Рецензия на доклад

Удивительная сила алгебраических доказательств константной глубины

Примечание: summary сделан на основе доклада, поскольку значительная часть статьи рассказана не была

1 Определения

Определение. Пусть есть множество многочленов $\{P_1, \ldots, P_m\}$ над переменными $\{x_1, \ldots, x_n\}$. Опровержение PC (Polynomial Calculus) на них есть последовательность многочленов $R_1, \ldots, R_s$, где $R_s = 1$ и каждый многочлен R_j получается из предыдущих одним из следующих способов:

- $R_j = P_i$
- $R_j = \alpha R_k + \beta R_l (k, l < j)$
- $R_j = x_i R_k (k < j)$

Определение. Пусть есть поле $\mathbb{F}$ и переменные $\{x_1, \ldots, x_n\}$. SLP (Straight Line Program) на них есть последовательность многочленов $y_1, \ldots, y_m$, где каждый многочлен y_j получается из предыдущих одним из следующих способов:

- $y_j = x_i$
- $y_j = \sum a_l y_l, l < j$

- $y_j = \prod y_l, l < j$

Можно рассмотреть SLP как ациклический граф, проведя стрелки от многочлена в зависящие от него. Его глубина и есть глубина SLP.

Некоторые расширения позволяют заводить новые переменные, равные многочленам от старых:

- $\sum\prod\sum$-*PC* – многочленам первой степени (*Trinomial*-$\prod\sum$-*PC* добавляет условие на то, что каждый из многочленов как на входе, так и на выходе PC состоит не более, чем из трёх мономов);
- *Depth-d-PC* – многочленам из SLP глубины не более $d-2$.

Определение. Пусть есть множество переменных $\{x_1, \ldots, x_n\}$ и набор неравенств на них вида $a_1x_1 + \ldots + a_nx_n \geq c$ (a_i и c при этом целые). Опровержение *CP* на них есть последовательность неравенств, каждое из которых есть либо сумма предыдущих, либо предыдущее умножить на константу, либо предыдущее делить на константу (если все a_i делятся; в таком случае результат деления c округляется вверх), а последнее неверно.

*CP** – CP с полиномиальным ограничением на возможные значения x_i.

2 Содержательная часть

Теорема. Trinomial-$\prod\sum$-PC над $\mathbb{Q}$ может симулировать CP* с полиномиальным увеличением длины доказательства.

Лемма 1. *(Substitution Lemma)* Пусть $R(z-a_1)\ldots(z-a_k) = 0$ и $Rp(z) = 0$ – два выражения в опровержении *Depth-d′-PC*, $deg\, p = d$, $p(a_i) \neq 0\,\forall i$. Тогда можно вывести $R = 0$ за $O(kd\,|R|)$ шагов.

Доказательство. Собираем $R(z-a_1)\ldots(z-a_{k-1})(z^i - a_k^i)$ для всех i от 1 до d (умножая на многочлен), собираем из них $R(z-a_1)\ldots(z-a_{k-1})(p(z)-p(a_k))$, вычитаем $R(z-a_1)\ldots(z-a_{k-1})p(z)$ и делим на $-p(a_k) = const$. Продолжаем.

Лемма 2. Пусть $Q(z-a) = 0$ и $Q(z-b_1)\ldots(z-b_k) = 0$ – два выражения в опровержении *Trinomial*-$\prod\sum$-*PC*, $a \neq b_i\,\forall i$. Тогда можно вывести $Q = 0$ за $O(k)$ шагов.

Доказательство. Заводим $z_1 = z - a$, $z_2 = z - b_1$, $Q_1 = (z - b_2) \dots (z - b_k)$, $c = a - b_1 \neq 0$ (тогда $z_1 - z_2 + c = 0$) – тогда есть $Qz_1 = 0$, $QQ_1z_2 = 0$. Умножаем первое на Q_1, умножаем $z_1 - z_2 + c = 0$ на QQ_1 и вычитаем из него оба исходных равенства – имеем $QQ_1c = 0$. Делим на c, продолжаем.

Лемма 3. Пусть A и B – два множества из $\mathbb{F}$. Пусть $\prod\limits_{a \in A} (z - a) = 0$ и $\prod\limits_{b \in B} (z - b) = 0$ – два выражения в опровержении *Trinomial*-$\prod\sum$-*PC*. Тогда можно вывести $\prod\limits_{c \in A \cap B} (z - c) = 0$ за $O(|A \backslash B| \cdot |B \backslash A|)$ шагов.

Доказательство. Выкидываем элементы из A, которые не входят в B. Это делается леммой 2, если домножить второе выражение на оставшиеся $(z - a)$ с $a \in A, a \notin B$.

Теперь о том, как симулировать. Добавляем для каждой переменной x многочлен – произведение $(x - c)$ со всеми возможными значениями c, которые можно туда ставить. С неравенством – то же самое, но все возможные значения неравенства.

Умножение делается в лоб умножением, деление – делением (с последующим выкидыванием некорректных скобок по Intersection Lemma).

Сумма делается немного сложнее:

Лемма 4. Пусть $x(x - 1) \dots (x - a) = 0$ и $y(y - 1) \dots (y - b) = 0$ – два выражения в опровержении *Trinomial*-$\prod\sum$-*PC*, $a \geq b$. Тогда можно вывести $z(z - 1) \dots (z - a - b) = 0$ за $O(ab)$ шагов.

Доказательство. Обозначим $z_i = x + y - i$, $x_j = x - j$, $y_k = y - k$. Обозначим $Y_i = \prod\limits_{k=0, k \neq i}^{b} y_k$

Умножив $z_i - x_0 - y_i = 0$ на оставшиеся y и убрав произведение y, получим $z_iY_i - x_0Y_i = 0$. Умножив $x_i - x_0 - i = 0$ на оставшиеся y, получаем $x_iY_i - x_0Y_i - iY_i = 0$, аналогично с z. Комбинируя все три, получаем $z_{i+j}Y_j - x_iY_j = 0$. Из этого можно выводить штуки вида $z_{i+j}z_{i+j-1}Y_j - x_iz_{i+j-1}Y_j = 0$ и $z_{i+j}x_{i+1}Y_j - x_ix_{i+1}Y_j = 0$, собирая $z_jz_{j+1} \dots zj + iY_j - x_0x_1 \dots x_iY_j = 0$.

Проделываем это для $i = a$ – тогда второй кусок можно убрать. К остальному добавляем остальные z и применяем Intersection Lemma (точнее, её вариант, где ещё отдельно храним Q).