Lower bounds on the sum of 25^{th}-powers of univariates lead to complete derandomization of PIT

Pranjal Dutta (CMI & IIT Kanpur)
Nitin Saxena (IIT Kanpur)
Thomas Thierauf (Aalen University)

SIGTACS Webinar @CSE, IITK

Table of contents

1. Introduction
2. Conjecture C1 and Algebraic Complexity
3. Circuit Normal Form (CNF) and Algebraic Complexity
4. Proof Idea of Main Theorems
5. Conclusion

Introduction

Sum of r^{th}-powers

Sum of r^{th}-powers

For a *univariate* polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$, and a positive integer r, we say that f is computed as a *sum of r^{th}-powers*, if

Sum of r^{th}-powers

For a *univariate* polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$, and a positive integer r, we say that f is computed as a *sum of r^{th}-powers*, if

$$f = \sum_{i=1}^{s} c_i \cdot \ell_i^r , \tag{1}$$

for some $s \geq 1$, $c_i \in \mathbb{F}$ and $\ell_i(x) \in \mathbb{F}[x]$.

Sum of r^{th}-powers

For a *univariate* polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$, and a positive integer r, we say that f is computed as a *sum of r^{th}-powers*, if

$$f = \sum_{i=1}^{s} c_i \cdot \ell_i^r , \tag{1}$$

for some $s \geq 1$, $c_i \in \mathbb{F}$ and $\ell_i(x) \in \mathbb{F}[x]$.

- The *sum of r^{th}-powers* is a complete model (for large enough $\mathbb{F}$).

Sum of r^{th}-powers

For a *univariate* polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$, and a positive integer r, we say that f is computed as a *sum of r^{th}-powers*, if

$$f \;=\; \sum_{i=1}^{s} c_i \cdot \ell_i^r \;, \tag{1}$$

for some $s \geq 1$, $c_i \in \mathbb{F}$ and $\ell_i(x) \in \mathbb{F}[x]$.

- The *sum of r^{th}-powers* is a complete model (for large enough $\mathbb{F}$). Because, for any *distinct* λ_i, there are $c_i \in \mathbb{F}$ such that

$$f(x) \;=\; \sum_{i=0}^{r} c_i \cdot (f(x) + \lambda_i)^r$$

Sum of r^{th}-powers

For a *univariate* polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$, and a positive integer r, we say that f is computed as a *sum of r^{th}-powers*, if

$$f \;=\; \sum_{i=1}^{s} c_i \cdot \ell_i^r \;, \tag{1}$$

for some $s \geq 1$, $c_i \in \mathbb{F}$ and $\ell_i(x) \in \mathbb{F}[x]$.

- The *sum of r^{th}-powers* is a complete model (for large enough $\mathbb{F}$). Because, for any *distinct* λ_i, there are $c_i \in \mathbb{F}$ such that

$$f(x) \;=\; \sum_{i=0}^{r} c_i \cdot (f(x) + \lambda_i)^r$$

- For a fixed f, r, s representation Eqn. (1) might not exist.

Sum of r^{th}-powers

For a *univariate* polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$, and a positive integer r, we say that f is computed as a *sum of* r^{th}*-powers*, if

$$f \;=\; \sum_{i=1}^{s} c_i \cdot \ell_i^r \;, \tag{1}$$

for some $s \geq 1$, $c_i \in \mathbb{F}$ and $\ell_i(x) \in \mathbb{F}[x]$.

- The *sum of* r^{th}*-powers* is a complete model (for large enough $\mathbb{F}$). Because, for any *distinct* λ_i, there are $c_i \in \mathbb{F}$ such that

$$f(x) \;=\; \sum_{i=0}^{r} c_i \cdot (f(x) + \lambda_i)^r$$

- For a fixed f, r, s representation Eqn. (1) might not exist. Eg. $(x+1)^{r+1} \;=\; c_1 \cdot \ell_1^r + c_2 \cdot \ell_2^r$ is not possible!

New Measure

New Measure

- A natural complexity measure in (1) is the *support-union size*, namely the number of distinct monomials in the representation, $\left|\bigcup_{i=1}^{s} \mathrm{supp}(\ell_i)\right|$ where *support* $\mathrm{supp}(\ell)$ denotes the set of nonzero monomials in the polynomial ℓ.

New Measure

- A natural complexity measure in (1) is the *support-union size*, namely the number of distinct monomials in the representation, $\left|\bigcup_{i=1}^{s} \mathrm{supp}(\ell_i)\right|$ where *support* $\mathrm{supp}(\ell)$ denotes the set of nonzero monomials in the polynomial ℓ.
  Eg. $(s = 1)$ Let $(x+1)^d = \ell_1^r$ where $r \mid d$. So, $\ell_1 = (x+1)^{d/r}$. Thus, $\mathrm{supp}(\ell_1) = \{x^0, \ldots, x^{d/r}\} \implies |\mathrm{supp}(\ell_1)| = d/r + 1$.

New Measure

- A natural complexity measure in (1) is the *support-union size*, namely the number of distinct monomials in the representation, $\left|\bigcup_{i=1}^{s} \mathrm{supp}(\ell_i)\right|$ where *support* $\mathrm{supp}(\ell)$ denotes the set of nonzero monomials in the polynomial ℓ.
  Eg. $(s = 1)$ Let $(x+1)^d = \ell_1^r$ where $r \mid d$. So, $\ell_1 = (x+1)^{d/r}$. Thus, $\mathrm{supp}(\ell_1) = \{x^0, \ldots, x^{d/r}\} \implies |\mathrm{supp}(\ell_1)| = d/r + 1$.
- The *support-union size of* f with respect to r and s, denoted $U_{\mathbb{F}}(f, r, s)$ is defined as the minimum support-union size when f is written in the form (1), and ∞, if no such representation exists.

New Measure

- A natural complexity measure in (1) is the *support-union size*, namely the number of distinct monomials in the representation, $\left|\bigcup_{i=1}^{s} \mathrm{supp}(\ell_i)\right|$ where *support* $\mathrm{supp}(\ell)$ denotes the set of nonzero monomials in the polynomial ℓ.
  Eg. $(s = 1)$ Let $(x+1)^d = \ell_1^r$ where $r \mid d$. So, $\ell_1 = (x+1)^{d/r}$. Thus, $\mathrm{supp}(\ell_1) = \{x^0, \ldots, x^{d/r}\} \implies |\mathrm{supp}(\ell_1)| = d/r + 1$.

- The *support-union size of* f with respect to r and s, denoted $U_{\mathbb{F}}(f, r, s)$ is defined as the minimum support-union size when f is written in the form (1), and ∞, if no such representation exists.

- **Observe:** $|\mathrm{supp}(\ell^r)| \leq |\mathrm{supp}(\ell)|^r$ for $r \geq 1$.

New Measure

- A natural complexity measure in (1) is the *support-union size*, namely the number of distinct monomials in the representation, $\left|\bigcup_{i=1}^{s} \text{supp}(\ell_i)\right|$ where *support* $\text{supp}(\ell)$ denotes the set of nonzero monomials in the polynomial ℓ.
  Eg. $(s = 1)$ Let $(x+1)^d = \ell_1^r$ where $r \mid d$. So, $\ell_1 = (x+1)^{d/r}$. Thus, $\text{supp}(\ell_1) = \{x^0, \ldots, x^{d/r}\} \implies |\text{supp}(\ell_1)| = d/r + 1$.

- The *support-union size of* f with respect to r and s, denoted $U_{\mathbb{F}}(f, r, s)$ is defined as the minimum support-union size when f is written in the form (1), and ∞, if no such representation exists.

- **Observe:** $|\text{supp}(\ell^r)| \leq |\text{supp}(\ell)|^r$ for $r \geq 1$. Thus, for all f, r, s:

$$\boxed{U_{\mathbb{F}}(f, r, s) \;\geq\; \Omega(|\text{supp}(f)|^{1/r})}$$

Understanding $U((x+1)^d, r, \cdot)$

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Question: What can we say about $U_{\mathbb{F}}(f_d, r, \cdot)$?

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Question: What can we say about $U_{\mathbb{F}}(f_d, r, \cdot)$? Here are few observations:

- For $s = 1$, if $r \mid d$, then we have $\boxed{U_{\mathbb{F}}(f_d, r, 1) = d/r + 1}$.

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Question: What can we say about $U_{\mathbb{F}}(f_d, r, \cdot)$? Here are few observations:

- For $s = 1$, if $r \mid d$, then we have $\boxed{U_{\mathbb{F}}(f_d, r, 1) = d/r + 1}$.
- For $s = 2$, we show that $\boxed{U_{\mathbb{F}}(f_d, r, 2) \geq d/r + 1}$.

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Question: What can we say about $U_{\mathbb{F}}(f_d, r, \cdot)$? Here are few observations:

- For $s = 1$, if $r \mid d$, then we have $\boxed{U_{\mathbb{F}}(f_d, r, 1) = d/r + 1}$.
- For $s = 2$, we show that $\boxed{U_{\mathbb{F}}(f_d, r, 2) \geq d/r + 1}$.
- (Small s). For $s = r + 1$ and *any* d, we show that

$$\boxed{U_{\mathbb{F}}(f_d, r, r+1) \ \leq \ d/r + r}.$$

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Question: What can we say about $U_{\mathbb{F}}(f_d, r, \cdot)$? Here are few observations:

- For $s = 1$, if $r \mid d$, then we have $\boxed{U_{\mathbb{F}}(f_d, r, 1) = d/r + 1}$.
- For $s = 2$, we show that $\boxed{U_{\mathbb{F}}(f_d, r, 2) \geq d/r + 1}$.
- (Small s). For $s = r + 1$ and *any* d, we show that

$$\boxed{U_{\mathbb{F}}(f_d, r, r+1) \;\leq\; d/r + r}.$$

- (Large s). For $s \geq c \cdot (d+1)$ for *any* $c > r$, we show that

$$\boxed{U_{\mathbb{F}}(f_d, r, s) \;\leq\; O(d^{1/r})}\;.$$

Understanding $U((x+1)^d, r, \cdot)$

Fix the notations: $f_d(x) := (x+1)^d$ and $\mathbb{F} = \mathbb{Q}$.

Question: What can we say about $U_{\mathbb{F}}(f_d, r, \cdot)$? Here are few observations:

- For $s = 1$, if $r \mid d$, then we have $\boxed{U_{\mathbb{F}}(f_d, r, 1) = d/r + 1}$.
- For $s = 2$, we show that $\boxed{U_{\mathbb{F}}(f_d, r, 2) \geq d/r + 1}$.
- (Small s). For $s = r + 1$ and *any* d, we show that

$$\boxed{U_{\mathbb{F}}(f_d, r, r+1) \ \leq \ d/r + r}\ .$$

- (Large s). For $s \geq c \cdot (d+1)$ for *any* $c > r$, we show that

$$\boxed{U_{\mathbb{F}}(f_d, r, s) \ \leq \ O(d^{1/r})}\ .$$

Thus, for large s, we get $U_{\mathbb{F}}(f_d, r, s) = \Theta(d^{1/r})$, which resolves this case.

Support-union Conjecture

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{ r^m - 1 \mid m \in \mathbb{N} \} .$$

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{ r^m - 1 \mid m \in \mathbb{N} \} .$$

Motivated from the examples above, we *could* conjecture the following.

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{ r^m - 1 \mid m \in \mathbb{N} \} .$$

Motivated from the examples above, we *could* conjecture the following.

Possible Conjecture 1

For $s \leq d$ and a constant prime-power r,

$$U_{\mathbb{F}}(f_d, r, s) \geq d/r$$

for all large enough $d \in I_r$.

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{\, r^m - 1 \mid m \in \mathbb{N} \,\} .$$

Motivated from the examples above, we *could* conjecture the following.

Possible Conjecture 2

For positive constant $\delta_1 \leq 1$ and a constant prime-power r,

$$U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \;\geq\; d/r$$

for all large enough $d \in I_r$.

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{\, r^m - 1 \mid m \in \mathbb{N} \,\} .$$

Motivated from the examples above, we **conjecture** the following.

Support-union Conjecture (C1)

For positive constants $\delta_1 \leq 1, \delta_2 \geq 1$ and a constant prime-power r,

$$U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \;\geq\; d/r^{\delta_2}$$

for all large enough $d \in I_r$.

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{ r^m - 1 \mid m \in \mathbb{N} \} .$$

Motivated from the examples above, we **conjecture** the following.

Support-union Conjecture (C1)

For positive constants $\delta_1 \leq 1, \delta_2 \geq 1$ and a constant prime-power r,

$$U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \;\geq\; d/r^{\delta_2}$$

for all large enough $d \in I_r$.

There are other intricate polynomial families for which we suspect that C1 is true; for e.g. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$.

Support-union Conjecture

For technical reasons, we will restrict d to the domain

$$I_r := \{ r^m - 1 \mid m \in \mathbb{N} \} .$$

Motivated from the examples above, we **conjecture** the following.

Support-union Conjecture (C1)

For positive constants $\delta_1 \leq 1, \delta_2 \geq 1$ and a constant prime-power r,

$$U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \;\geq\; d/r^{\delta_2}$$

for all large enough $d \in I_r$.

There are other intricate polynomial families for which we suspect that C1 is true; for e.g. $\prod_{i \in [d]}(x - i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$.

Reason to choose f_d is that it is a very simple polynomial.

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Proof.

If $r = p^\ell$ for some prime p and $\ell \in \mathbb{N}$, then for $d \in I_r$:

$$\binom{d}{i} \equiv \pm 1 \bmod p \implies |\mathrm{supp}(f_d \bmod p)| = d + 1 \; .$$

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Proof.

If $r = p^\ell$ for some prime p and $\ell \in \mathbb{N}$, then for $d \in I_r$:

$$\binom{d}{i} \equiv \pm 1 \bmod p \implies |\mathrm{supp}(f_d \bmod p)| = d + 1 \; .$$

Observe: $\ell_i(x)^r \equiv \ell_i(x^r) \bmod p$ and $\left|\bigcup_i \mathrm{supp}(\ell_i(x))\right| = \left|\bigcup_i \mathrm{supp}(\ell_i(x^r))\right|$.

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Proof.

If $r = p^\ell$ for some prime p and $\ell \in \mathbb{N}$, then for $d \in I_r$:

$$\binom{d}{i} \equiv \pm 1 \bmod p \implies |\mathrm{supp}(f_d \bmod p)| = d + 1 \ .$$

Observe: $\ell_i(x)^r \equiv \ell_i(x^r) \bmod p$ and $\left|\bigcup_i \mathrm{supp}(\ell_i(x))\right| = \left|\bigcup_i \mathrm{supp}(\ell_i(x^r))\right|$.

$$f_d = \sum c_i \cdot \ell_i^r$$

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Proof.

If $r = p^\ell$ for some prime p and $\ell \in \mathbb{N}$, then for $d \in I_r$:

$$\binom{d}{i} \equiv \pm 1 \bmod p \implies |\mathrm{supp}(f_d \bmod p)| = d + 1 \ .$$

Observe: $\ell_i(x)^r \equiv \ell_i(x^r) \bmod p$ and $\left|\bigcup_i \mathrm{supp}(\ell_i(x))\right| = \left|\bigcup_i \mathrm{supp}(\ell_i(x^r))\right|$.

$$f_d = \sum c_i \cdot \ell_i^r \implies f_d \bmod p = \sum c_i \cdot \ell_i(x^r) \bmod p$$

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Proof.

If $r = p^\ell$ for some prime p and $\ell \in \mathbb{N}$, then for $d \in I_r$:

$$\binom{d}{i} \equiv \pm 1 \bmod p \implies |\mathrm{supp}(f_d \bmod p)| = d + 1 \ .$$

Observe: $\ell_i(x)^r \equiv \ell_i(x^r) \bmod p$ and $\left|\bigcup_i \mathrm{supp}(\ell_i(x))\right| = \left|\bigcup_i \mathrm{supp}(\ell_i(x^r))\right|$.

$$\begin{aligned} f_d &= \sum c_i \cdot \ell_i^r \implies f_d \bmod p = \sum c_i \cdot \ell_i(x^r) \bmod p \\ &\implies \left|\bigcup \mathrm{supp}(\ell_i)\right| \geq d + 1 \end{aligned}$$

Conjecture C1 over $\mathbb{Z}$ (Integer ring)

C1 over $\mathbb{Z}$

Conjecture C1 holds true over $\mathbb{Z}$.

Proof.

If $r = p^\ell$ for some prime p and $\ell \in \mathbb{N}$, then for $d \in I_r$:

$$\binom{d}{i} \equiv \pm 1 \bmod p \implies |\mathrm{supp}(f_d \bmod p)| = d + 1 \ .$$

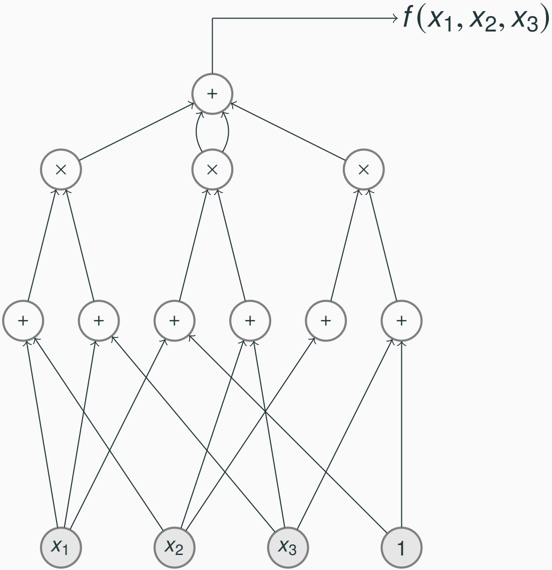
Observe: $\ell_i(x)^r \equiv \ell_i(x^r) \bmod p$ and $\left|\bigcup_i \mathrm{supp}(\ell_i(x))\right| = \left|\bigcup_i \mathrm{supp}(\ell_i(x^r))\right|$.

$$\begin{aligned} f_d = \sum c_i \cdot \ell_i^r &\implies f_d \bmod p = \sum c_i \cdot \ell_i(x^r) \bmod p \\ &\implies \left|\bigcup \mathrm{supp}(\ell_i)\right| \geq d + 1 \\ &\implies U_{\mathbb{Z}}(f_d, r, \cdot) \geq d + 1 > d/r^{\delta_2} \end{aligned}$$

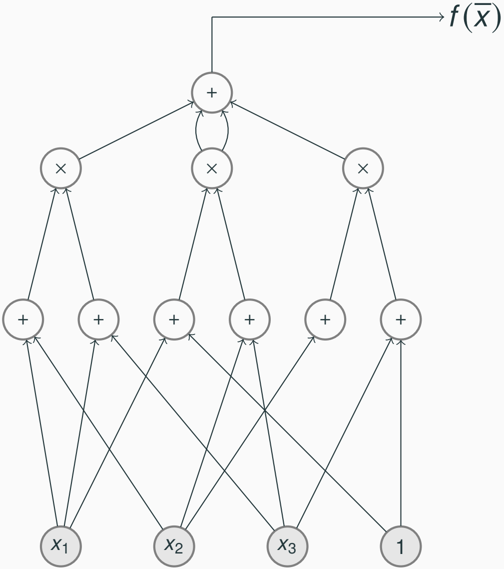
□

Conjecture C1 and Algebraic Complexity

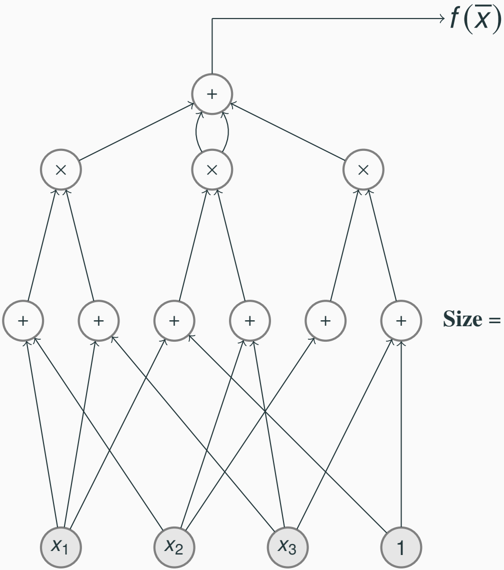
Arithmetic Circuits



Arithmetic Circuits

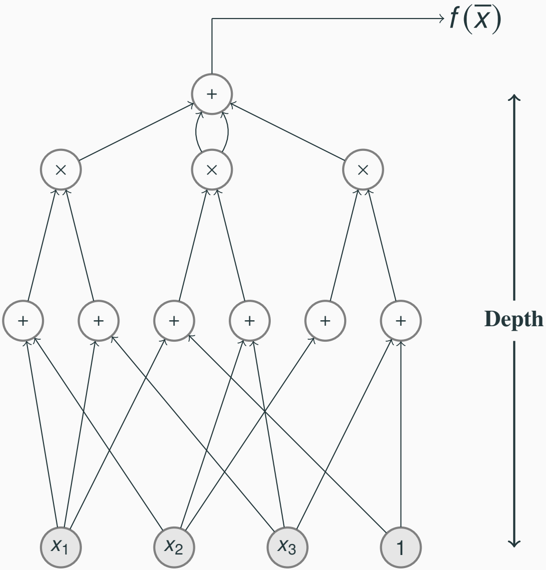


Arithmetic Circuits



Size = number of nodes + edges

Arithmetic Circuits



Two Important Questions

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit.

VP vs. VNP

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a $\mathrm{poly}(n)$-variate polynomial, of degree $\mathrm{poly}(n)$ over $\mathbb{F}$, computed by $\mathrm{poly}(n)$-size circuit.

VP vs. VNP

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a poly(n)-variate polynomial, of degree poly(n) over $\mathbb{F}$, computed by poly(n)-size circuit.
- VNP : A family $\{f_n\}_n \in \mathsf{VNP}$ (over $\mathbb{F}$) if $\exists \{g_n\}_n \in \mathsf{VP}$ & $t(n) = \text{poly}(n)$:

$$\boxed{f_n(\overline{x}) \;=\; \sum_{w \in \{0,1\}^{t(n)}} g_n(\overline{x}, w)}\,.$$

VP vs. VNP

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a poly(n)-variate polynomial, of degree poly(n) over $\mathbb{F}$, computed by poly(n)-size circuit.
- VNP : A family $\{f_n\}_n \in \mathsf{VNP}$ (over $\mathbb{F}$) if $\exists \{g_n\}_n \in \mathsf{VP}$ & $t(n) = \mathrm{poly}(n)$:

$$\boxed{f_n(\overline{x}) \;=\; \sum_{w \in \{0,1\}^{t(n)}} g_n(\overline{x}, w)}\;.$$

- $\{f_n\}_n \in \mathsf{VNP} \implies f_n$ is *explicit*.

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a $\mathrm{poly}(n)$-variate polynomial, of degree $\mathrm{poly}(n)$ over $\mathbb{F}$, computed by $\mathrm{poly}(n)$-size circuit.
- VNP : A family $\{f_n\}_n \in \mathsf{VNP}$ (over $\mathbb{F}$) if $\exists \{g_n\}_n \in \mathsf{VP}$ & $t(n) = \mathrm{poly}(n)$:

$$\boxed{f_n(\overline{x}) \;=\; \sum_{w \in \{0,1\}^{t(n)}} g_n(\overline{x}, w)}\,.$$

- $\{f_n\}_n \in \mathsf{VNP} \implies f_n$ is *explicit*.
- **Sufficient explicitness** (Valiant's Criterion):

VP vs. VNP

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a poly(n)-variate polynomial, of degree poly(n) over $\mathbb{F}$, computed by poly(n)-size circuit.
- VNP : A family $\{f_n\}_n \in \mathsf{VNP}$ (over $\mathbb{F}$) if $\exists \{g_n\}_n \in \mathsf{VP}$ & $t(n) = \text{poly}(n)$:

$$\boxed{f_n(\overline{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\overline{x}, w)}.$$

- $\{f_n\}_n \in \mathsf{VNP} \implies f_n$ is *explicit*.
- **Sufficient explicitness** (Valiant's Criterion): Suppose $\phi : \{0,1\}^* \to \mathbb{N}$ is a function in the class P. Then, the family $\{f_n\}_n \in \mathsf{VNP}$ if

$$f_n(\overline{x}) = \sum_{\boldsymbol{e} \in \{0,1\}^n} \phi(\boldsymbol{e})\, \overline{x}^{\boldsymbol{e}}.$$

VP vs. VNP

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a poly(n)-variate polynomial, of degree poly(n) over $\mathbb{F}$, computed by poly(n)-size circuit.
- VNP : A family $\{f_n\}_n \in \mathsf{VNP}$ (over $\mathbb{F}$) if $\exists \{g_n\}_n \in \mathsf{VP}$ & $t(n) = \mathrm{poly}(n)$:

$$\boxed{f_n(\overline{x}) \;=\; \sum_{w \in \{0,1\}^{t(n)}} g_n(\overline{x}, w)}\,.$$

- $\{f_n\}_n \in \mathsf{VNP} \implies f_n$ is *explicit*.
- **Sufficient explicitness** (Valiant's Criterion): Suppose $\phi : \{0,1\}^* \to \mathbb{N}$ is a function in the class P/poly. Then, the family $\{f_n\}_n \in \mathsf{VNP}$ if

$$f_n(\overline{x}) = \sum_{\boldsymbol{e} \in \{0,1\}^n} \phi(\boldsymbol{e})\, \overline{x}^{\boldsymbol{e}}\,.$$

VP vs. VNP

- **Valiant's Hypothesis:** Prove that symbolic perm_n requires $n^{\omega(1)}$-size circuit. An *equivalent* version is: Prove $\boxed{\mathsf{VP} \neq \mathsf{VNP}}$.
- VP : A family $\{f_n\}_n \in \mathsf{VP}$ (over $\mathbb{F}$) if f_n is a $\mathrm{poly}(n)$-variate polynomial, of degree $\mathrm{poly}(n)$ over $\mathbb{F}$, computed by $\mathrm{poly}(n)$-size circuit.
- VNP : A family $\{f_n\}_n \in \mathsf{VNP}$ (over $\mathbb{F}$) if $\exists\{g_n\}_n \in \mathsf{VP}$ & $t(n) = \mathrm{poly}(n)$:

$$\boxed{f_n(\overline{x}) \;=\; \sum_{w \in \{0,1\}^{t(n)}} g_n(\overline{x}, w)}\;.$$

- $\{f_n\}_n \in \mathsf{VNP} \implies f_n$ is *explicit*.
- **Sufficient explicitness** (Valiant's Criterion): Suppose $\phi : [0,c]^* \to \mathbb{N}$ is a function in the class P/poly. Then, the family $\{f_n\}_n \in \mathsf{VNP}$ if

$$f_n(\overline{x}) = \sum_{\boldsymbol{e} \in [0,c]^n} \phi(\boldsymbol{e})\, \overline{x}^{\boldsymbol{e}}\,.$$

Polynomial Identity Testing

- **Polynomial Identity Testing (*PIT*):** Given a circuit C, test whether C computes the *zero* polynomial *(deterministically)*.

Polynomial Identity Testing

- **Polynomial Identity Testing (*PIT*):** Given a circuit C, test whether C computes the *zero* polynomial *(deterministically)*.
  - *Blackbox*-PIT asks for an algorithm to test the zeroness of a given algebraic circuit via mere *query access*.

Polynomial Identity Testing

- **Polynomial Identity Testing (*PIT*):** Given a circuit C, test whether C computes the *zero* polynomial *(deterministically)*.
  - *Blackbox*-PIT asks for an algorithm to test the zeroness of a given algebraic circuit via mere *query access*.
  - **Hitting sets:** Find a set of points H such that any "small" circuit C that is computing a nonzero polynomial *must* satisfy $C(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in H$.

Polynomial Identity Testing

- **Polynomial Identity Testing (*PIT*):** Given a circuit C, test whether C computes the *zero* polynomial *(deterministically)*.
  - *Blackbox*-PIT asks for an algorithm to test the zeroness of a given algebraic circuit via mere *query access*.
  - **Hitting sets:** Find a set of points H such that any "small" circuit C that is computing a nonzero polynomial *must* satisfy $C(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in H$.

Polynomial Identity Lemma (Ore, Demillo-Lipton, Schwartz, Zippel)

If $P(\overline{x})$ is a nonzero polynomial of degree d, and $S \subseteq \mathbb{F}$ of size at least $d+1$, then $P(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in S^n$.

Polynomial Identity Testing

- **Polynomial Identity Testing (*PIT*):** Given a circuit C, test whether C computes the *zero* polynomial *(deterministically)*.
    - *Blackbox*-PIT asks for an algorithm to test the zeroness of a given algebraic circuit via mere *query access*.
    - **Hitting sets:** Find a set of points H such that any "small" circuit C that is computing a nonzero polynomial *must* satisfy $C(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in H$.

Polynomial Identity Lemma (Ore, Demillo-Lipton, Schwartz, Zippel)

If $P(\overline{x})$ is a nonzero polynomial of degree d, and $S \subseteq \mathbb{F}$ of size at least $d+1$, then $P(\boldsymbol{a}) \neq 0$ for some $\boldsymbol{a} \in S^n$.

This above lemma puts PIT $\in$ RP.

$\mathsf{VP} \neq \mathsf{VNP}$ & **Efficient PIT**

$\boxed{\mathsf{VP} \neq \mathsf{VNP}}$

$\boxed{\text{Explicit Hitting Sets}}$

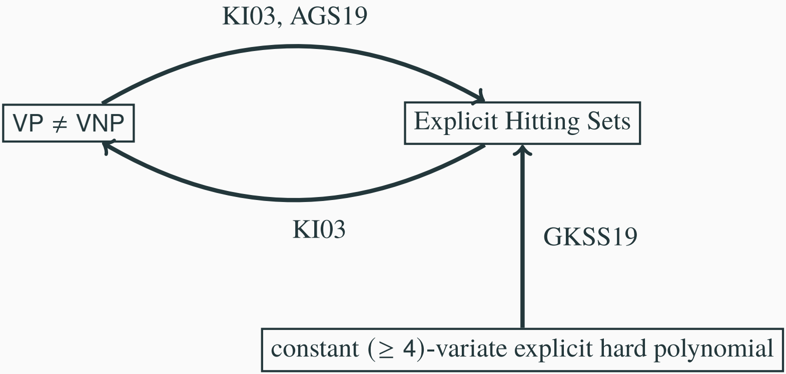
VP ≠ VNP & **Efficient PIT**

$$\boxed{\text{VP} \neq \text{VNP}} \xrightarrow{\text{KI03, AGS19}} \boxed{\text{Explicit Hitting Sets}}$$

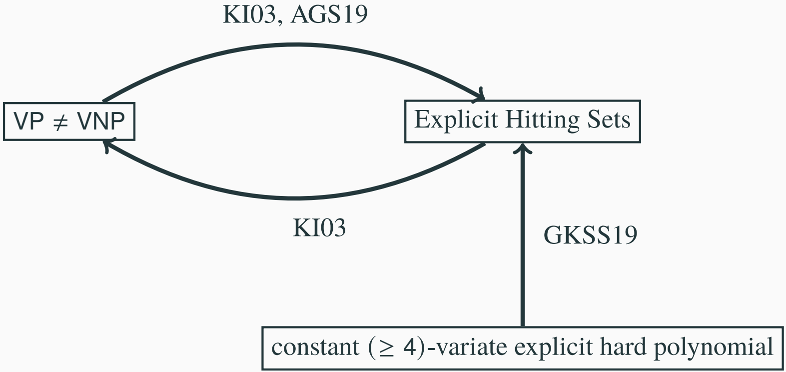
VP $\neq$ VNP & Efficient PIT

$$\begin{tikzcd}
\boxed{\mathsf{VP} \neq \mathsf{VNP}} \arrow[rr, bend left, "\text{KI03, AGS19}"] & & \boxed{\text{Explicit Hitting Sets}} \arrow[ll, bend left, "\text{KI03}"]
\end{tikzcd}$$

VP ≠ VNP & **Efficient PIT**



VP $\neq$ VNP & Efficient PIT



$$\boxed{f(x) = \sum_{i=1}^{s} Q_i^{e_i}, \deg(Q_i) \leq t \text{ and } e_i = \omega(1) \implies s \geq (d/t)^{\Omega(1)}}$$

$$
\begin{tikzcd}
\boxed{\mathsf{VP} \neq \mathsf{VNP}} \arrow[rr, bend left, "\text{KI03, AGS19}"] & & \boxed{\text{Explicit Hitting Sets}} \arrow[ll, bend left, "\text{KI03}"] \\
& & \boxed{\text{constant } (\geq 4)\text{-variate explicit hard polynomial}} \arrow[u, "\text{GKSS19}"'] \\
\boxed{f(x) = \sum_{i=1}^{s} Q_i^{e_i}, \deg(Q_i) \leq t \text{ and } e_i = \omega(1) \implies s \geq (d/t)^{\Omega(1)}} \arrow[uu, bend left, "\text{AV08, Koi12}"]
\end{tikzcd}
$$

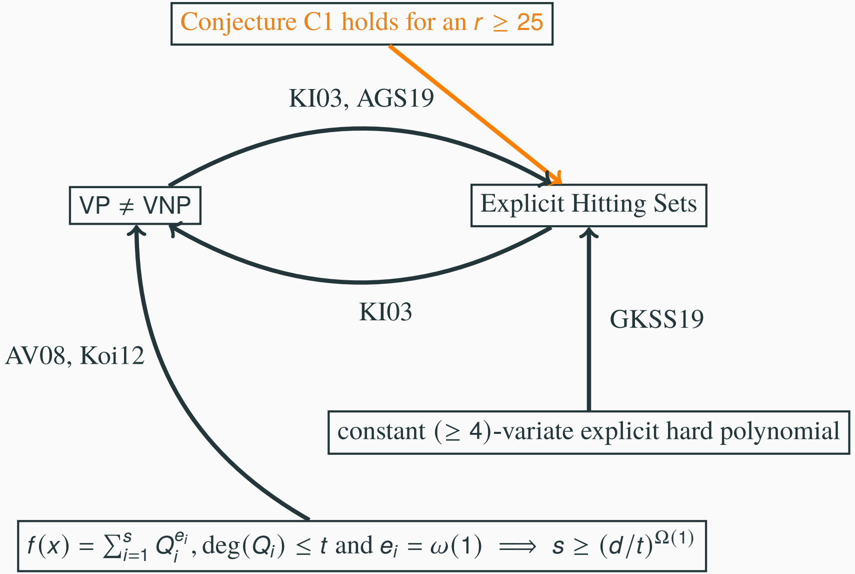
Connecting Conjecture C1 to Algebraic Complexity

Conjecture C1 holds for an $r \geq 25$

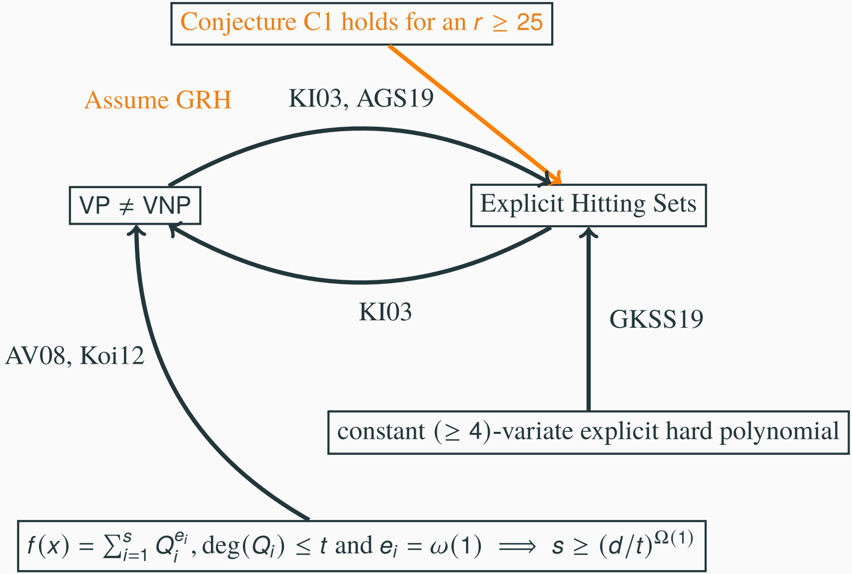
$$\begin{array}{ccc} \mathsf{VP} \neq \mathsf{VNP} & \xrightarrow{\text{KI03, AGS19}} & \text{Explicit Hitting Sets} \\ & \xleftarrow[\text{KI03}]{} & \\ \uparrow{\scriptstyle \text{AV08, Koi12}} & & \uparrow{\scriptstyle \text{GKSS19}} \\ & & \text{constant } (\geq 4)\text{-variate explicit hard polynomial} \end{array}$$

$$f(x) = \sum_{i=1}^{s} Q_i^{e_i}, \deg(Q_i) \leq t \text{ and } e_i = \omega(1) \implies s \geq (d/t)^{\Omega(1)}$$

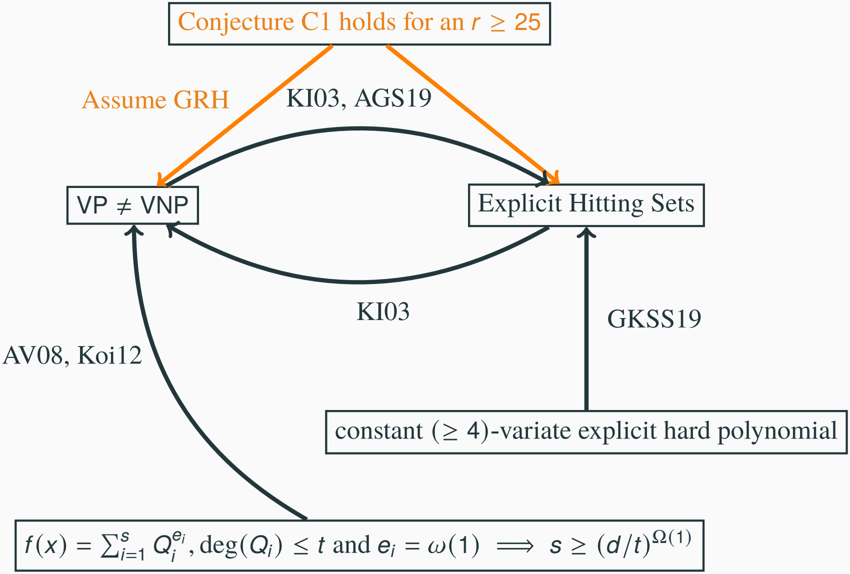
Connecting Conjecture C1 to Algebraic Complexity



Connecting Conjecture C1 to Algebraic Complexity



Connecting Conjecture C1 to Algebraic Complexity



Conjecture C1 and Algebraic Complexity

Recall Conjecture C1.

Conjecture C1 and Algebraic Complexity

$$\text{C1}: \quad \boxed{(x+1)^d = \sum_{i=1}^{d^{\delta_1}} \ell_i^r \implies \Big|\bigcup_i \operatorname{supp}(\ell_i)\Big| \geq d/r^{\delta_2} = \Omega(d)}.$$

Conjecture C1 and Algebraic Complexity

$$\text{C1}: \quad \boxed{(x+1)^d = \sum_{i=1}^{d^{\delta_1}} \ell_i^r \implies \left|\bigcup_i \operatorname{supp}(\ell_i)\right| \geq d/r^{\delta_2} = \Omega(d)}.$$

Theorem 1: Conjecture C1 to PIT

If Conjecture C1 holds for an $r \geq 25$, then blackbox-PIT $\in \mathsf{P}$.

Conjecture C1 and Algebraic Complexity

$$\text{C1}: \quad \boxed{(x+1)^d \; = \; \sum_{i=1}^{d^{\delta_1}} \ell_i^r \implies \left|\bigcup_i \operatorname{supp}(\ell_i)\right| \; \geq \; d/r^{\delta_2} \; = \; \Omega(d)}\,.$$

Theorem 1: Conjecture C1 to PIT

If Conjecture C1 holds for an $r \geq 25$, then blackbox-PIT $\in \mathsf{P}$.

Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

Assume GRH, and Conjecture C1 holds for an $r \geq 25$, then $\mathsf{VP} \neq \mathsf{VNP}$.

Conjecture C1 and Algebraic Complexity

Theorem 1: Conjecture C1 to PIT

If Conjecture C1 holds for an $r \geq 25$, then blackbox-PIT $\in \mathsf{P}$.

Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

Assume GRH, and Conjecture C1 holds for an $r \geq 25$, then $\mathsf{VP} \neq \mathsf{VNP}$.

Theorem 2 is *reminiscent* to the following:

Conjecture C1 and Algebraic Complexity

Theorem 1: Conjecture C1 to PIT

If Conjecture C1 holds for an $r \geq 25$, then blackbox-PIT $\in \mathsf{P}$.

Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

Assume GRH, and Conjecture C1 holds for an $r \geq 25$, then $\mathsf{VP} \neq \mathsf{VNP}$.

Theorem 2 is *reminiscent* to the following:

> *Strong lower bound on sum-of-squares in non-commutative settings implies Permanent is hard [HWY11].*

More on Conjecture C1 and Theorem 1-2

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i \in [d]} (x - i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$. C1 holds for them implies Theorem 1 & 2.

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$. C1 holds for them implies Theorem 1 & 2.
- C1 holds for $\sum_{i=0}^{d} 2^{i^2} x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2}x^i$. C1 holds for them implies Theorem 1 & 2.
- C1 holds for $\sum_{i=0}^{d} 2^{i^2}x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!
- It is *enough* to consider poly-degree restriction on ℓ_i. In fact, for Theorem 1, we can assume $\deg(\ell_i) = O(d)$ while for Theorem 2, we can assume $\deg(\ell_i) = O(d \log d)$.

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$. C1 holds for them implies Theorem 1 & 2.
- C1 holds for $\sum_{i=0}^{d} 2^{i^2} x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!
- It is *enough* to consider poly-degree restriction on ℓ_i. In fact, for Theorem 1, we can assume $\deg(\ell_i) = O(d)$ while for Theorem 2, we can assume $\deg(\ell_i) = O(d\log d)$.
- There is a *relaxed* version of C1 where, instead of the measure $\left|\bigcup \operatorname{supp}(\ell_i)\right|$, we look at $\sum_i |\operatorname{supp}(\ell_i)|$.

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2}x^i$. C1 holds for them implies Theorem 1 & 2.
- C1 holds for $\sum_{i=0}^{d} 2^{i^2}x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!
- It is *enough* to consider poly-degree restriction on ℓ_i. In fact, for Theorem 1, we can assume $\deg(\ell_i) = O(d)$ while for Theorem 2, we can assume $\deg(\ell_i) = O(d\log d)$.
- There is a *relaxed* version of C1 where, instead of the measure $\left|\bigcup \operatorname{supp}(\ell_i)\right|$, we look at $\sum_i |\operatorname{supp}(\ell_i)|$.
    - We call it $S_{\mathbb{F}}(f,r,s)$. Trivially, $U_{\mathbb{F}}(f,r,s) \leq S_{\mathbb{F}}(f,r,s)$.

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$. C1 holds for them implies Theorem 1 & 2.
- C1 holds for $\sum_{i=0}^{d} 2^{i^2} x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!
- It is *enough* to consider poly-degree restriction on ℓ_i. In fact, for Theorem 1, we can assume $\deg(\ell_i) = O(d)$ while for Theorem 2, we can assume $\deg(\ell_i) = O(d \log d)$.
- There is a *relaxed* version of C1 where, instead of the measure $\left|\bigcup \mathrm{supp}(\ell_i)\right|$, we look at $\sum_i |\mathrm{supp}(\ell_i)|$.
  - We call it $S_{\mathbb{F}}(f, r, s)$. Trivially, $U_{\mathbb{F}}(f, r, s) \leq S_{\mathbb{F}}(f, r, s)$.
  - We could similarly conjecture (C2) that $S_{\mathbb{F}}(f_d, r, \cdot)$ is large.

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i\in[d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$. C1 holds for them implies Theorem 1 & 2.
- C1 holds for $\sum_{i=0}^{d} 2^{i^2} x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!
- It is *enough* to consider poly-degree restriction on ℓ_i. In fact, for Theorem 1, we can assume $\deg(\ell_i) = O(d)$ while for Theorem 2, we can assume $\deg(\ell_i) = O(d\log d)$.
- There is a *relaxed* version of C1 where, instead of the measure $\left|\bigcup \mathrm{supp}(\ell_i)\right|$, we look at $\sum_i |\mathrm{supp}(\ell_i)|$.
  - We call it $S_{\mathbb{F}}(f,r,s)$. Trivially, $U_{\mathbb{F}}(f,r,s) \leq S_{\mathbb{F}}(f,r,s)$.
  - We could similarly conjecture (C2) that $S_{\mathbb{F}}(f_d,r,\cdot)$ is large.
  - C2 and GRH implies $\mathsf{VP} \neq VNP$;

More on Conjecture C1 and Theorem 1-2

- There are other candidate polynomials for C1, for eg. $\prod_{i \in [d]}(x-i)$, $\sum_{i=0}^{d} 2^{i^2} x^i$. C1 holds for them implies Theorem 1 & 2.

- C1 holds for $\sum_{i=0}^{d} 2^{i^2} x^i$ implies $\mathsf{VP} \neq \mathsf{VNP}$ without GRH!

- It is *enough* to consider poly-degree restriction on ℓ_i. In fact, for Theorem 1, we can assume $\deg(\ell_i) = O(d)$ while for Theorem 2, we can assume $\deg(\ell_i) = O(d \log d)$.

- There is a *relaxed* version of C1 where, instead of the measure $\left|\bigcup \operatorname{supp}(\ell_i)\right|$, we look at $\sum_i |\operatorname{supp}(\ell_i)|$.
  - We call it $S_{\mathbb{F}}(f, r, s)$. Trivially, $U_{\mathbb{F}}(f, r, s) \leq S_{\mathbb{F}}(f, r, s)$.
  - We could similarly conjecture (C2) that $S_{\mathbb{F}}(f_d, r, \cdot)$ is large.
  - C2 and GRH implies $\mathsf{VP} \neq VNP$; it's not clear whether it implies PIT $\in \mathsf{P}$.

Circuit Normal Form (CNF) and Algebraic Complexity

An Important CNF

An Important CNF

- It was established in [VSBR83, Sap19] that an n-variate, degree d polynomial $f(\overline{x})$, computed by a circuit of size s, can be decomposed as

An Important CNF

- It was established in [VSBR83, Sap19] that an n-variate, degree d polynomial $f(\overline{x})$, computed by a circuit of size s, can be decomposed as

$$\boxed{f(\overline{x}) \;=\; \sum_{i=1}^{s'} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}}\;,$$

An Important CNF

- It was established in [VSBR83, Sap19] that an n-variate, degree d polynomial $f(\overline{x})$, computed by a circuit of size s, can be decomposed as

$$\boxed{f(\overline{x}) \;=\; \sum_{i=1}^{s'} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}}\,,$$

where

1. top-fanin $s' = \mathrm{poly}(s, d)$,

An Important CNF

- It was established in [VSBR83, Sap19] that an n-variate, degree d polynomial $f(\overline{x})$, computed by a circuit of size s, can be decomposed as

$$\boxed{f(\overline{x}) \;=\; \sum_{i=1}^{s'} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}} \,,$$

  where

  1. top-fanin $s' = \mathrm{poly}(s, d)$,
  2. where each f_{ij} has circuit size at most $\mathrm{poly}(s, d)$

An Important CNF

- It was established in [VSBR83, Sap19] that an n-variate, degree d polynomial $f(\overline{x})$, computed by a circuit of size s, can be decomposed as

$$\boxed{f(\overline{x}) \;=\; \sum_{i=1}^{s'} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}}\;,$$

  where

  1. top-fanin $s' = \mathrm{poly}(s, d)$,
  2. where each f_{ij} has circuit size at most $\mathrm{poly}(s, d)$
  3. $\deg(f_{ij}) \leq d/2$, for all i, j.

An Important CNF

- It was established in [VSBR83, Sap19] that an n-variate, degree d polynomial $f(\overline{x})$, computed by a circuit of size s, can be decomposed as

$$\boxed{f(\overline{x}) \;=\; \sum_{i=1}^{s'} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}}\;,$$

  where

  1. top-fanin $s' = \text{poly}(s, d)$,
  2. where each f_{ij} has circuit size at most $\text{poly}(s, d)$
  3. $\deg(f_{ij}) \leq d/2$, for all i, j.

- This circuit normal-form (CNF) has played a key role in all recent depth-reduction results [AV08, Koi12, GKKS13, Tav15].

CNF to sum of 25-product

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) = \sum_{i=1}^{\mathrm{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) \;=\; \sum_{i=1}^{\text{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

$\text{size}(f_{ij}) = \text{poly}(s, d)$ and $\deg(f_{ij}) \leq d/2$.

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) = \sum_{i=1}^{\mathrm{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

$\mathrm{size}(f_{ij}) = \mathrm{poly}(s, d)$ and $\deg(f_{ij}) \leq d/2$. Apply CNF to each of f_{ij} to get:

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) = \sum_{i=1}^{\text{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

size(f_{ij}) = poly(s, d) and deg$(f_{ij}) \le d/2$. Apply CNF to each of f_{ij} to get:

$$f(\overline{x}) = \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} f_{ij}$$

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) = \sum_{i=1}^{\text{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

$\text{size}(f_{ij}) = \text{poly}(s, d)$ and $\deg(f_{ij}) \leq d/2$. Apply CNF to each of f_{ij} to get:

$$\begin{aligned} f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} f_{ij} \\ &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} \left(\sum_{k=1}^{\text{poly}(s,d)} \prod_{l=1}^{5} f_{ijkl} \right) \end{aligned}$$

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) = \sum_{i=1}^{\text{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

$\text{size}(f_{ij}) = \text{poly}(s, d)$ and $\deg(f_{ij}) \leq d/2$. Apply CNF to each of f_{ij} to get:

$$\begin{aligned} f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} f_{ij} \\ &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} \left(\sum_{k=1}^{\text{poly}(s,d)} \prod_{l=1}^{5} f_{ijkl} \right) \\ &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{25} g_{ij} \end{aligned}$$

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) \;=\; \sum_{i=1}^{\mathrm{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

$\mathrm{size}(f_{ij}) = \mathrm{poly}(s,d)$ and $\deg(f_{ij}) \le d/2$. Apply CNF to each of f_{ij} to get:

$$\begin{aligned}
f(\overline{x}) &= \sum_{i=1}^{\mathrm{poly}(s,d)} \prod_{j=1}^{5} f_{ij} \\
&= \sum_{i=1}^{\mathrm{poly}(s,d)} \prod_{j=1}^{5} \left(\sum_{k=1}^{\mathrm{poly}(s,d)} \prod_{l=1}^{5} f_{ijkl} \right) \\
&= \sum_{i=1}^{\mathrm{poly}(s,d)} \prod_{j=1}^{25} g_{ij} \qquad \because \prod^{a} \sum^{b} \prod^{c} = \sum^{b^a} \prod^{a \cdot c}
\end{aligned}$$

CNF to sum of 25-product

Given d-degree $f(\overline{x})$, computed by size-s circuit, we decompose f as

$$f(\overline{x}) = \sum_{i=1}^{\text{poly}(s,d)} f_{i1} \cdot f_{i2} \cdot f_{i3} \cdot f_{i4} \cdot f_{i5}$$

$\text{size}(f_{ij}) = \text{poly}(s, d)$ and $\deg(f_{ij}) \leq d/2.$ Apply CNF to each of f_{ij} to get:

$$\begin{aligned} f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} f_{ij} \\ &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{5} \left(\sum_{k=1}^{\text{poly}(s,d)} \prod_{l=1}^{5} f_{ijkl} \right) \\ &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{25} g_{ij} \qquad \because \prod^{a} \sum^{b} \prod^{c} = \sum^{b^a} \prod^{a \cdot c} \end{aligned}$$

Note that $\deg(g_{ij}) \leq d/4$.

CNF to sum of 25^{th}-powers

CNF to sum of 25^{th}-powers

Fischer's Trick (Fischer94)

$\mathbb{F}$ be a field of characteristic 0 or $> m$. One can write $g = \prod_{i \in [m]} g_i$ as:

CNF to sum of 25^{th}-powers

Fischer's Trick (Fischer94)

$\mathbb{F}$ be a field of characteristic 0 or $> m$. One can write $g = \prod_{i \in [m]} g_i$ as:

$$g \; = \; g_1 \cdot g_2 \cdot \ldots g_m \; = \; \sum_{j=1}^{2^m} c_j \cdot h_j^m$$

where $c_j \in \mathbb{F}$ and $h_j \in \text{span}_{\mathbb{F}} \left(g_i \mid i \in [m] \right)$, for $j \in [2^m]$.

CNF to sum of 25^{th}-powers

Fischer's Trick (Fischer94)

$\mathbb{F}$ be a field of characteristic 0 or $> m$. One can write $g = \prod_{i \in [m]} g_i$ as:

$$g \; = \; g_1 \cdot g_2 \cdot \ldots g_m \; = \; \sum_{j=1}^{2^m} c_j \cdot h_j^m$$

where $c_j \in \mathbb{F}$ and $h_j \in \text{span}_{\mathbb{F}} \left(g_i \mid i \in [m] \right)$, for $j \in [2^m]$.

From previous slide, we expressed d-degree s-sized $f(\overline{x}) = \sum \prod g_{ij}$ with $\deg(g_{ij}) \leq d/4$.

CNF to sum of 25^{th}-powers

Fischer's Trick (Fischer94)

$\mathbb{F}$ be a field of characteristic 0 or $> m$. One can write $g = \prod_{i \in [m]} g_i$ as:

$$g \;=\; g_1 \cdot g_2 \cdot \ldots g_m \;=\; \sum_{j=1}^{2^m} c_j \cdot h_j^m$$

where $c_j \in \mathbb{F}$ and $h_j \in \mathrm{span}_{\mathbb{F}}\,(g_i \mid i \in [m])$, for $j \in [2^m]$.

From previous slide, we expressed d-degree s-sized $f(\overline{x}) = \sum \prod g_{ij}$ with $\deg(g_{ij}) \leq d/4$. Apply Fischer's trick on each $\prod_{j \in [25]} g_{ij}$ to get:

$$f(\overline{x}) \;=\; \sum_{i=1}^{\mathrm{poly}(s,d)} \prod_{j=1}^{25} g_{ij}$$

CNF to sum of 25^{th}-powers

Fischer's Trick (Fischer94)

$\mathbb{F}$ be a field of characteristic 0 or $> m$. One can write $g = \prod_{i \in [m]} g_i$ as:

$$g = g_1 \cdot g_2 \cdot \ldots g_m = \sum_{j=1}^{2^m} c_j \cdot h_j^m$$

where $c_j \in \mathbb{F}$ and $h_j \in \text{span}_{\mathbb{F}} (g_i \mid i \in [m])$, for $j \in [2^m]$.

From previous slide, we expressed d-degree s-sized $f(\overline{x}) = \sum \prod g_{ij}$ with $\deg(g_{ij}) \leq d/4$. Apply Fischer's trick on each $\prod_{j \in [25]} g_{ij}$ to get:

$$\begin{aligned} f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{25} g_{ij} \\ &= \sum_{i=1}^{\text{poly}(s,d)} c_i \cdot g_i^{25} \end{aligned}$$

CNF to sum of 25^{th}-powers

Fischer's Trick (Fischer94)

$\mathbb{F}$ be a field of characteristic 0 or $> m$. One can write $g = \prod_{i \in [m]} g_i$ as:

$$g \;=\; g_1 \cdot g_2 \cdot \ldots g_m \;=\; \sum_{j=1}^{2^m} c_j \cdot h_j^m$$

where $c_j \in \mathbb{F}$ and $h_j \in \operatorname{span}_{\mathbb{F}} (g_i \mid i \in [m])$, for $j \in [2^m]$.

From previous slide, we expressed d-degree s-sized $f(\overline{x}) = \sum \prod g_{ij}$ with $\deg(g_{ij}) \leq d/4$. Apply Fischer's trick on each $\prod_{j \in [25]} g_{ij}$ to get:

$$\begin{aligned} f(\overline{x}) \;&=\; \sum_{i=1}^{\text{poly}(s,d)} \prod_{j=1}^{25} g_{ij} \\ &=\; \sum_{i=1}^{\text{poly}(s,d)} c_i \cdot g_i^{25} \qquad\qquad \text{where } \deg(g_i) \leq d/4. \end{aligned}$$

m^{th} power to sum of r^{th}-power

m^{th} power to sum of r^{th}-power

Sum-Identity Lemma (DST20)

Let $\mathbb{F}$ be a field of characteristic 0 or large. Let $h(\overline{x}) \in \mathbb{F}[\overline{x}]$ and $0 \leq m \leq r$. There exist $c_{m,i} \in \mathbb{F}$ and *distinct* $\lambda_i \in \mathbb{F}$, for $0 \leq i \leq r$, such that

$$h(\overline{x})^m \;=\; \sum_{i=0}^{r} c_{m,i} \left(h(\overline{x}) + \lambda_i\right)^r .$$

m^{th} power to sum of r^{th}-power

Sum-Identity Lemma (DST20)

Let $\mathbb{F}$ be a field of characteristic 0 or large. Let $h(\overline{x}) \in \mathbb{F}[\overline{x}]$ and $0 \le m \le r$. There exist $c_{m,i} \in \mathbb{F}$ and *distinct* $\lambda_i \in \mathbb{F}$, for $0 \le i \le r$, such that

$$h(\overline{x})^m \;=\; \sum_{i=0}^{r} c_{m,i} \left(h(\overline{x}) + \lambda_i\right)^r .$$

Proof Sketch.

m^{th} power to sum of r^{th}-power

Sum-Identity Lemma (DST20)

Let $\mathbb{F}$ be a field of characteristic 0 or large. Let $h(\overline{x}) \in \mathbb{F}[\overline{x}]$ and $0 \leq m \leq r$. There exist $c_{m,i} \in \mathbb{F}$ and *distinct* $\lambda_i \in \mathbb{F}$, for $0 \leq i \leq r$, such that

$$h(\overline{x})^m \ = \ \sum_{i=0}^{r} c_{m,i} \left(h(\overline{x}) + \lambda_i\right)^r .$$

Proof Sketch.

Consider $(h(\overline{x}) + t)^r = \sum_{i=0}^{r} \binom{r}{i} h^i \cdot t^{r-i}$.

m^{th} power to sum of r^{th}-power

Sum-Identity Lemma (DST20)

Let $\mathbb{F}$ be a field of characteristic 0 or large. Let $h(\overline{x}) \in \mathbb{F}[\overline{x}]$ and $0 \leq m \leq r$. There exist $c_{m,i} \in \mathbb{F}$ and *distinct* $\lambda_i \in \mathbb{F}$, for $0 \leq i \leq r$, such that

$$h(\overline{x})^m \;=\; \sum_{i=0}^{r} c_{m,i} \left(h(\overline{x}) + \lambda_i\right)^r .$$

Proof Sketch.

Consider $(h(\overline{x}) + t)^r = \sum_{i=0}^{r} \binom{r}{i} h^i \cdot t^{r-i}$. As $m \leq r$, one of the h^i must be h^m.

m^{th} power to sum of r^{th}-power

Sum-Identity Lemma (DST20)

Let $\mathbb{F}$ be a field of characteristic 0 or large. Let $h(\overline{x}) \in \mathbb{F}[\overline{x}]$ and $0 \le m \le r$. There exist $c_{m,i} \in \mathbb{F}$ and *distinct* $\lambda_i \in \mathbb{F}$, for $0 \le i \le r$, such that

$$h(\overline{x})^m \; = \; \sum_{i=0}^{r} c_{m,i} \left(h(\overline{x}) + \lambda_i\right)^r .$$

Proof Sketch.

Consider $(h(\overline{x}) + t)^r = \sum_{i=0}^{r} \binom{r}{i} h^i \cdot t^{r-i}$. As $m \le r$, one of the h^i must be h^m. Interpolate at $t = \lambda_i$ for $0 \le i \le r$ ($r+1$-many distinct points).

m^{th} power to sum of r^{th}-power

Sum-Identity Lemma (DST20)

Let $\mathbb{F}$ be a field of characteristic 0 or large. Let $h(\overline{x}) \in \mathbb{F}[\overline{x}]$ and $0 \le m \le r$. There exist $c_{m,i} \in \mathbb{F}$ and *distinct* $\lambda_i \in \mathbb{F}$, for $0 \le i \le r$, such that

$$h(\overline{x})^m \;=\; \sum_{i=0}^{r} c_{m,i}\,(h(\overline{x}) + \lambda_i)^r\,.$$

Proof Sketch.

Consider $(h(\overline{x}) + t)^r = \sum_{i=0}^{r} \binom{r}{i} h^i \cdot t^{r-i}$. As $m \le r$, one of the h^i must be h^m. Interpolate at $t = \lambda_i$ for $0 \le i \le r$ ($r+1$-many distinct points).

$$\begin{bmatrix} \binom{r}{0}\lambda_0^r & \binom{r}{1}\lambda_0^{r-1} & \dots & \binom{r}{r}\lambda_0^0 \\ \binom{r}{0}\lambda_1^r & \binom{r}{1}\lambda_1^{r-1} & \dots & \binom{r}{r}\lambda_1^0 \\ \vdots & \vdots & \vdots & \vdots \\ \binom{r}{0}\lambda_r^r & \binom{r}{1}\lambda_r^{r-1} & \dots & \binom{r}{r}\lambda_r^0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ h \\ \vdots \\ h^r \end{bmatrix} = \begin{bmatrix} (h(\overline{x}) + \lambda_0)^r \\ (h(\overline{x}) + \lambda_1)^r \\ \vdots \\ (h(\overline{x}) + \lambda_r)^r \end{bmatrix}$$

$\square$

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\overline{x})$ computed by size-s circuit can be written as poly(s, d)-many sum of 25^{th}-powers of degree at most $d/4$.

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\overline{x})$ computed by size-s circuit can be written as poly(s, d)-many sum of 25^{th}-powers of degree at most $d/4$. Using the Sum-Identity lemma, for $r \geq 25$, we get:

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\overline{x})$ computed by size-s circuit can be written as poly(s, d)-many sum of 25^{th}-powers of degree at most $d/4$. Using the Sum-Identity lemma, for $r \geq 25$, we get:

$$f(\overline{x}) \;=\; \sum_{i=1}^{\text{poly}(s,d)} c_i \cdot g_i^{25}$$

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\overline{x})$ computed by size-s circuit can be written as poly(s,d)-many sum of 25^{th}-powers of degree at most $d/4$. Using the Sum-Identity lemma, for $r \geq 25$, we get:

$$\begin{aligned} f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} c_i \cdot g_i^{25} \\ &= \sum_{i=1}^{\text{poly}(s,d)} \left(\sum_{j=0}^{r} c_{ij} \cdot \left(g_i + \lambda_j\right)^r \right) \end{aligned}$$

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\bar{x})$ computed by size-s circuit can be written as poly(s, d)-many sum of 25^{th}-powers of degree at most $d/4$. Using the Sum-Identity lemma, for $r \geq 25$, we get:

$$\begin{aligned} f(\bar{x}) &= \sum_{i=1}^{\mathrm{poly}(s,d)} c_i \cdot g_i^{25} \\ &= \sum_{i=1}^{\mathrm{poly}(s,d)} \left(\sum_{j=0}^{r} c_{ij} \cdot (g_i + \lambda_j)^r \right) \\ &= \sum_{i=1}^{(r+1)\cdot \mathrm{poly}(s,d)} c_i' \cdot \tilde{g}_i^r \end{aligned}$$

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\overline{x})$ computed by size-s circuit can be written as poly(s, d)-many sum of 25^{th}-powers of degree at most $d/4$. Using the Sum-Identity lemma, for $r \geq 25$, we get:

$$
\begin{aligned}
f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} c_i \cdot g_i^{25} \\
&= \sum_{i=1}^{\text{poly}(s,d)} \left(\sum_{j=0}^{r} c_{ij} \cdot (g_i + \lambda_j)^r \right) \\
&= \sum_{i=1}^{(r+1)\cdot\text{poly}(s,d)} c_i' \cdot \tilde{g}_i^r \qquad \text{where } \deg(\tilde{g}_i) \leq d/4 \text{ and } c_i' \in \mathbb{F}
\end{aligned}
$$

CNF to sum of constant r^{th}-power

We have already established that n-variate, d-degree $f(\overline{x})$ computed by size-s circuit can be written as poly(s,d)-many sum of 25^{th}-powers of degree at most $d/4$. Using the Sum-Identity lemma, for $r \geq 25$, we get:

$$\begin{aligned}
f(\overline{x}) &= \sum_{i=1}^{\text{poly}(s,d)} c_i \cdot g_i^{25} \\
&= \sum_{i=1}^{\text{poly}(s,d)} \left(\sum_{j=0}^{r} c_{ij} \cdot \left(g_i + \lambda_j\right)^r \right) \\
&= \sum_{i=1}^{(r+1)\cdot\text{poly}(s,d)} c_i' \cdot \tilde{g}_i^r \qquad \text{where } \deg(\tilde{g}_i) \leq d/4 \text{ and } c_i' \in \mathbb{F} \\
&\in \sum^{\text{poly}(s,d)} \bigwedge^{r} \sum \prod^{d/4} .
\end{aligned}$$

Proof Idea of Main Theorems

Proof of Theorem 1: Conjecture C1 to PIT

Proof of Theorem 1: Conjecture C1 to PIT

- Assume C1 holds i.e. for $f_d := (x+1)^d$, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \geq d/r^{\delta_2}$.

Proof of Theorem 1: Conjecture C1 to PIT

- Assume C1 holds i.e. for $f_d := (x+1)^d$, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \geq d/r^{\delta_2}$.
- Idea: use C1 to prove that a *fixed* constant k-variate $O(n)$-degree hard polynomial family $(P_{k,n})_n$ exists i.e. size$(P_{k,n}) = n^{\Omega(1)}$.

Proof of Theorem 1: Conjecture C1 to PIT

- Assume C1 holds i.e. for $f_d := (x+1)^d$, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \geq d/r^{\delta_2}$.
- Idea: use C1 to prove that a *fixed* constant k-variate $O(n)$-degree hard polynomial family $(P_{k,n})_n$ exists i.e. $\text{size}(P_{k,n}) = n^{\Omega(1)}$.
  - Use f_d to construct a k-variate $O(n)$ degree polynomial $P_{k,n}$ ($d := d(n)$).

Proof of Theorem 1: Conjecture C1 to PIT

- Assume C1 holds i.e. for $f_d := (x+1)^d$, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) \geq d/r^{\delta_2}$.
- Idea: use C1 to prove that a *fixed* constant k-variate $O(n)$-degree hard polynomial family $(P_{k,n})_n$ exists i.e. $\text{size}(P_{k,n}) = n^{\Omega(1)}$.
  - Use f_d to construct a k-variate $O(n)$ degree polynomial $P_{k,n}$ ($d := d(n)$).
- Use GKSS19: constant k-variate ($k \geq 4$) explicit hard polynomial implies blackbox-PIT $\in \mathsf{P}$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k .

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k $(k \geq \max(17(\delta_2 + 1), 19r/\delta_1))$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.
- Apply *inverse Kronecker substitution* on f_d to construct $P_{k,n}$:

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.

- Apply *inverse Kronecker substitution* on f_d to construct $P_{k,n}$:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.

- Apply *inverse Kronecker substitution* on f_d to construct $P_{k,n}$:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

  $P_{k,n}$ is a k-variate polynomial with individual degree at most n. Thus, it is a bijection between $\mathrm{supp}(P_{k,n})$ and $\mathrm{supp}(f_d)$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.

- Apply *inverse Kronecker substitution* on f_d to construct $P_{k,n}$:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

  $P_{k,n}$ is a k-variate polynomial with individual degree at most n. Thus, it is a bijection between $\mathrm{supp}(P_{k,n})$ and $\mathrm{supp}(f_d)$.

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(n)$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.

- Apply *inverse Kronecker substitution* on f_d to construct $P_{k,n}$:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

  $P_{k,n}$ is a k-variate polynomial with individual degree at most n. Thus, it is a bijection between $\mathrm{supp}(P_{k,n})$ and $\mathrm{supp}(f_d)$.

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(n)$.

- **Claim:** $\mathrm{size}(P_{k,n}) = \left(\deg(P_{k,n})\right)^{\Omega(1)} = d^{\Omega(1)}$.

Conjecture C1 to constant k-variate hard polynomial

- Fix a *large* k . For *every* $n \in \mathbb{N}$, choose the *largest* $d := d(n)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Observe: $d = \Omega((n+1)^k)$.

- Apply *inverse Kronecker substitution* on f_d to construct $P_{k,n}$:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

  $P_{k,n}$ is a k-variate polynomial with individual degree at most n. Thus, it is a bijection between $\mathrm{supp}(P_{k,n})$ and $\mathrm{supp}(f_d)$.

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(n)$.

- **Claim:** $\mathrm{size}(P_{k,n}) = \left(\deg(P_{k,n})\right)^{\Omega(1)} = d^{\Omega(1)}$. Proof by contradiction: If $P_{k,n}$ is *not* hard, then C1 doesn't hold for *infinitely* many $d \in I_r$.

Proof of hardness of $P_{k,n}$

Proof of hardness of $P_{k,n}$

- Suppose, size$(P_{k,n}) \leq d^{1/\mu}$ (μ, depending on r, δ_1, δ_2, fixed later).

Proof of hardness of $P_{k,n}$

- Suppose, size$(P_{k,n}) \leq d^{1/\mu}$ (μ, depending on r, δ_1, δ_2, fixed later).

- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} = \sum_{i=1}^{\mathrm{poly}(d^{1/\mu}, kn)} c_i' \cdot \tilde{g}_i^r$$

where $\deg(\tilde{g}_i) \leq kn/4$.

Proof of hardness of $P_{k,n}$

- Suppose, size$(P_{k,n}) \leq d^{1/\mu}$ (μ, depending on r, δ_1, δ_2, fixed later).

- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} = \sum_{i=1}^{\mathrm{poly}(d^{1/\mu}, kn)} c_i' \cdot \tilde{g}_i^r$$

  where $\deg(\tilde{g}_i) \leq kn/4$.

- Direct counting argument shows: $\left|\bigcup_i \mathrm{supp}(\tilde{g}_i)\right| \leq \binom{k+kn/4}{k}$.

Proof of hardness of $P_{k,n}$

- Suppose, $\text{size}(P_{k,n}) \leq d^{1/\mu}$ (μ, depending on r, δ_1, δ_2, fixed later).

- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} = \sum_{i=1}^{\text{poly}(d^{1/\mu}, kn)} c_i' \cdot \tilde{g}_i^r$$

where $\deg(\tilde{g}_i) \leq kn/4$.

- Direct counting argument shows: $\left|\bigcup_i \text{supp}(\tilde{g}_i)\right| \leq \binom{k+kn/4}{k}$.

- Let ϕ be the Kronecker map $\phi : x_i \mapsto x^{(n+1)^{i-1}}$ for $i \in [k]$. Then,

$$f_d = \phi(P_{k,n}) = \sum_{i=1}^{\text{poly}(d^{1/\mu}, kn)} c_i' \cdot \phi(\tilde{g}_i)^r$$

Proof of hardness of $P_{k,n}$

- Suppose, $\mathrm{size}(P_{k,n}) \le d^{1/\mu}$ (μ, depending on r, δ_1, δ_2, fixed later).
- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} \;=\; \sum_{i=1}^{\mathrm{poly}(d^{1/\mu},kn)} c_i' \cdot \tilde{g}_i^r$$

  where $\deg(\tilde{g}_i) \le kn/4$.

- Direct counting argument shows: $\left|\bigcup_i \mathrm{supp}(\tilde{g}_i)\right| \le \binom{k+kn/4}{k}$.
- Let ϕ be the Kronecker map $\phi : x_i \mapsto x^{(n+1)^{i-1}}$ for $i \in [k]$. Then,

$$f_d \;=\; \phi(P_{k,n}) \;=\; \sum_{i=1}^{\mathrm{poly}(d^{1/\mu},kn)} c_i' \cdot \phi(\tilde{g}_i)^r$$

- ϕ *cannot* increase the union-support or the top fan-in.

Finishing Theorem 1

- f_d has sum of r-th power representation with top fan-in $s_0 := \mathrm{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.

Finishing Theorem 1

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.

Finishing Theorem 1

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.

Finishing Theorem 1

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.
- This means, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) < d/r^{\delta_2}$ for infinitely many $d \in I_r$, a contradiction!

Finishing Theorem 1

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.
- This means, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) < d/r^{\delta_2}$ for infinitely many $d \in I_r$, a contradiction!
- $P_{k,n}$ is hard $\implies$ PIT $\in \mathsf{P}$ (using GKSS19).

Finishing Theorem 1

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.
- This means, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) < d/r^{\delta_2}$ for infinitely many $d \in I_r$, a contradiction!
- $P_{k,n}$ is hard $\implies$ PIT $\in \mathsf{P}$ (using GKSS19).
- Instead of 25-CNF, we could have used 5-CNF, then $s_1 := \binom{k+kn/2}{k}$ which is $> d$. Thus, $r \geq 25$ is *required*!

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n.

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$.

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Thus, $d = \Omega((n+1)^k) = 2^{\Omega(k)}$.

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Thus, $d = \Omega((n+1)^k) = 2^{\Omega(k)}$.

- From f_d construct $P_{k,n}$, a k-variate, n-individual degree polynomial:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Thus, $d = \Omega((n+1)^k) = 2^{\Omega(k)}$.

- From f_d construct $P_{k,n}$, a k-variate, n-individual degree polynomial:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(k)$.

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Thus, $d = \Omega((n+1)^k) = 2^{\Omega(k)}$.

- From f_d construct $P_{k,n}$, a k-variate, n-individual degree polynomial:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(k)$.

- We will show that Conjecture C1 implies $\mathrm{size}(P_{k,n}) \geq d^{\Omega(1)} = 2^{\Omega(k)} = 2^{\Omega\left(\deg(P_{k,n})\right)} \implies \{P_{k,n}\}_k \notin \mathsf{VP}$.

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Thus, $d = \Omega((n+1)^k) = 2^{\Omega(k)}$.

- From f_d construct $P_{k,n}$, a k-variate, n-individual degree polynomial:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(k)$.

- We will show that Conjecture C1 implies $\text{size}(P_{k,n}) \geq d^{\Omega(1)} = 2^{\Omega(k)} = 2^{\Omega(\deg(P_{k,n}))} \implies \{P_{k,n}\}_k \notin \mathsf{VP}$.

- Assume GRH and $\mathsf{VP} = \mathsf{VNP}$, we will show that $\{P_{k,n}\}_k \in \mathsf{VP}$.

Proof of Theorem 2: Conjecture C1 to $\mathsf{VP} \neq \mathsf{VNP}$

- Fix a *large constant* n. For *every* $k \in \mathbb{N}$, choose the *largest* $d := d(k)$ which is $\leq (n+1)^k - 1$ and $d \in I_r$. Thus, $d = \Omega((n+1)^k) = 2^{\Omega(k)}$.

- From f_d construct $P_{k,n}$, a k-variate, n-individual degree polynomial:

$$P_{k,n}(x_1, \ldots, x_k) \mapsto P_{k,n}\left(x^{(n+1)^0}, \ldots, x^{(n+1)^{k-1}}\right) = f_d(x),$$

- Note that: $\deg(P_{k,n}) \leq k \cdot n = O(k)$.

- We will show that Conjecture C1 implies $\text{size}(P_{k,n}) \geq d^{\Omega(1)} = 2^{\Omega(k)} = 2^{\Omega\left(\deg(P_{k,n})\right)} \implies \{P_{k,n}\}_k \notin \mathsf{VP}$.

- Assume GRH and $\mathsf{VP} = \mathsf{VNP}$, we will show that $\{P_{k,n}\}_k \in \mathsf{VP}$.

- Thus, GRH and Conjecture C1 $\implies \mathsf{VP} \neq \mathsf{VNP}$.

GRH and $\mathsf{VP} = \mathsf{VNP} \implies \{P_{k,n}\}_k \in \mathsf{VP}$

GRH and $\mathsf{VP} = \mathsf{VNP} \implies \{P_{k,n}\}_k \in \mathsf{VP}$

- One can write $P_{k,n}(\overline{x})$ as

$$P_{k,n}(\overline{x}) = \sum_{\overline{e}\in[0,c]^k} \binom{d}{e} \cdot \overline{x}^{\overline{\boldsymbol{e}}}$$

GRH and VP = VNP $\implies \{P_{k,n}\}_k \in$ VP

- One can write $P_{k,n}(\overline{x})$ as

$$P_{k,n}(\overline{x}) \;=\; \sum_{\overline{e} \in [0,c]^k} \binom{d}{e} \cdot \overline{x}^{\overline{e}}$$

- $\binom{d}{e}$ are computable in complexity class CH (Counting Hierarchy).

GRH and VP = VNP $\implies \{P_{k,n}\}_k \in \mathsf{VP}$

- One can write $P_{k,n}(\overline{x})$ as

$$P_{k,n}(\overline{x}) = \sum_{\overline{e} \in [0,c]^k} \binom{d}{e} \cdot \overline{x}^{\overline{e}}$$

- $\binom{d}{e}$ are computable in complexity class CH (Counting Hierarchy).
- Bürgisser proved (in 2000) that if $\mathsf{VP} = \mathsf{VNP}$ and GRH, then CH = $\mathsf{P}/$poly. This means, $\binom{d}{e}$ are computable in $\mathsf{P}/$poly.

GRH and $\mathsf{VP} = \mathsf{VNP} \implies \{P_{k,n}\}_k \in \mathsf{VP}$

- One can write $P_{k,n}(\overline{x})$ as

$$P_{k,n}(\overline{x}) = \sum_{\overline{e}\in[0,c]^k} \binom{d}{e} \cdot \overline{x}^{\overline{e}}$$

- $\binom{d}{e}$ are computable in complexity class CH (Counting Hierarchy).
- Bürgisser proved (in 2000) that if $\mathsf{VP} = \mathsf{VNP}$ and GRH, then CH = P/poly. This means, $\binom{d}{e}$ are computable in P/poly.
- Using Valiant's Criterion, $\{P_{k,n}\}_k \in \mathsf{VNP} = \mathsf{VP}$.

From C1 to $\{P_{k,n}\}_k \notin \mathsf{VP}$

From C1 to $\{P_{k,n}\}_k \notin \mathsf{VP}$

- Assume size$(P_{k,n}) \leq d^{1/\mu}$; where μ depends on r, δ_1, δ_2, fixed later.

From C1 to $\{P_{k,n}\}_k \notin \mathsf{VP}$

- Assume $\text{size}(P_{k,n}) \leq d^{1/\mu}$; where μ depends on r, δ_1, δ_2, fixed later.
- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} = \sum_{i=1}^{\text{poly}(d^{1/\mu}, kn)} c_i' \cdot \tilde{g}_i^r$$

where $\deg(\tilde{g}_i) \leq kn/4$.

From C1 to $\{P_{k,n}\}_k \notin \mathsf{VP}$

- Assume size$(P_{k,n}) \leq d^{1/\mu}$; where μ depends on r, δ_1, δ_2, fixed later.
- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} \;=\; \sum_{i=1}^{\mathrm{poly}(d^{1/\mu},kn)} c_i' \cdot \tilde{g}_i^r$$

  where $\deg(\tilde{g}_i) \leq kn/4$.
- Direct counting argument shows: $\left|\bigcup_i \mathrm{supp}(\tilde{g}_i)\right| \leq \binom{k+kn/4}{k}$.

From C1 to $\{P_{k,n}\}_k \notin \mathsf{VP}$

- Assume $\text{size}(P_{k,n}) \leq d^{1/\mu}$; where μ depends on r, δ_1, δ_2, fixed later.
- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} \; = \; \sum_{i=1}^{\text{poly}(d^{1/\mu},kn)} c_i' \cdot \tilde{g}_i^r$$

  where $\deg(\tilde{g}_i) \leq kn/4$.
- Direct counting argument shows: $\left|\bigcup_i \text{supp}(\tilde{g}_i)\right| \leq \binom{k+kn/4}{k}$.
- Let ϕ be the Kronecker map $\phi \, : \, x_i \, \mapsto \, x^{(n+1)^{i-1}}$ for $i \in [k]$. Then,

$$f_d \; = \; \phi(P_{k,n}) \; = \; \sum_{i=1}^{\text{poly}(d^{1/\mu},kn)} c_i' \cdot \phi(\tilde{g}_i)^r$$

From C1 to $\{P_{k,n}\}_k \notin \mathsf{VP}$

- Assume size$(P_{k,n}) \leq d^{1/\mu}$; where μ depends on r, δ_1, δ_2, fixed later.
- We know, using the *derived* CNF, $P_{k,n}$ can be written as

$$P_{k,n} \;=\; \sum_{i=1}^{\text{poly}(d^{1/\mu},kn)} c_i' \cdot \tilde{g}_i^r$$

  where $\deg(\tilde{g}_i) \leq kn/4$.

- Direct counting argument shows: $\left|\bigcup_i \text{supp}(\tilde{g}_i)\right| \leq \binom{k+kn/4}{k}$.
- Let ϕ be the Kronecker map $\phi \,:\, x_i \,\mapsto\, x^{(n+1)^{i-1}}$ for $i \in [k]$. Then,

$$f_d \;=\; \phi(P_{k,n}) \;=\; \sum_{i=1}^{\text{poly}(d^{1/\mu},kn)} c_i' \cdot \phi(\tilde{g}_i)^r$$

- ϕ *cannot* increase the union-support or the top fan-in.

Finishing Theorem 2

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.

Finishing Theorem 2

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.

Finishing Theorem 2

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.

Finishing Theorem 2

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.
- This means, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) < d/r^{\delta_2}$ for infinitely many $d \in I_r$, a contradiction!

Finishing Theorem 2

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.
- This means, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) < d/r^{\delta_2}$ for infinitely many $d \in I_r$, a contradiction!
- $P_{k,n}$ is exponentially hard i.e. $\text{size}(P_{k,n}) \geq d^{1/\mu} = 2^{\Omega(n)}$. Thus, it cannot be in VP.

Finishing Theorem 2

- f_d has sum of r-th power representation with top fan-in $s_0 := \text{poly}(d^{1/\mu}, kn)$ and support-union at most $s_1 := \binom{k+kn/4}{k}$.
- This means, in notation: $U_{\mathbb{F}}(f_d, r, s_0) \leq s_1$.
- Choose μ appropriately so that $s_0 \leq d^{\delta_1}$ and $s_1 < d/r^{\delta_2}$.
- This means, $U_{\mathbb{F}}(f_d, r, d^{\delta_1}) < d/r^{\delta_2}$ for infinitely many $d \in I_r$, a contradiction!
- $P_{k,n}$ is exponentially hard i.e. $\text{size}(P_{k,n}) \geq d^{1/\mu} = 2^{\Omega(n)}$. Thus, it cannot be in VP.
- Instead of 25-CNF, we could have used 5-CNF, then $s_1 := \binom{k+kn/2}{k}$ which is $> d$. Thus, $r \geq 25$ is *required*!

Conclusion

Conclusion

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*.

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$?

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?
- Can we improve the exponent 25?

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?
- Can we improve the exponent 25? Very recently, Dutta and Saxena *improved* 25 to 4.

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?
- Can we improve the exponent 25? Very recently, Dutta and Saxena *improved* 25 to 4. Can we improve further to 3 (or 2)?

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?
- Can we improve the exponent 25? Very recently, Dutta and Saxena *improved* 25 to 4. Can we improve further to 3 (or 2)?
- Can we remove GRH for $(x+1)^d$?

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?
- Can we improve the exponent 25? Very recently, Dutta and Saxena *improved* 25 to 4. Can we improve further to 3 (or 2)?
- Can we remove GRH for $(x + 1)^d$?
- Be *ambitious*. Prove Conjecture C1!

Conclusion

- We showed that for $r = 2$, Conjecture C1 implies *matrix rigidity*. Could we solve the conjecture for special cases like *constant* some of powers?
- Is C1 true for random f over $\mathbb{Q}$? over $\mathbb{C}$?
- Can we improve the exponent 25? Very recently, Dutta and Saxena *improved* 25 to 4. Can we improve further to 3 (or 2)?
- Can we remove GRH for $(x+1)^d$?
- Be *ambitious*. Prove Conjecture C1!

#StaySafe 😄