргументов $D(f) = O(\log n)$.
  Подсказака: Рассмотрим следующую коммуникационную игру. $A, B \subseteq [n]$ такие, что $|A| \neq |B|$.
  Цель: найти элемент из симметрической разницы $(A - B) \cup (B - A)$.
  Необходимо разработать коммуникационный протокол для этой игры со сложностью $O(\log n)$.
  Если чётности $|A|$ и $|B|$ различны, то из леммы 13, бинарным поиском получаем $O(\log n)$ битов коммуникации. Если же чётности одинаковые, то следует использовать более сложный бинарный поиск.
  Рассмотрите $A^{l,s} = A \cap \{l, l+1, \ldots, l+s-1\}$, храните младший индекс, в котором $|A^{l,s}|$ и $|B^{l,s}|$ различаются.

Открытые задачи

- Улучшить верхнюю оценку на коммуникационную сложность задачи MOD_3. Лучшая известная оценка равна $2.881 \log_2 n$.
- Известно, что коммуникационная сложность задачи Thr_2 равна $\log_2 n + \log_2 \log_2 n$. Доказать такую нижнюю оценку на количество одноцветных прямоугольников.

Спасибо за внимание!