20. Blackbox PIT for ROABPs

Monday, November 6, 2023 12:40 AM

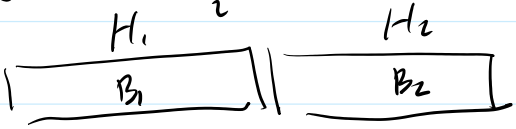
<u>Thm</u> (Forbes-Shpilka '12). Let C be the family of ROABPs over $\mathbb{F}$ of length n, width w, and degree d in a <u>known</u> variable order $x_1, \dots, x_n$.

There is an explicit construction of hitting sets for C of size $\le (nwd)^{O(\log n)}$.

Same result holds if the variable order is unknown (Agrawal-Gurjar-Korwar-Saxena '14).

High-level idea: recurse and merge.

Recursively construct H_i for the two halves B_1 and B_2



Then $H_1 \times H_2$ is a hitting set for $B = B_1 \circ B_2$.

Instead of using $H_1 \times H_2$, we merge H_1 and H_2 in a ~~more~~ efficient way.

This approach is the analogue of the PRG constructions of Nisan and Impagliazzo-Nisan-Wigderson.

$G_{i+1}(x,y) := G_i(x) \cdot G_{i+1}(E(x,y))$.

E is constructed via extractors or hash functions.

$B = (A_1 \cdots A_n)[1,1]$, $A_i[j,k] \in \mathbb{F}[x_i]$, $\deg(A_i) \le d$.

Recall for $A \in \mathbb{F}[x_1, \dots, x_n]^{w \times w}$, $\mathrm{coeffspan}(A) = \mathrm{span}_{\mathbb{F}}(\mathrm{coeff}_m(A) : m \text{ monomial of } A)$.

For $A = A_i \cdots A_{i+k-1} \in \mathbb{F}[x_i, \dots, x_{i+k-1}]^{w \times w}$, we recursively construct

$H = \bigcup_{s \in \{0,1\}^r} H_s \subseteq \mathbb{F}^k$ s.t. $|H_s| \le \max(w^2, d+1)$ and for most $s \in \{0,1\}^r$, it holds:

$$\mathrm{span}\{A(a) : a \in H_s\} = \mathrm{coeffspan}(A).$$

Base case: $A = A_i$. Then for any H of size $d+1$, $\mathrm{span}(A(a) : a \in H) = \mathrm{coeffspan}(A)$.

Base case: $A = A_i$. Then for any H of size $d+1$, $\mathrm{span}(A(a) : a \in H_S) = \mathrm{coeffspan}(A)$.
$r = 0$. (see the last lecture.)

Induction: $A = B \cdot C$, B, C each depends on $k/2$ variables.

Suppose $H_1 = \bigcup_{S \in \{0,1\}^r} H_{1,S} \subseteq \mathbb{F}^{k/2}$, and $H_2 = \bigcup_{S \in \{0,1\}^r} H_{2,S} \subseteq \mathbb{F}^{k/2}$ work for B and C respectively.

Then $H = \bigcup_{S \in \{0,1\}^r} (H_{1,S} \times H_{2,S})$ works for $A = BC$

use same S for both B and C.

S is good w.h.p. by the union bound.

i.e. $\mathrm{span}(A(a) : a \in H_{1,S} \times H_{2,S}) = \mathrm{coeffspan}(A)$

Fix good S. Then $\exists$ $g_1, \dots, g_k$ s.t. $g_i \in \mathbb{F}[X_i]$, $\deg(g_i) \leq (\max(w^2, d+1))^2$

s.t. $H_{1,S} \times H_{2,S} = \{(g_1(a), \dots, g_k(a)) : a \in S\}$, $S \subseteq \mathbb{F}$, $|S| = H_{1,S} \times H_{2,S}$

i.e. we find a curve passing through the points in $H_{1,S} \times H_{2,S}$

Such $g_1, \dots, g_k$ exist and can be constructed by interpolation.

Then $\mathrm{coeffspan}(A) = \mathrm{span}(A(a) : a \in H_{1,S} \times H_{2,S}) \subseteq \mathrm{coeffspan}(A(g_1(z), \dots, g_k(z)))$
$\subseteq \mathrm{coeffspan}(A)$, with $A(g_1(z), \dots, g_k(z)) \in \mathbb{F}[z]^{w \times w}$

$\Rightarrow \mathrm{coeffspan}(A(g_1(z), \dots, g_k(z))) = \mathrm{coeffspan}(A)$.

Let $\tilde{A} = A(g_1(z), \dots, g_k(z)) \in \mathbb{F}[z]^{w \times w}$. Then $\deg(\tilde{A}) \leq dk(\max(w^2, d+1))^2 =: D$.

Lemma: Let $M \in \mathbb{F}[z]^{w \times w}$ be of degree $\leq D$. Let $S \subseteq \mathbb{F}^\times$ be a finite set.

$\omega \in \mathbb{F}^\times$ s.t. $1, \omega, \dots, \omega^D$ are distinct.

Then for all but $\leq \mathrm{poly}(D, w)$ values of $\alpha \in S$

$$\mathrm{coeffspan}(M) = \mathrm{span}_{\mathbb{F}}(M(\alpha), M(\alpha\omega), \dots, M(\alpha\omega^{w^2-1})).$$

Pf: For $i \in \{0, 1, \dots, D\}$, straighten $\mathrm{coeff}_{z^i}(M) \in \mathbb{F}^{w \times w}$ to a (column) vector in $\mathbb{F}^{w^2}$

Let $A = (\mathrm{coeff}_{z^i}(M))_{i=0,\dots,D} = \left[\mathrm{coeff}_1(M), \dots, \mathrm{coeff}_{z^D}(M)\right] \in \mathbb{F}^{w^2 \times (D+1)}$.

For $j \in \{0,\dots,w^2-1\}$ and $\alpha \in S$, $M(\alpha w^j) = \sum_{i=0}^{D} \mathrm{coeff}_{z^i}(M) \cdot (\alpha w^j)^i$

So $A \cdot \left[(\alpha w^j)^i\right]_{\underset{\uparrow\ \text{row index}}{i=0,\dots,D},\ \underset{\uparrow\ \text{column index.}}{j=0,\dots,w^2-1}} = \left(M(\alpha), \dots, M(\alpha w^{w^2-1})\right)$

By the fact that $\left[(\alpha w^j)^i\right]_{\alpha \in S}$ is a seeded (lossless) rank extractor, for most $\alpha \in S$,

$\mathrm{rank}\left(M(\alpha) \cdots M(\alpha w^{w^2-1})\right) = \mathrm{rank}(A)$, which means the two matrices have the same column span.

This is exactly coeffspan(A) $\square$

Apply the lemma to $M = A$. This shows

$$H = \bigcup_{s \in \{0,1\}^r} \bigcup_{\alpha \in S'} \{(g_1(\alpha w^i), \dots, g_k(\alpha w^i)) : 0 \le i < w^2-1\} \text{ works for } A = BC.$$

$\subseteq H_{1,s} \times H_{2,s}$

S' of size $\mathrm{poly}(n, w, d)$ ← n needed for the union bound over all layers.

$r' = r + \log_2 |S'| = r + O(\log(nwd))$

Final $r = O(\log n \cdot \log(nwd))$ since there are $\log_2 n$ levels of recursion

$\Rightarrow$ Final H has size $\le 2^{O(\log n \cdot \log(nwd))} \cdot w^2 = (nwd)^{O(\log n)}$.

$\square$ (proof of Thm).

The above construction requires the variable order $x_1, \dots, x_n$ to be known.

[AGKS '14] : same result except the variable order can be unknown.

In [FS'12], the coefficient span coeffspan(A) is spanned by

$\{A(a_i)\}_{i \in I}$, a_i pseudorandom.

$a_i = (a_{i,1}, \dots, a_{i,n})$.

$\shortparallel$

$A[x_1 \dots x_n] / \langle x_1 - a_{i,1}, \dots, x_n - a_{i,n} \rangle$

$$a_i = \langle a_{i,1}, \cdots, a_{i,n} \rangle.$$

$$A[x_1, \ldots, x_n] / \langle x_1 - a_{i,1}, \ldots, x_n - a_{i,n} \rangle$$

[AGKS'14]: pseudorandomly translate $x_i \mapsto x_i - a_i$, s.t. coeffspan(A) is spanned by the low **degree** coefficients of A.

Then perform substitutions $x_i \mapsto y^{w(x_i)}$

where $w(x_i) = \sum_{j=1}^{k} w_j(x_i) \cdot h^{k-j}$, h large enough.

$w_1, \ldots, w_k$ pseudorandom weight assignments $\{x_1, \ldots, x_i\} \mapsto \mathbb{N}^+$

s.t. w.h.p. w isolates a collection of low-degree monomials m_i for which coeff$_{m_i}(A)$ span coeffspan(A).

Analysis is recursive and similar to [FS'12]. But the required property of the construction is <u>invariant</u> under permutation of variables. So the variable order can be unknown.