1 Определения

Пусть $f : X \times Y \to Z$ – функция. Есть два игрока, Алиса и Боб, Алисе известен x, Бобу – y, они хотят посчитать $f(x, y)$, переслав друг другу как можно меньшее число бит.

Definition 1. *Коммуникационный протокол – это бинарное дерево, каждая вершина которого помечена функцией $a_v : X \to \{0, 1\}$ или функцией $b_v : Y \to \{0, 1\}$. Значение протокола на входе (x, y) определяется значением, записанным в листе дерева, после прохождения по пути от корня дерева. Из текущей вершины путь идёт налево, если $a_v(x) = 0$ ($b_v(y) = 0$), и направо, если $a_v(x) = 1$ ($b_v(y) = 1$).*

Definition 2. *Коммуникационная сложность функции f ($cc(f)$) – это минимальная глубина коммуникационного протокола.*

Обобщением tree-like коммуникационных протоколов являются dag-like коммуникационные протоколы.

Definition 3. *Пусть $Q \subseteq X \times Y \times O$ – отношение. Тогда dag-like протокол (dag прямоугольников) для этого отношения – это dag, обладающий следующими свойствами:*

- *У каждой вершины, кроме стоков, ровно 2 потомка.*
- *Существует ровно один исток.*
- *Каждой вершине v приписан комбинаторный прямоугольник $R_v \in X \times Y$; истоку приписан прямоугольник $X \times Y$.*
- *Пусть u, w – потомки v, тогда $R_v \subseteq R_u \cup R_w$.*
- *Каждому стоку t приписан элемент $o \in O$ т.ч. $\forall (x, y) \in R_t$ $(x, y, o) \in Q$.*

Можно заменить в определении прямоугольники на множества коммуникационной сложности не более t, и рассматривать dag множеств небольшой коммуникационной сложности.

Lemma 1 ([3]). *Если для отношения Q существует dag множеств коммуникационной сложности не более t размера S, то для отношения Q существует dag прямоугольников размера не более $S \cdot 2^{3t}$.*

Dag-like коммуникационные протоколы могут использоваться для переноса нижних оценок с резолюций на другие системы доказательств, а также на монотонные схемы.

Definition 4. *Пусть φ – невыполнимая формула в КНФ, X, Y – некоторое разделение её переменных. Тогда определим задачу поиска $Search_\varphi$ следующим образом: $(x, y, C) \in Search_\varphi \Leftrightarrow$ дизъюнкт C опровергается подстановкой (x, y), где x – подстановка в переменные X, y – подстановка в переменные Y.*

Lemma 2 (?). *Пусть S – резолюционное доказательство невыполнимой формулы φ. Тогда существует dag-like протокол для $Search_\varphi$ размера $|S|$.*

Доказательство. Инвертируем все рёбра в графе резолюционного доказательства. Вершины графа помечены клозами доказательства. Пусть вершине v соответствует клоз C, тогда соотнесём с ней множество входов (x, y), т.ч. (x, y) не выполняет C. Легко понять, что это множество является комбинаторным прямоугольником. Истоком является вершина с пустым дизъюнктом; его не выполняют все возможные подстановки. В стоках dag-а написаны дизъюнкты исходной формулы, являющиеся ответами на задачу. Осталось проверить, что прямоугольники в потомках вершины покрывают прямоугольник в ней самой. Пусть v – вершина, u, w – её потомки. Тогда дизъюнкт C_v получен из C_u и C_w по правилу резолюции; а значит, любой вход, который не выполняет C_v, обязан не выполнить либо C_u, либо C_w.

Theorem 1 ([1]). *$m = n^{O(1)}$, $w(\varphi)$ – минимальная ширина резолюционного доказательства формулы φ от n переменных, $Ind_m : [m] \times \{0,1\}^m$ – функция индексирования.*
Тогда размер любой монотонной схемы для $CSP - SAT_{\varphi \circ Ind_m}$ не менее $n^{w(\varphi)}$

Вопрос, можно ли получить аналог этой теоремы для гаджета константного размера, остаётся открытым.
Для некоторых константных гаджетов существуют нижние оценки на коммуникационную сложность функций после их подстановки.

Рассмотрим функцию $VER : \mathbf{Z}_4 \times \mathbf{Z}_4 \to \{0,1\}$. $VER(x, y) = 1 \Leftrightarrow x + y \in \{2, 3\}$

Далее пусть S – некоторая задача поиска $S \subseteq \{0,1\}^n \times Q$ (предполагается, что ответ на задачу существует для любого $\alpha \in \{0,1\}^n$).

Definition 5. *$f \subseteq S$ – функция, реализующая S, если $\forall \alpha \in \{0,1\}^n$ $(\alpha, f(\alpha)) \in S$).*

Definition 6. *$\alpha \in \{0,1\}$ – критический вход, если $\exists!$ $\beta : (\alpha, \beta) \in S$.*

Definition 7. *Пусть $f \subseteq S$ – некоторая функция, реализующая S. Назовём $bs(f, \alpha)$ максимальное число непересекающихся блоков координат $B_1, \ldots, B_{bs} \subseteq [n]$ т.ч. $f(\alpha) \neq f(\alpha^{B_i})$ $\forall i$, где α^{B_i} означает, что у входа α все координаты x из множества B_i заменили на $1 - x$. Тогда определим критическую блочную чувствительность отношения S следующим образом:*

$$cbs(S) = min_{f \subseteq S} max_\alpha bs(f, \alpha),$$

где α из множества критических входов.

Theorem 2 ([2]). *Для любой задачи поиска $S \subseteq \{0,1\}^n \times Q$ вероятностная коммуникационная сложность $S \circ VER^n$ не менее $\Omega(cbs(S))$*

2 Основная часть

Lemma 3. *Пусть D – дизъюнкт, P – множество его положительных литералов, N – множество отрицательных литералов. Тогда $cc(D \circ AND) \leq |P| + 3$.*

Доказательство. Покажем, как определить значение дизъюнкта, переслав $|P| + 3$ бита. $D = N \vee P$, поэтому $D \circ AND = \neg C \vee DISJ_P$, где C – это клоз, состоящий из всех переменных $N \circ AND$, взятых как положительные литералы, а $DISJ_P$ – задача, полученная после подстановки в переменные P гаджета AND. Узнать значение $\neg C$ можно за 2 бита коммуникации, значение же $DISJ_P$ можно узнать за $|P| + 1$ бит коммуникации.

Theorem 3. *Существует семейство формул φ_n в КНФ с минимальной шириной резолюционного доказательства $\Omega(\sqrt{n})$, т.ч. размер dag-like протокола для отношения $Search_{\varphi_n \circ AND}$ равен $poly(n)$.*

Доказательство. Нам достаточно указать семейство формул с большой шириной и небольшим размером резолюционного доказательства, при условии, что в каждом дизъюнкте этого резолюционного доказательства немного (константное количество) положительных литералов. После этого можно воспользоваться леммой 3. Тогда у каждого дизъюнкта резолюционного доказательства маленькая коммуникационная сложность, и из dag-а доказательства инвертированием рёбер можно получить dag множеств маленькой коммуникационной сложности, значит, существует и dag прямоугольников, чей размер также полиномиален.
Искомой формулой будет $ORDERING$:

- $x_{i,j} \vee x_{j,i}$
- $\neg x_{i,j} \vee \neg x_{j,i}$
- $\neg x_{i,j} \vee \neg x_{j,k} \vee x_{i,k}$
- $\bigvee_j x_{j,i} = D_i \quad \forall i$

$x_{i,j} = 1 \Leftrightarrow i < j$

Также можно рассматривать $ORDERING$ на графе, где вместо дизъюнктов четвёртого типа используются следующие дизъюнкты:

- $\bigvee_{j:(i,j) \in E(G)} x_{j,i} \quad \forall i$

Для $ORDERING$ (в т.ч. на графе, если G – экспандер) известна оценка на ширину $\Omega(\sqrt{n})$.
Укажем короткое резолюционное доказательство, где в каждом дизъюнкте константное число отрицательных литералов. Заметим, что после этого можно заменить в формуле $x_{i,j}$ на $\neg x_{i,j}$ и наоборот, и оценка на ширину сохранится. Резолюционное доказательство при этом превратится в доказательство с малым количеством положительных литералов.

Резолюционное доказательство будет состоять из n шагов, на каждом шаге полиномиальное число действий. Неформально, мы будем по очереди удалять из D_i переменные $x_{j,i}$, начиная с бóльших j, пока не получим пустой дизъюнкт. Это соответствует перебору возможного минимума от n-го элемента до 1-го.
Опишем j-й шаг. В конце j-го шага получим набор дизъюнктов $D_{i,j}$, полученных из D_i удалением всех $x_{k,i}$, $k > n - j$ (и, возможно, добавлением некоторых $x_{k,i}$, $k \leq n - j$). $D_{i,0} = D_i$, покажем, как из $D_{i,j-1}$ получить $D_{i,j}$.

- Пусть в $D_{i,j-1}$ нет переменной $x_{n-j+1,i}$ – тогда $D_{i,j} = D_{i,j-1}$.
- Иначе резольвируем $D_{i,j-1}$ с $\neg x_{n-j+1,i} \vee \neg x_{i,n-j+1}$
- Пусть $x_{k,n-j+1} \in D_{n-j+1,j}$. Резольвируем $D_{n-j+1,j}$ с $\neg x_{i,k} \vee \neg x_{k,n-j+1} \vee x_{i,n-j+1}$, а затем с $x_{i,k} \vee x_{k,i}$. Повторяем для всех таких k.
- Резольвируем результаты двух предыдущих действий.

После n-го шага получаем пустой дизъюнкт.
Можно видеть, что в каждом дизъюнкте данного доказательства не более 2 отрицательных литералов.

Remark 1. Можно обойтись без замены $x_{i,j}$ на $\neg x_{i,j}$, используя первые два типа дизъюнктов формулы. С помощью резолюции с $x_{i,j} \vee x_{j,i}$ можно заменить все отрицательные литералы $\neg x_{i,j}$ на положительные $x_{j,i}$. Далее будем моделировать исходное доказательство. Пусть в исходном доказательстве происходит резолюция $C_1 \vee x_{i,j}$ и $C_2 \vee \neg x_{i,j}$. Тогда в новом доказательстве есть клозы $\tilde{C_1} \vee x_{i,j}$ и $\tilde{C_2} \vee x_{j,i}$ из соответствующих положительных литералов. Резольвируем $\tilde{C_2} \vee x_{j,i}$ с $\neg x_{i,j} \vee \neg x_{j,i}$, а потом с $\tilde{C_1} \vee x_{i,j}$. Т.к., дизъюнкты, кодирующие, что $x_{i,j} = \neg x_{j,i}$ $\forall i, j$, позволяют добавлять отрицания в формулу по необходимости, можно получить резолюционное доказательство с малым количеством отрицаний в каждом дизъюнкте, а можно – с почти всеми отрицаниями. Таким образом, данный пример даёт полиномиальный размер dag-like протокола не только при подстановке AND, но и при подстановке OR в качестве гаджета.

Список литературы

[1] Ankit Garg и др. “Monotone circuit lower bounds from resolution”. в: *Proceedings of the annual ACM Symposium on Theory of Computing* (июнь 2018).

[2] Mika Göös и Toniann Pitassi. “Communication Lower Bounds via Critical Block Sensitivity”. в: *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*. STOC ’14. New York, New York: ACM, 2014, с. 847—856.

[3] Dmitry Sokolov. “Dag-like communication and its applications”. в: *Computer Science - Theory and Applications - 12th International Computer Science Symposium in Russia, CSR 2017, Kazan, Russia, June 8-12* (2017), с. 294—307.