Лекция 5

Нижние оценки для CP. Нижняя оценка для цейтинских формул в Res (21.10.2010)

(Конспект: В. Опарин)

В данной лекции будут представлены два метода для получения нижних оценок на длины доказательств: монотонная интерполяция и нижняя оценка на ширину дизъюнкций.

5.1 Монотонная интерполяция: нижняя оценка для CP

Пусть $G_0(\bar{x},\bar{y})$, $G_1(\bar{x},\bar{z})$ задают два непересекающихся **NP**-множества. Будем говорить, что система обладает свойством эффективной интерполяции, если по доказательству π формулы $G_0 \vee G_1$ можно получить схему $C(\bar{x})$ полиномиального от длины доказательства размера, разделяющую соответствующие множества, т.е. такую, что

$$G_{C(\bar{x})} \notin \text{TAUT}.$$

То есть мы научимся разделять **NP**-пару за полиномиальное от размера доказательства время. Если у нас имеются нижние оценки на разделение **NP**-пары, мы сможем оценить и длины доказательств. Конечно, экспоненциальные нижние оценки для произвольных схем не известны, однако, имеются оценки для подклассов — например, для монотонных схем. Чтобы ими воспользоваться, по доказательству придётся строить не простую схему, а монотонную. Естественно, это можно сделать не для каждой системы и не для каждой формулы.

5.1.1 Монотонная интерполяция

Будем говорить, что система обладает свойством эффективной монотонной интерполяции, если из доказательства соответствующей формулы можно построить монотонную разделяющую схему.

Определение 5.1. *Булева (*соответственно, *арифметическая) схема* — это ациклический направленный граф, каждая вершина которого либо не имеет ни одного входящего ребра (такие вершины называются входами схемы, или переменными), либо имеет несколько входящих ребер (такие вершины называются гейтами). Каждый гейт помечен булевой (соответственно, арифметической) функцией. Некоторые гейты или входы помечены как выходы.

Определение 5.2. Схема является *монотонной*, если каждый ее гейт монотонен (т.е. если аргументы его не уменьшаются, то и значение не уменьшается).

Гейтами булевой монотонной схемы могут быть дизъюнкции или конъюнкции. В случае арифметических схем — ими могут быть сложение, умножение и другие монотонные операции. Отрицание, очевидно, не монотонно.

Зададимся вопросом о существовании монотонных схем для некоторой задачи. В общем случае их может и не быть, так как монотонными операциями можно вычислить только монотонные функции. Нас будет интересовать вопрос о существовании в графе клики некоторого размера — эта функция, очевидно, монотонна (если добавить в граф рёбра, клика может появиться, но не может исчезнуть). Такие графы будут отделяться от раскрашиваемых в некоторое количество цветов (эта функция, очевидно, "антимонотонна" — т.е., монотонно убывает).

Теорема 5.1 (Пудлак)**.** *Пусть в формуле $A(\vec{x},\vec{y}) \supset B(\vec{x},\vec{z})$ все вхождения x_i положительны. (Для эквивалентной отрицанию этой формулы КНФ $F(\vec{x},\vec{y}) \wedge G(\vec{x},\vec{z})$ это просто означает, что в F переменные x_i входят без отрицаний, а в G — с отрицаниями.) Тогда по доказательству в Res (соответственно, CP) можно построить монотонный интерполянт — монотонную булеву (соответственно, арифметическую) схему $C(\vec{x})$ полиномиального размера, удовлетворяющую*

$$A(\vec{x},\vec{y}) \supset C(\vec{x}) \supset B(\vec{x},\vec{z}).$$

Такому свойству удовлетворяет тавтология "Если в графе есть клика размера n, то его нельзя раскрасить в $n-1$ цвет". Ранее уже была представлена запись отрицания этой тавтологии, соответствующей двум гомоморфизмам $K_n \to G \to K_{n-1}$. Пронумеруем вершины графа и клик. Пусть в графе m вершин. Напомним, что переменная p_{ij} обозначает наличие ребра в G между i и j, q_{ki} обозначает переход вершины k первой клики в вершину i графа, а r_{il} говорит, что вершина i была покрашена (переведена во вторую клику) в цвет l. Тогда в CP гомоморфизмы будут выглядеть следующим образом:

$$K_n \to G \Leftrightarrow \begin{cases} \sum_{i=1}^{n} q_{ki} & \geq & 1, \\ \sum_{k=1}^{m} q_{ki} & \leq & 1, \\ \sum_{i=1}^{n} q_{ki} & \leq & 1, \\ q_{ki} + q_{k'j} & \leq & p_{ij} + 1 \quad (\forall k \neq k', i < j). \end{cases}$$

$$G \to K_{n-1} \Leftrightarrow \begin{cases} \sum_{l=1}^{m-1} r_{il} & \geq & 1, \\ p_{ij} + r_{il} + r_{jl} & \leq & 2 \quad (\forall i < j). \end{cases}$$

В роли $\vec{x}$ здесь выступают p_{ij}. Как видно, знаки их вхождений соответствуют условию теоремы. Заключение же теоремы, применённой к этим формулам, противоречит следующему известному результату (который мы не будем доказывать в этом курсе). (Этим и обусловлен выбор формул.)

Теорема 5.2 (Разборов; Алон-Бопанна; Пудлак)**.** *Для булевых (как и арифметических) схем, разделяющих n -клики и $(n-1)$ -раскрашиваемые графы с m вершинами,*

$$|C| = 2^{\Omega(\sqrt{n})},$$

где $n = \lfloor \frac{1}{8}(m/\log m)^{2/3} \rfloor$.

Основные шаги доказательства теоремы Пудлака для CP. В рамках доказательства мы ограничимся формулами в конъюнктивной нормальной форме (КНФ).

Прежде всего запишем формулы F и G в CP.

- Формуле F будут соответствовать формулы вида $\sum_j \pm y_j + \sum_i x_i \geq c$.
- Формуле G будут соответствовать формулы вида $\sum_k \pm z_k - \sum_i x_i \geq c'$.

В доказательстве могут быть формулы вида

$$\sum_k \pm z_k + \sum_j \pm y_j + \sum_i \pm x_i \geq c''.$$

Для удобства записи мы пока опустили коэффициенты при x_i, y_j, z_k (имея в виду, что некоторые из переменных повторяются, а некоторые — не встречаются). Конечный результат — это неравенство вида $0 \geq 1$.

Подставим конкретные значения x_i в наше доказательство (обозначим через a_i) и сопоставим каждому неравенству два: одно — только с y_j, другое — только с z_k. Для удобства обозначим исходное неравенство черным, а неравенства из пар — красным и зеленым соответственно.

$$\sum_k \pm z_k + \sum_j \pm y_j + \sum_i \pm x_i \geq c'' \rightarrow \begin{array}{rcl} \sum_j \pm y_j & \geq & d_y \\ \sum_k \pm z_k & \geq & d_z \end{array}$$

Мы хотим, чтобы система из двух полученных неравенств была не менее сильной, чем изначальное неравенство. Иначе говоря, если на некотором наборе значений переменных изначальное неравенство оказалось неверным, то хотя бы одно из сопоставляемых неравенств окажется также неверным на этом наборе. Для этого достаточно соблюдать условия

$$d_y + d_z \geq c'' - \sum_i \pm x_i.$$

Сопоставление будем делать по индукции по длине вывода неравенства. Каждой формуле из F сопоставим

$$\left[\begin{array}{rcl} \sum_j \pm y_j & \geq & c - \sum_i a_i \\ 0 & \geq & 0 \end{array} \right],$$

а формуле из G

$$\left[\begin{array}{rcl} 0 & \geq & 0 \\ \sum_k \pm z_k & \geq & c - \sum_i a_i \end{array} \right],$$

В общем виде такие пары будут выглядеть так

$$\left[\begin{array}{rcl} \sum_j \pm y_j & \geq & c - \sum_i a_i \\ \sum_k \pm z_k & \geq & c' - \sum_i a_i \end{array}\right].$$

Необходимо разобрать четыре вида правил: сложение, умножение и деление на константу с округлением — и доказать, что на каждом шаге неравенству сопоставляется не менее сильная пара.

1) Сложение. Суммы x_i, y_j, z_k обозначим соответствующими буквами X, Y, Z. Пусть

$$\frac{X_1 + Y_1 + Z_1 \geq C_1 \left[\begin{array}{rcl} Y_1 & \geq & C_1' \\ Z_1 & \geq & C_1'' \end{array}\right], \; X_2 + Y_2 + Z_2 \geq C_2 \left[\begin{array}{rcl} Y_2 & \geq & C_2' \\ Z_2 & \geq & C_2'' \end{array}\right]}{(X_1 + X_2) + (Y_1 + Y_2) + (Z_1 + Z_2) \geq C_1 + C_2 \left[\begin{array}{rcl} Y_1 + Y_2 & \geq & C_1' + C_2' \\ Z_1 + Z_2 & \geq & C_1'' + C_2'' \end{array}\right]}$$

Нам необходимо показать, что

$$(C_1' + C_2') + (C_1'' + C_2'') \geq (C_1 + C_2) - (X_1 + X_2).$$

При этом относительно верхних неравенств известно

$$\begin{array}{rcl} C_1' + C_1'' & \geq & C_1 - X_1, \\ C_2' + C_2'' & \geq & C_2 - X_2. \end{array}$$

Сложим их и получим необходимое утверждение.

2) Умножение на константу делается аналогично:

$$\frac{X + Y + Z \geq C \left[\begin{array}{rcl} Y & \geq & C' \\ Z & \geq & C'' \end{array}\right]}{dX + dY + dZ \geq dC \left[\begin{array}{rcl} dY & \geq & dC' \\ dZ & \geq & dC'' \end{array}\right]}$$

Повторяя рассуждение, получаем

$$C' + C'' \geq C - X \Rightarrow dC' + dC'' \geq dC - dX.$$

3) Деление на константу с округлением. Пусть

$$\frac{dX + dY + dZ \geq C \left[\begin{array}{rcl} dY & \geq & C' \\ dZ & \geq & C'' \end{array}\right]}{X + Y + Z \geq \left\lceil \frac{C}{d} \right\rceil \left[\begin{array}{rcl} Y & \geq & \left\lceil \frac{C'}{d} \right\rceil \\ Z & \geq & \left\lceil \frac{C''}{d} \right\rceil \end{array}\right]}$$

Известно, что

$$C' + C'' \geq C - dX,$$

из чего следует

$$\left\lceil \frac{C'}{d} \right\rceil + \left\lceil \frac{C''}{d} \right\rceil \geq \left\lceil \frac{C}{d} \right\rceil - X.$$

В конце доказательства мы получим

$$0 \geq 1 \to \left[\begin{array}{lll} 0 & \geq & C', \\ 0 & \geq & C''. \end{array} \right]$$

Об этих константах известно

$$C' + C'' \geq 1.$$

Значит, хотя бы в одной из пар мы получим противоречие, и мы можем узнать в какой из первоначальных формул было противоречие.

Построим по полученной конструкции монотонную схему. Пойдем с конца. Если $C'' > 0$, то возвращаем 1, иначе 0. Проверка > 0 является, очевидно, монотонной. В случаях сложения, умножения и деления на константу с округлением (производимыми над правыми частями неравенств), очевидно, тоже используются монотонные гейты.

Теперь заметим, что достаточно проводить все операции только в одной части неравенств. Т.е. в нашем случае в зеленых. Монотонным будет и добавление значений x_i.

Примечание. Помимо неравенств из F и G в доказательстве встречаются и аксиомы

$$0 \leq x_i \leq 1.$$

Соответственно, отнесем

$$x_i \geq 0$$

к формулам из F, а

$$-x_i \geq -1$$

к формулам из G. □

Доказательство для Res аналогично (вернее, ещё проще).

5.2 Ширина дизъюнкций: нижняя оценка для Res

В предыдущем разделе в качестве побочного результата мы получили нижние оценки на длины доказательств Res. Цель этого раздела: альтернативный метод доказать такие оценки (для других формул).

Посмотрим на доказательство π в любой системе, в которой вывод строится переходами от утверждений к их логическим следствиям. Каждая его строчка имеет какую-то ширину: некоторый параметр, отражающий ее размер. Если строчка доказательства — это полином, то ширина — это степень полинома; если строчка доказательства — это дизъюнкция, то ширина — это число переменных в ней. Шириной доказательства π назовем ширину самой длиной строчки и обозначим ее за $W(\pi)$.

Доказательство экспоненциальной нижней оценки проходит в два этапа. Сперва мы доказываем нижнюю оценку на ширину доказательства (в нашем случае она

будет линейна), а затем из линейной оценки мы получаем экспоненциальный размер доказательства. Для этого мы докажем небольшую лемму о том, что если у нас есть короткие доказательства, то есть и узкие: маленькой ширины.

Введем несколько обозначений касательно метода резолюций:

- строка доказательства — это дизъюнкция $l_1 \vee l_2 \vee \cdots \vee l_k$;
- длина доказательства S — число дизъюнкций в нем;
- ширина строки $W(l_1 \vee l_2 \vee \cdots \vee l_k) = k$, где k — число переменных;
- ширина множества дизъюнкций $W(S) = \max_{s \in S} W(s)$;
- ширина вывода из одного множества дизъюнкции другого — это ширина самой длинной дизъюнкции в выводе;
- будем писать $G \vdash_W H$, если из множества дизъюнкций G можно вывести множество дизъюнкций H, используя дизъюнкции ширины не больше W (разумеется, ширина G и H не превосходит W);
- $W_\vdash(F)$ — минимально возможная ширина доказательства формулы F;
- $S_\vdash(F)$ — минимально возможная длина доказательства формулы F.

5.2.1 Связь длины доказательств с их шириной

Докажем лемму о переходе от нижней оценки на ширину к нижней оценке на длину. А именно, что по доказательству π можно получить π' шириной $\ln(S(\pi))$.

Лемма 5.1. *Пусть есть доказательство π формулы F от n переменных, тогда*

$$W_\vdash(F) \quad \leq \quad W(F) + O(\sqrt{n \ln S_\vdash(F)})$$

Из этой формулы видно, что если ширина вывода $W_\vdash(F)$ обязана быть линейна, а ширина исходной формулы $W(F)$ невелика, то из-за логарифма длина доказательства должна быть как минимум экспоненциального размера. Что и дает нам нижнюю оценку.

Сперва научимся из узких выводов формул $F|_{x=0}$ и $F|_{x=1}$ строить узкий вывод самой формулы F.

Лемма 5.2. *1.* $F|_{x=0} \vdash_W C \Rightarrow F \vdash_{W+1} C \vee x$.

2. $W_\vdash(F|_{x=0}) \leq w - 1, W_\vdash(F_{x=1}) \leq w \Rightarrow W_\vdash(F) \leq \max\{w, W(\{C \in F | \neg x \in C\})\}$

Доказательство. 1. Итак, есть вывод $F|_{x=0} \vdash_W C$. Перестанем подставлять вместо x значение 0.

Если x не входила в дизъюнкцию, то после отмены подстановки она не изменилась. Дизъюнкции, в которые x входила отрицательно (и делала дизъюнкцию тождественно истинной), в выводе не участвовали. Дизъюнкции, в которые x входила положительно, в выводе участвовали. Однако дописывание x к каждой дизъюнкции

вывода не делает его неверным. Пусть в выводе присутствовали дизъюнкции $D \vee y$ и $E \vee \neg y$, а также вывод

$$\frac{D \vee y \; E \vee \neg y}{D \vee Y}.$$

Допишем ко всем дизъюнкциям x

$$\frac{x \vee D \vee y \; x \vee E \vee \neg y}{x \vee D \vee Y}.$$

Вывод останется корректным. Таким образом, если раньше мы выводили C, то теперь мы выведем $C \vee x$; при этом ширина каждой дизъюнкции вывода увеличится не более, чем на единицу.

2. У нас есть вывод $F|_{x=0}$ ширины $W_{\vdash}(F|_{x=0}) \leq w - 1$. Т.е. у нас есть вывод, начинающийся с дизъюнкций $F|_{x=0}$ и заканчивающийся пустой дизъюнкцией, противоречием. По первому пункту мы можем получить вывод $F \vdash_W x$. Резольвируя дизъюнкции формулы F с полученным x, получим дизъюнкции формулы $F|_{x=1}$, а из них уже выведем противоречие (по предположению теоремы). Кроме дизъюнкций, использованных в выводах $F|_{x=0}$ и $F|_{x=1}$, мы использовали некоторые из F (те, что содержали x с отрицанием). Но их ширину оценивает второй член в max из формулировки теоремы. □

Справедлива и симметричная формулировка, которая доказывается абсолютно также с точностью до отрицаний и замен констант.

Лемма 5.3. *1.* $F|_{x=1} \vdash_W C \Rightarrow F \vdash_{W+1} C \vee \neg x$.

2. $W_{\vdash}(F|_{x=1}) \leq w - 1, W_{\vdash}(F_{x=0}) \leq w \Rightarrow W_{\vdash}(F) \leq \max\{w, W(\{C \in F | x \in C\})\}$

Вернемся теперь к основной лемме. Пусть мы имеем короткое, но толстое доказательство. Будем сужать его, убивая толстые дизъюнкции. Т.к. доказательство короткое, толстых дизъюнкций мало. Будем выбирать переменную, которая входит в максимальное число толстых дизъюнкций. Если ей присвоить значения, то при одном эти дизъюнкции исчезнут, а при другом их ширина сократится на единицу. Повторив такую операцию несколько раз, мы получим узкое доказательство; по доказанной только что лемме из таких доказательств можно вновь "собрать" доказательство исходной формулы.

Пусть $d = \sqrt{2n \ln S_{\vdash}(F)}$ и $\alpha = (1 - \frac{d}{2n})$. Мы будем считать дизъюнкцию толстой, если ее ширина не меньше d.

Дадим небольшое пояснение α. Пусть имеется t толстых дизъюнкций, литералов в них не менее td. Всего переменных n, при этом они могут входить с разными знаками, т.е. литералов $2n$. Значит, некоторый литерал встретится не менее чем в $\frac{td}{2n}$ толстых дизъюнкциях. Или же в части $1 - \alpha$ толстых дизъюнкций. Значит, если означить литерал истиной, то $1 - \alpha$ дизъюнкций уйдет, а α останется. Повторив эту операцию небольшое (логарифмическое) число раз, мы избавимся от всех толстых дизъюнкций.

Докажем более формально. Пусть Π — наше короткое и толстое доказательство. Обозначим $\Pi_d = \{C \in \Pi \mid |C| \geq d\}$. Покажем, что если $|\Pi_d| < \alpha^{-k}$, где k — некоторая константа, то $W_{\vdash}(F) \leq d + k + W(F)$.

Будем доказывать индукцией по k и числу переменных n. Выберем такой литерал l, который встречается в хотя бы $1-\alpha$ толстых дизъюнциях, и означим его единичкой. Получим некоторое доказательство Π'. При этом $|\Pi'_d| < \alpha^{-(k-1)}$. По предположению индукции по k имеем: $W_{\vdash}(F|_{l=1}) \leq d+k+W(F)-1$. С другой стороны, если мы подставим 0 в литерал l, то получим $W_{\vdash}(F|_{l=0}) \leq d+k+W(F)$ по предположению индукции относительно числа переменных n (в F теперь на одну переменную меньше). Таким образом, использую маленькую лемму, мы можем реконструировать доказательство F шириной не более $d+k+W(F)$ (максимумы мажорируются $W(F)$).

База индукции очевидна. При $k=0$ в формуле нет толстых дизъюнкций. Если $n=0$, то в формуле просто нет переменных.

Связь между длинами доказательств и минимальной шириной доказана. Осталась получить линейную нижнюю оценку на $W_{\vdash}(F)$.

5.2.2 Цейтинские формулы

Рассмотрим граф $G = \langle V, E\rangle$ с нечетным числом вершин. Пусть мы покрасили его ребра в два цвета 0 и 1. Цейтинские формулы кодируют тавтологию, означающую, что нельзя покрасить граф так, чтобы для каждой вершины сумма цветов по всем инцидентным ей ребрам была бы нечетна:

$$\exists k \in \mathbb{Z}\,(|V| = 2k+1 \wedge \forall v \in V \bigoplus_{v \in e \in E} x_e = 1).$$

Быть такого не может. Если все уравнения сложить, то получим нечетное число. С другой стороны, каждое ребро должно входить в эту сумму ровно два раза. Значит, результат сложения должен быть четным. Получаем противоречие.

Слегка обобщим эту тавтологию. Создадим для каждой вершины метку $c_v \in \{0,1\}$ и потребуем

$$\begin{array}{rcl} \bigoplus_{v\in V} c_v & = & 1, \\ \forall v \in V \bigoplus_{v\in e\in E} x_e & = & c_v. \end{array}$$

В изначальной постановке все c_v были равны единице.

Замечание 5.1. Заметим, что если $\bigoplus_{v\in V} c_v = 0$ и G связен, то выполняющий набор существует. Действительно, тогда можно разбить на пары все вершины с $c_v = 1$. Начнём с нулевой раскраски и будем исправлять её. Поочерёдно для каждой из построенных пар возьмём какой-нибудь путь между ними и прибавим к каждому ребру этого пути единичку по модулю два. Очевидно, что четность промежуточных вершин такая операция не поменяет. Зато у начальной и конечной вершины она изменится.

Имеется проблема: формула, которую мы записали содержит сложение по модулю два, да еще и в больших количествах. А Res — система доказательств для формул в КНФ. Если непосредственно записать большой xor (сложение по модулю два) в КНФ, то конъюнкций будет экспоненциально много. Этой проблемы нет, если степень вершин нашего графа невелика. Например, для степени три xor трёх переменных записывается по таблице истинности четырьмя дизъюнкциями.

Мы также потребуем от графа дополнительные условия, которые позволят нам доказать нижнюю оценку на ширину вывода.

Определение 5.3. Пусть *расширительная способность* графа G

$$e(G) = \min_{V' \subset V} \{|\mathrm{cut}(V', V \setminus V')| \, | V' \subset V, \frac{1}{3}|V| \le |V'| \le \frac{2}{3}|V|\},$$

где $\mathrm{cut}(A, B)$ — множество ребер, соединяющих вершины множества A с вершинами множества B. Граф является *расширителем*, если $e(G) = \Omega(|V|)$.

Факт 5.1. *Существуют связные регулярные расширители степени 3.*

Пусть у нас есть цейтинская формула

$$\bigwedge_{v \in V} (\bigoplus_{v \in e \in V} x_e = c_v),$$

построенная по регулярному расширителю степени 3. Формула будет противоречивой. Докажем, что ее резолюционное доказательство будет широким.

У нас есть набор xor-ов X, из которых мы выводим противоречие. Заметим, что если хотя бы один из этих xor-ов опустить, то, как обсуждалось выше, мы получим выполнимую формулу.

Определение 5.4. Дизъюнкция C поточечно следует из U, если C истинна, как минимум, при тех значениях переменных, при которых каждый xor из U истинен. C в точности следует из U, если C поточечно следует из U и не следует из любого его собственного подмножества.

Зададимся вопросом, что можно вывести из подмножества X. Утверждается, что в выводе будет дизъюнкция C которая следует из множества $U \subset X$ и только из него, где $\frac{1}{3}|X| \le |U| \le \frac{2}{3}|X|$.

Найдём такую . Пусть в выводе очередная дизъюнкция $D \vee E$ получена резолюцией дизъюнкций $D \vee x$, следующей из s xor-ов, и $E \vee \neg x$ — из t xor-ов. Тогда $D \vee E$ следует не более чем из $s + t$ xor-ов. Теперь отметим следующее: каждый начальный xor в точности следует сам из себя; последняя дизъюнкция (противоречие) — в точности из всех. Ввиду указанных ограничений "перепрыгнуть" в процессе вывода интервал от $\frac{1}{3}|X|$ до $\frac{2}{3}|X|$ мы не сможем. Значит, дизъюнкция C, следующая примерно из половины xor-ов, действительно имеется в выводе.

Покажем теперь, что эта дизъюнкция является достаточно широкой. Каждый xor соответствует сумме по ребрам вокруг некоторой вершины $v \in V$. Сопоставим множеству xor-ов U множество соответствующих ему вершин V_U. Итак, C следует в точности из

$$\bigwedge_{v \in V_U} (\bigoplus_{u \in e \in E} x_e = c_v).$$

Мы знаем, что $\frac{1}{3}|V| \le |V_U| \le \frac{2}{3}|V|$. И, вспоминая свойства расширителя, знаем, что между V_U и $V \setminus V_U$ найдется $\Omega(|V|)$ ребер. Относительно формул это значит, что найдется порядка $\Omega(|V|)$ переменных x_e которые входят по одному разу в U и в $X \setminus U$. Покажем, что все такие переменные войдут в дизъюнкцию C.

Рассмотрим x_e. Пусть у нас имеется конъюнкция вида $\psi = (a \oplus b \oplus x_e) \wedge \phi$, где ϕ — конъюнкция оставшихся xor-ов из U, из ψ в точности следует C. Предположим, что x_e не входит в C. Если выкинуть первый xor, должен появиться набор, на котором ϕ

истинна, а C ложна (т.к. C не следует из ϕ). Т.к. C следует из ψ, то $(a \oplus b \oplus x_e)$ должна оказаться ложной. Поменяем значение x_e на противоположное. Т.к. в C переменная x_e не входит, то истинность ее не изменится. Зато как $(a \oplus b \oplus x_e)$, так и вся формула ψ окажутся истинными. Противоречие.

Таким образом, ширина $W(C) = \Omega(|V|)$, а значит и ширина любого доказательства формулы будет $\Omega(|V|)$.

По результатам предыдущего раздела отсюда следует экспоненциальная нижняя оценки на длину кратчайшего доказательства.