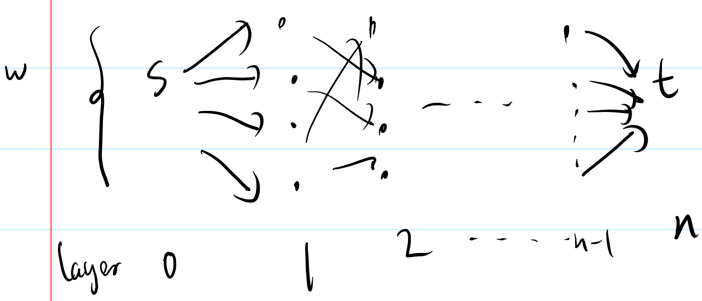
19. Whitebox PIT for ROABPs

Wednesday, November 1, 2023 12:15 AM

A read-once oblivious branching program (ROABP) in variable order $X_1, \cdots, X_n$ is a layered weighted directed graph B:



n = length $\quad d$ = degree

w = width

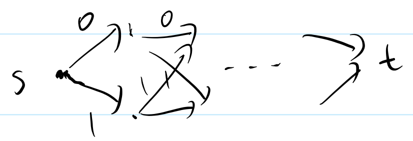
For u on layer $i-1$, v on layer i,

$w(u,v) \in \mathbb{F}[X_i]$ and $\deg(w(u,v)) \le d$.

B computes the polynomial $\sum_{\text{path } p: s \to t} \prod_{e \in p} w(e)$, which we also denote by B.

<u>Thm</u> (Raz - Shpilka '04) $\exists$ a white-box PIT algorithm for the class of ROABPs with length n, width w, degree d, whose time complexity is $\text{poly}(n,d,w)$.

ROABPs are analogues of read-once branching programs. The latter can be used to model small-space algorithms ($w = 2^{\text{space}}$).



We will describe a poly-time algorithm that constructs a hitting set for B given B.

IMM representation $\quad B$ = (1,1)-th entry of $A_1 A_2 \cdots A_n$, where $A_i \in \mathbb{F}[X_i]^{w \times w}$ and $\deg(A_i(j,k)) \le d$.

$A_1, \cdots, A_n$ can be easily read off from B.

Let $A \in \mathbb{F}[X_1, \cdots, X_n]^{w \times w}$.

We can view A as a "polynomial over $\mathbb{F}^{w \times w}$":

$$A = \sum_{\text{monomial } m} A_m \cdot m, \text{ where } A_m \in \mathbb{F}^{w \times w}$$ and m's multiplied to each entry of A_m individually.

Define $\text{coeff}_m(A) = A_m$.

Define $\text{coeffspan}(A) = \text{span}_{\mathbb{F}}(\text{coeff}_m(A) : m \text{ monomial of } A)$.

Define coeffspan$(A) = \mathrm{span}_{\mathbb{F}}(\mathrm{coeff}_m(A)) \ldots$

For $a \in \mathbb{F}^n$, let $A(a) = \sum_m A_m \cdot m(a) \in \mathbb{F}^{w \times w}$.

Note $A(a) \in$ coeffspan(A).

For $A = A_1 \cdots A_n$, we will construct points $a_1, \ldots, a_t$, $t = \mathrm{poly}(n,d,w)$,

s.t. $\mathrm{span}(A(a_i) : 1 \le i \le t) =$ coeffspan(A).

Then $B \ne 0 \Leftrightarrow A(1,1) \ne 0 \Leftrightarrow (A(a_i))(1,1) \ne 0$ for some $i \in \{1, \ldots, t\}$.

So this gives a poly-time PIT algorithm.

It remains to construct $a_1, \ldots, a_t$ from $A_1, \ldots, A_n$.

We will recursively construct $a_1, \ldots, a_t \in \mathbb{F}^{\ell - j + 1}$ for $A_j \cdots A_\ell$ $(j \le \ell)$

s.t. $\mathrm{span}(A(a_i)) =$ coeffspan$(A_j \cdots A_\ell)$

Base case: $j = \ell$

Let $a_0, \ldots, a_d \in \mathbb{F}$ be distinct.

Then $A_j = \sum_{i=0}^{d} A(a_i) \cdot \prod_{\substack{1 \le i' \le d \\ i' \ne i}} \frac{x_j - a_{i'}}{a_i - a_{i'}}$ (Lagrange interpolation)

So $\mathrm{span}(A_j(a_i) : 0 \le i \le d) =$ coeffspan(A_j).

Consider $A = BC$, $B \in \mathbb{F}[x_j, \ldots, x_k]^{w \times w}$, $C \in \mathbb{F}[x_{k+1}, \ldots, x_\ell]^{w \times w}$.

Suppose $b_1, \ldots, b_{t_1} \in \mathbb{F}^{k-j+1}$ s.t. $\mathrm{span}(B(b_i) : 1 \le i \le t_1) =$ coeffspan(B),

$c_1, \ldots, c_{t_2} \in \mathbb{F}^{\ell - k}$ s.t. $\mathrm{span}(C(c_i) : 1 \le i \le t_2) =$ coeffspan(C).

Lemma: Let $a_{i,i'} = (b_i, c_{i'})$. Then $\mathrm{span}(A(a_{i,i'}) : 1 \le i \le t_1, 1 \le i' \le t_2)$
$=$ coeffspan(A).

Pf: Consider a monomial $m = m_1 \cdot m_2$ in $x_j, \ldots, x_\ell$

where m_1 depends on $x_j, \ldots, x_k$ and m_2 depends on $x_{k+1}, \ldots, x_\ell$.

Then $\ldots$ t_1 $\ldots$

where m_1 depends on $X_j, \ldots, X_k$ and m_2 depends on $X_{k+1}, \ldots, X_\ell$.

Then $\mathrm{coeff}_{m_1}(B) = \sum_{i=1}^{t_1} \alpha_i B(b_i)$ for some $\alpha_i \in \mathbb{F}$ and

$\mathrm{coeff}_{m_2}(C) = \sum_{i=1}^{t_2} \beta_i C(c_i)$ for some $\beta_i \in \mathbb{F}$.

Note $B = \sum_{m} \mathrm{coeff}_m(B) \cdot m$ (in $X_j, \ldots, X_k$), $C = \sum_{m} \mathrm{coeff}_m(C) \cdot m$ (in $X_{k+1}, \ldots, X_\ell$).

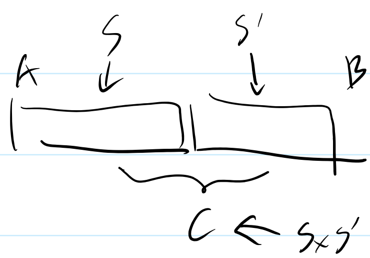
So
$$A = B \cdot C = \left(\sum_m \mathrm{coeff}_m(B) \cdot m\right)\left(\sum_{m'} \mathrm{coeff}_{m'}(C)\, m'\right)$$
$$= \sum_{m,m'} \underbrace{\mathrm{coeff}_m(B) \cdot \mathrm{coeff}_{m'}(C)}\, \cdot m m'$$
$$= \sum_{m,m'} \mathrm{coeff}_{mm'}(A)\, mm'.$$

($m = \begin{pmatrix} m & & \\ & \ddots & \\ & & m \end{pmatrix}$ commutes with everything.)

So
$$\mathrm{coeff}_{m_1 m_2}(A) = \mathrm{coeff}_{m_1}(B) \cdot \mathrm{coeff}_{m_2}(C) = \sum_{i=1}^{t_1} \sum_{i'=1}^{t_2} \alpha_i \beta_{i'} B(b_i) \cdot C(c_{i'})$$
$$= \sum_{i=1}^{t_1} \sum_{i'=1}^{t_2} \alpha_i \beta_{i'} A(a_{i,i'})$$

So $\mathrm{coeffspan}(A) = \mathrm{span}(A(a_{i,i'}) : 1 \le i \le t_1,\ 1 \le i' \le t_2)$.

So from $S = \{b_i\}$ and $S' = \{c_i\}$, we can just construct $S \times S'$.



However, this increase the size of the set of points...

Note $\mathrm{coeffspan}(A) \subseteq \mathbb{F}^{w \times w}$ and hence its dimension is at most w^2.

By picking a subset of a_i s.t. $A(a_i)$ form a basis of $\mathrm{coeffspan}(A)$,

we reduce # of a_i to $\le w^2$ at each step.

This yields a poly-time algorithm. $\square$

On the other hand, no black-box PIT algorithm is known.
Known explicit hitting sets have quasi polynomial size.

This is analogous to PRG constructions for read-once branching programs with seed length $O(\log^2 n)$ (Nisan, Impagliazzo-Nisan-Wigderson).