Тождества глубины 3 с многочленами

Иванова А. В.

Московский физико-технический институт.
Кафедра «Интеллектуальные системы»

Научный руководитель
к.ф.-м.н., с.н.с. ВЦ РАН М. Н. Вялый

13 июня 2013 г.

- **Задача проверки тождества** (*Problem Identity Testing*): Пусть многочлен p задан в некотором виде (схема). Требуется ответить на вопрос: является ли p тождественным нулем или нет.

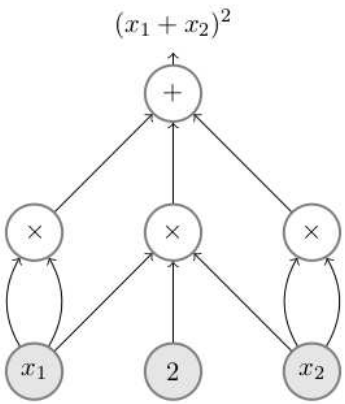
- Связь с PCP-теоремой;
- Связь с задачей дерандомизации (*Agrawal, 2005*);
- Связь с нижними оценками на вычисление детерминанта и перманента.

- Схема — это ориентированный граф, вершины которого разделены на слои;
- В узлах — операции $\times$ и $+$, в листьях — переменные и коэффициенты;
- Схемы глубины 3:

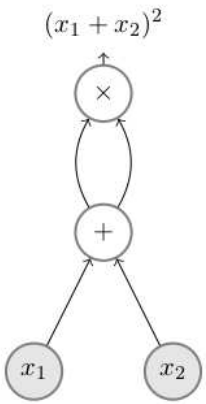
$$C = \sum_{i=1}^{k} T_{ij},$$

где T_{ij} - произведение линейных форм;

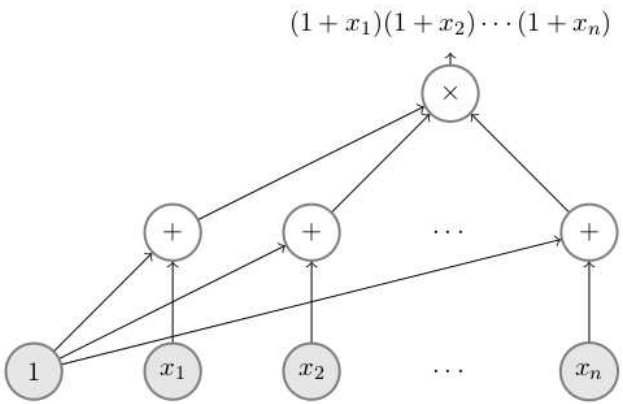
- k - величина верхнего слоя;
- d - формальная степень C.



Example 1



Example 2



Example 3

Рис.: Примеры схем

Сводимость к случаю глубины 3

Для случая многочлена на n переменных над полем $\mathbb{C}$ степени d, вычисляемого схемой размера s, можно построить схему глубины 3 размера $\exp O(\sqrt{d \log d \log n \log s})$

Определения

- [**Простая схема**] Схема $\mathcal{C}$ называется простой, если не существует ненулевой линейной формы, делящей каждый T_i.
- [**Минимальная схема**] Схема $\mathcal{C}$ называется минимальной, если для любого собственного подмножества $S \in [k]$: $\sum_{i \in S} T_i$ не нулевая.
- [**Ранг схемы**] Ранг схемы, $rank(\mathcal{C})$, определяется как ранг семейства линейных форм $l_{i,j}$, рассматриваемых как n–мерные вектора над полем $\mathbb{F}$.

Оценка на ранги тождеств

Пусть $|\mathbb{F}| > d$. Тогда ранг простого, минимального $\Sigma\Pi\Sigma(k, d)$ тождества, в котором наибольшее число независимых слагаемых равно k', не более, чем $\frac{3(k-1)(k-2)}{2} + 9(k - k')k' \log d$.

Случай $\mathbb{F} = \mathbb{F}_2$

- Нижние оценки на ранг $\Omega(k \log d)$

$$\mathcal{C}(x_1, \ldots, x_r) := \prod_{\substack{b_1,\ldots,b_{r-1}\in\mathbb{F}_2 \\ b_1+\cdots+b_{r-1}\equiv 1}} (b_1x_1 + \cdots + b_{r-1}x_{r-1}) +$$
$$+ \prod_{\substack{b_1,\ldots,b_{r-1}\in\mathbb{F}_2 \\ b_1+\cdots+b_{r-1}\equiv 0}} (x_r + b_1x_1 + \cdots + b_{r-1}x_{r-1}) +$$
$$+ \prod_{\substack{b_1,\ldots,b_{r-1}\in\mathbb{F}_2 \\ b_1+\cdots+b_{r-1}\equiv 1}} (x_r + b_1x_1 + \cdots + b_{r-1}x_{r-1})$$

Алгоритм построения тождества

Пусть $D := \sum_{j=1}^{k} T_j$ — простая, минимальная и нулевая $\Sigma\Pi\Sigma$ схема над $\mathbb{F}_2$, определенная на переменных $y_1, \ldots, y_s$. Пусть степень D равна g, верхний слой k, ранг s. $\mathcal{C}$ определена выше, причем $\mathcal{C} = S_1 + S_2 + S_3$. Тогда схема, определяемая

$$D' := \sum_{j=1}^{k-1} T_j \cdot S_1 - T_k \cdot S_2 - T_k \cdot S_3,$$

является минимальной, простой и нулевой со степенью $d' = d + g$, верхним слоем, равным $k' = k + 1$, и рангом $r' = s + r$.

Случай $\mathbb{F} = \mathbb{F}_p$

$$\mathcal{C}(x_1, \ldots, x_r) := \prod_{\substack{b_1,\ldots,b_{r-1}\in\mathbb{F}_p \\ b_1+\cdots+b_{r-1}\equiv 1}} (b_1x_1 + \cdots + b_{r-1}x_{r-1}) +$$
$$+ \prod_{\substack{b_1,\ldots,b_{r-1}\in\mathbb{F}_p \\ b_1+\cdots+b_{r-1}\equiv 0}} (x_r + b_1x_1 + \cdots + b_{r-1}x_{r-1}) +$$
$$+ \prod_{\substack{b_1,\ldots,b_{r-1}\in\mathbb{F}_p \\ b_1+\cdots+b_{r-1}\equiv 1}} (x_r + b_1x_1 + \cdots + b_{r-1}x_{r-1})$$

- Для случая большего k дальнейшее построение аналогично.

Случай поля бесконечной характеристики ($\mathbb{F} = \mathbb{R}$)

$$x_4(x_4 + x_1 + x_2)(x_4 + x_2 + x_3)(x_4 + x_3 + x_1) -$$
$$-(x_4 + x_1)(x_4 + x_2)(x_4 + x_3)(x_4 + x_1 + x_2 + x_3) +$$
$$+x_1x_2x_3(2x_4 + x_1 + x_2 + x_3)$$

- Можно показать, что в этом случае при $k = 3$ оценка оптимальна (ранг равен 4)

- S — конечное подмножество проективного пространства $\mathbb{FP}^n$. Иначе говоря, S — подмножество векторов в $\mathbb{F}^{n+1}$ такое, что ни один вектор в S не является коллинеарным другому. Предположим, что $\forall V \subset S$, состоящего из k линейно независимых векторов, линейная оболочка V содержит как минимум $k+1$ вектор из S. Тогда S называется SG_k-замкнутым.
- Наибольший возможный ранг SG_k-замкнутого множества из не более, чем m векторов $\mathbb{F}^n$ (для любого n) обозначается как $\mathrm{SG}_k(\mathbb{F}, m)$

Оценка на ранги тождеств

Пусть $|\mathbb{F}| > d$. Тогда ранг простого, минимального $\Sigma\Pi\Sigma(k,d)$ тождества, в котором наибольшее число независимых слагаемых равно k', не более, чем $\frac{3(k-1)(k-2)}{2} + (k-k') \cdot SG_{k'}(\mathbb{F}, d)$.

- Узел по модулю идеала I от мультипликативного члена(nod_I) — произведение всех линейных форм в мультипликативном члене, такие что они «похожи» по модулю идеала. Две формы l_1 и l_2 «похожи», если

$$\exists c \in \mathbb{F}^* : \ l_1 \equiv cl_2 \pmod{I}$$

- Пусть I - идеал, порожденный какими-то мультипликативными членами. Пусть v_i - подчлен T_i ($L(v_i) \subset L(T_i)$), $\forall i \in [k]$. Назовем кортеж $(I, v_1, \ldots, v_k)$ путем $\mathcal{C}$ по модулю I, если

$$\forall i \in [k] : \ v_i \ \in \ nod_{\langle I, v_1, \ldots, v_{i-1} \rangle}(T_i).$$

Сертификат для тождества

Пусть I - идеал, порожденный мультипликативными членами. Пусть $\mathcal{C} = \sum_{i \in [k]} T_i$ является $\Sigma\Pi\Sigma(k, d)$ и не является нулевой по модулю I. Тогда $\exists i \in \{0, \ldots, k-1\} : \mathcal{C}_{[i]} \pmod I$ имеет путь p такой, что

$$\mathcal{C}_{[i]'} \equiv \alpha \cdot T_{i+1} \not\equiv 0 (mod\ p).$$

- Для поля $\mathbb{F} = \mathbb{R}$ существует неадаптивный алгоритм, сложность которого зависит от k экспоненциально.

- Даже схемы глубины 3 — достаточно сложная структура;
- оценки на ранги тождеств дают надежду на то, что такие схемы имеют простой вид;
- из случая $\mathbb{F} = \mathbb{R}$ можно сделать вывод, что оценка $O(k^2 \log d)$ на ранг является сильно завышеной хотя бы для случая такого поля.