

Near-optimal Bootstrapping of Hitting Sets

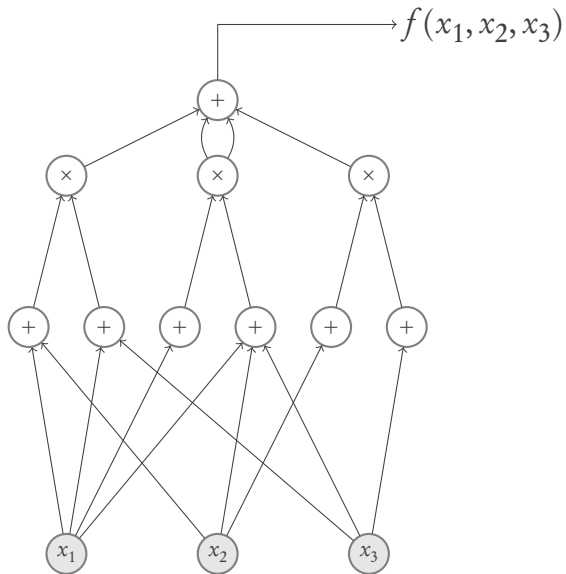
Mrinal Kumar
Simons Institute

Ramprasad Satharishi
TIFR, Mumbai

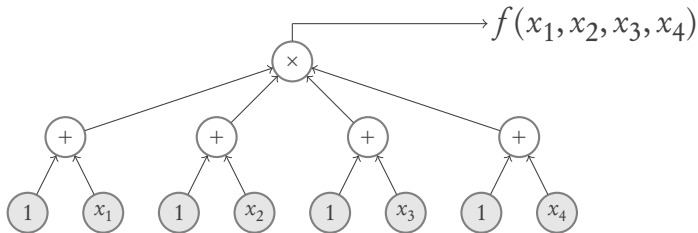
Anamay Tengse
TIFR, Mumbai

Simons Institute
December 2018

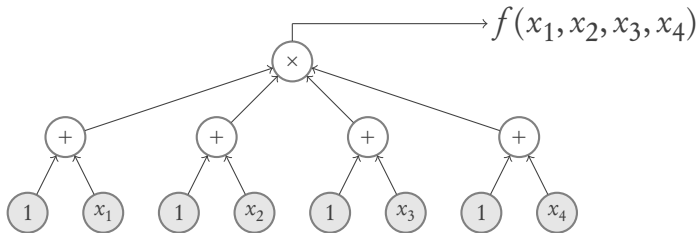
Algebraic Circuits



Algebraic Formulas

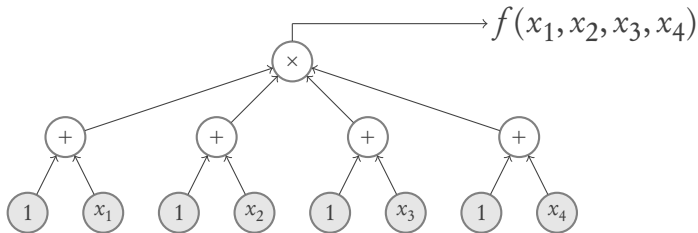


Algebraic Formulas



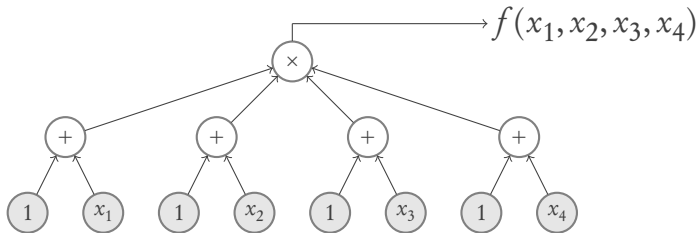
- A tree, made up of $+$ and \times gates. Leaves containing variables or constants

Algebraic Formulas



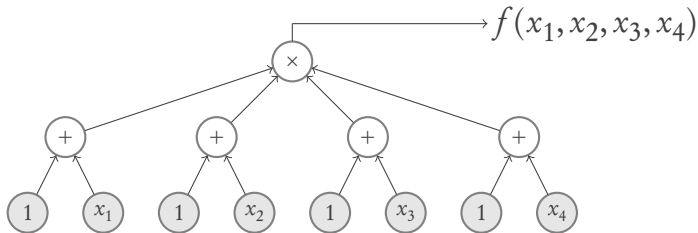
- A tree, made up of $+$ and \times gates. Leaves containing variables or constants. Size = number of leaves

Algebraic Formulas



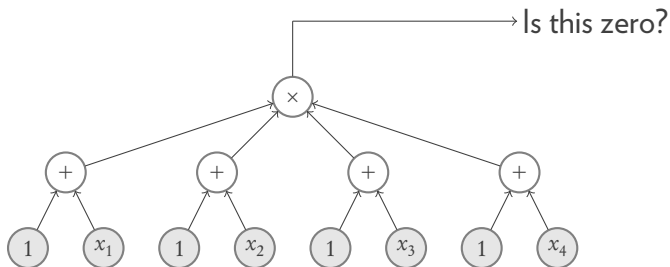
- ▶ A tree, made up of $+$ and \times gates. Leaves containing variables or constants. Size = number of leaves
- ▶ $\text{Size}(f(g_1, \dots, g_n)) \leq \text{Size}(f) \cdot \max_i (\text{Size}(g_i))$

Algebraic Formulas



- ▶ A tree, made up of $+$ and \times gates. Leaves containing variables or constants. Size = number of leaves
- ▶ $\text{Size}(f(g_1, \dots, g_n)) \leq \text{Size}(f) \cdot \max_i (\text{Size}(g_i))$
- ▶ $\text{Formula}(n, d, s)$: n -variate, degree $\leq d$ polynomials computable by size s formulas. (note: $d \leq s$)

Polynomial Identity Testing



Blackbox Polynomial Identity Testing

→ Is this zero?

This box contains a polynomial from $\mathcal{C}(n, d, s)$

Blackbox Polynomial Identity Testing

→ Is this zero?

This box contains a polynomial from $\mathcal{C}(n, d, s)$

Only have evaluation access to the circuit.

Blackbox Polynomial Identity Testing

→ Is this zero?

This box contains a polynomial from $\mathcal{C}(n, d, s)$

Only have evaluation access to the circuit.

Equivalent to constructing a **hitting set** H :

For every nonzero $P \in \mathcal{C}(n, d, s)$, there is some $\bar{a} \in H$ such that $P(\bar{a}) \neq 0$.

Hitting Sets



Hitting Sets

Counting argument

There are **non-explicit** hitting sets of $\text{poly}(s)$ size for $\mathcal{C}(n, d, s)$.

Hitting Sets

Counting argument

There are **non-explicit** hitting sets of $\text{poly}(s)$ size for $\mathcal{C}(n, d, s)$.

Lemma ([Ore*, DeMillo-Lipton, Schwartz-Zippel])

If $S \subseteq \mathbb{F}$ with $|S| \geq d + 1$, then S^n is a hitting set for $\mathcal{C}(n, d, s)$.

That is, we have an explicit, but trivial, hitting set of $(d + 1)^n$ size.

Hitting Sets

Counting argument

There are **non-explicit** hitting sets of $\text{poly}(s)$ size for $\mathcal{C}(n, d, s)$.

Lemma ([Ore*, DeMillo-Lipton, Schwartz-Zippel])

If $S \subseteq \mathbb{F}$ with $|S| \geq d + 1$, then S^n is a hitting set for $\mathcal{C}(n, d, s)$.

That is, we have an explicit, but trivial, hitting set of $(d + 1)^n$ size.

Question: Are there small **explicit** hitting sets for $\mathcal{C}(n, d, s)$?

Improving not-too-bad hitting sets

Theorem ([Agrawal-Ghosh-Saxena 2018])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\text{Circuits}(n, s, s)$ of size at most

$$(s + 1)^{n^{0.49}}.$$

(Trivial hitting set size: $(s + 1)^n$)

Improving not-too-bad hitting sets

Theorem ([Agrawal-Ghosh-Saxena 2018])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\text{Circuits}(n, s, s)$ of size at most

$$(s + 1)^{n^{0.49}}.$$

(Trivial hitting set size: $(s + 1)^n$)

Then there is an explicit hitting set for $\text{Circuits}(s, s, s)$ of size at most

$$s^{\text{tiny}(s)}.$$

Improving not-too-bad hitting sets

Theorem ([Agrawal-Ghosh-Saxena 2018])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\text{Circuits}(n, s, s)$ of size at most

$$(s + 1)^{n^{0.49}}.$$

(Trivial hitting set size: $(s + 1)^n$)

Then there is an explicit hitting set for $\text{Circuits}(s, s, s)$ of size at most

$$s^{\exp(\exp(O(\log^* s)))}.$$

Improving not-too-bad hitting sets

Theorem ([Agrawal-Ghosh-Saxena 2018])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\text{Circuits}(n, s, s)$ of size at most

$$(s + 1)^{n^{0.49}}.$$

(Trivial hitting set size: $(s + 1)^n$)

Then there is an explicit hitting set for $\text{Circuits}(s, s, s)$ of size at most

$$s^{\text{tiny}(s)}.$$

Improving almost-trivial hitting sets

Theorem ([Kumar-S-Tengse])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\text{Circuits}(n, s, s)$ of size at most

$$(s + 1)^{n-0.01}.$$

(Trivial hitting set size: $(s + 1)^n$)

Then there is an explicit hitting set for $\text{Circuits}(s, s, s)$ of size at most

$$s^{\text{tiny}(s)}.$$

Improving almost-trivial hitting sets

Theorem ([Kumar-S-Tengse])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$(s + 1)^{n-0.01}.$$

(Trivial hitting set size: $(s + 1)^n$)

Then there is an explicit hitting set for $\text{Formula}(s, s, s)$ of size at most

$$s^{\text{tiny}(s)}.$$

Improving almost-trivial hitting sets

Theorem ([Kumar-S-Tengse])

Say n large enough.

Suppose, for each $s \geq n$, there is an explicit hitting set for $\mathcal{C}(n, s, s)$ of size at most

$$(s + 1)^{n-0.01}.$$

(Trivial hitting set size: $(s + 1)^n$)

Then there is an explicit hitting set for $\mathcal{C}(s, s, s)$ of size at most

$$s^{\text{tiny}(s)}.$$

(where \mathcal{C} is any class well-behaved under sums, projections and compositions)

A very high-level overview

Non-trivial Hitting Sets

Explicit Lower Bounds

A *very* high-level overview

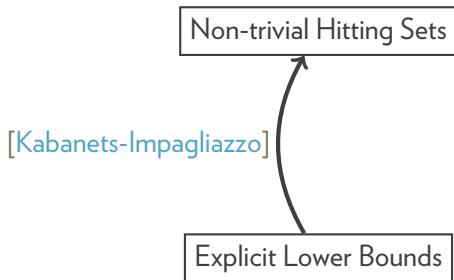
Non-trivial Hitting Sets

[Heintz-Schnorr, Agrawal]

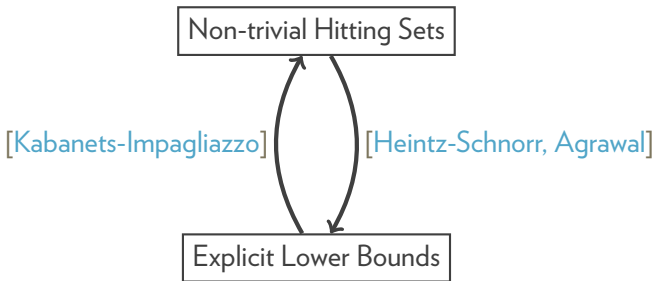
Explicit Lower Bounds



A *very* high-level overview



A *very* high-level overview



From a non-trivial hitting set, get a lower bound. Use that to get a *better* hitting set. And so on ...

Preliminaries:

Hardness vs Randomness
for algebraic models

Lower bounds from hitting sets

H is a hitting set for $\mathcal{C}(n, d, s)$ if

for all $0 \neq P \in \mathcal{C}(n, d, s)$, there is some $\bar{a} \in H$ such that $P(\bar{a}) \neq 0$.

Lower bounds from hitting sets

H is a hitting set for $\mathcal{C}(n, d, s)$ if

for all $0 \neq P \in \mathcal{C}(n, d, s)$, there is some $\bar{a} \in H$ such that $P(\bar{a}) \neq 0$.

Observation

If P is a nonzero polynomial that *vanishes* on H , then P cannot be a member of $\mathcal{C}(n, d, s)$.

Lower bounds from hitting sets

H is a hitting set for $\mathcal{C}(n, d, s)$ if

for all $0 \neq P \in \mathcal{C}(n, d, s)$, there is some $\bar{a} \in H$ such that $P(\bar{a}) \neq 0$.

Observation

If P is a nonzero polynomial that vanishes on H , then P cannot be a member of $\mathcal{C}(n, d, s)$.

Theorem ([Heintz-Schnorr, Agrawal])

For any $k \leq n$ such that $k |H|^{1/k} \leq d$, we can find a nonzero k -variate polynomial Q of individual degree less than $|H|^{1/k}$ such that Q requires size more than s .

Hitting sets from lower bounds

Theorem ([Kabanets-Impagliazzo] (Informal))

If Q is *hard-enough*, then for any small algebraic circuit computing P , we have

$$P(x_1, \dots, x_m) \neq 0 \iff P(Q(\bar{y}_1), \dots, Q(\bar{y}_m)) \neq 0$$

even if $\bar{y}_1, \dots, \bar{y}_m$ are *almost disjoint*.

Hitting sets from lower bounds

Aside: Combinatorial Designs



Hitting sets from lower bounds

Aside: Combinatorial Designs

Definition (Combinatorial designs)

$\{S_1, \dots, S_m\} \subseteq [\ell]$ is an (ℓ, k, r) -design if $|S_i| = k$ and $|S_i \cap S_j| < r$.

Hitting sets from lower bounds

Aside: Combinatorial Designs

Definition (Combinatorial designs)

$\{S_1, \dots, S_m\} \subseteq [\ell]$ is an (ℓ, k, r) -design if $|S_i| = k$ and $|S_i \cap S_j| < r$.

Fact

For all* $\ell \geq k^2$ and $r \leq k$, we have explicit (ℓ, k, r) -designs with $m = \binom{\ell}{k}^r$.

Hitting sets from lower bounds

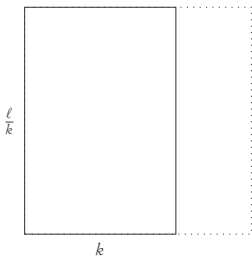
Aside: Combinatorial Designs

Definition (Combinatorial designs)

$\{S_1, \dots, S_m\} \subseteq [\ell]$ is an (ℓ, k, r) -design if $|S_i| = k$ and $|S_i \cap S_j| < r$.

Fact

For all* $\ell \geq k^2$ and $r \leq k$, we have explicit (ℓ, k, r) -designs with $m = \left(\frac{\ell}{k}\right)^r$.



$$|\mathbb{F}| = (\ell/k).$$

Hitting sets from lower bounds

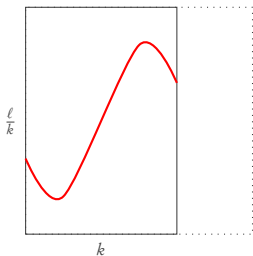
Aside: Combinatorial Designs

Definition (Combinatorial designs)

$\{S_1, \dots, S_m\} \subseteq [\ell]$ is an (ℓ, k, r) -design if $|S_i| = k$ and $|S_i \cap S_j| < r$.

Fact

For all* $\ell \geq k^2$ and $r \leq k$, we have explicit (ℓ, k, r) -designs with $m = \left(\frac{\ell}{k}\right)^r$.



$$|\mathbb{F}| = (\ell/k).$$

For $p(z) \in \mathbb{F}[z]$ with $\deg(p) < r$,

$$S_p = \{(i, p(i)) : i \in [k]\}.$$

Hitting sets from lower bounds

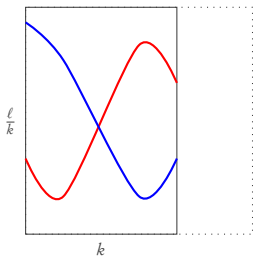
Aside: Combinatorial Designs

Definition (Combinatorial designs)

$\{S_1, \dots, S_m\} \subseteq [\ell]$ is an (ℓ, k, r) -design if $|S_i| = k$ and $|S_i \cap S_j| < r$.

Fact

For all* $\ell \geq k^2$ and $r \leq k$, we have explicit (ℓ, k, r) -designs with $m = \left(\frac{\ell}{k}\right)^r$.



$$|\mathbb{F}| = (\ell/k).$$

For $p(z) \in \mathbb{F}[z]$ with $\deg(p) < r$,

$$S_p = \{(i, p(i)) : i \in [k]\}.$$

Hitting sets from lower bounds

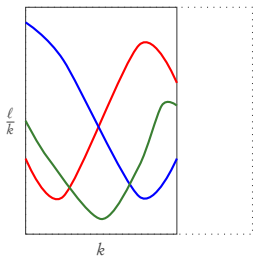
Aside: Combinatorial Designs

Definition (Combinatorial designs)

$\{S_1, \dots, S_m\} \subseteq [\ell]$ is an (ℓ, k, r) -design if $|S_i| = k$ and $|S_i \cap S_j| < r$.

Fact

For all* $\ell \geq k^2$ and $r \leq k$, we have explicit (ℓ, k, r) -designs with $m = \left(\frac{\ell}{k}\right)^r$.



$$|\mathbb{F}| = (\ell/k).$$

For $p(z) \in \mathbb{F}[z]$ with $\deg(p) < r$,

$$S_p = \{(i, p(i)) : i \in [k]\}.$$

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y} |_{S_1}), \dots, Q(\bar{y} |_{S_m}))$$

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.

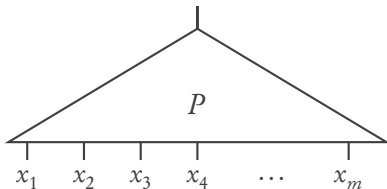
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y} |_{S_1}), \dots, Q(\bar{y} |_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



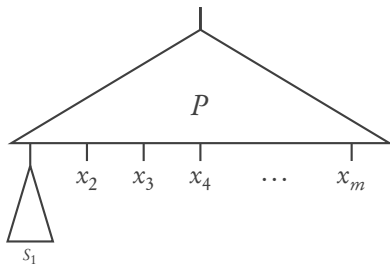
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has **small** circuits.



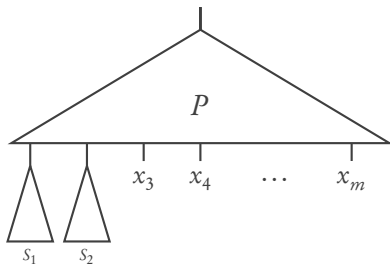
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



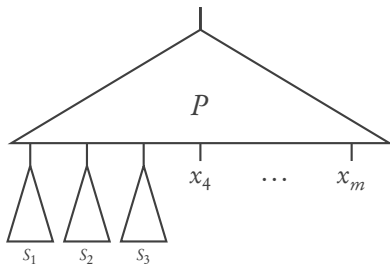
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



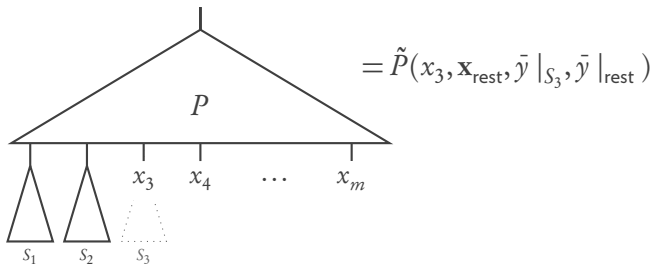
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



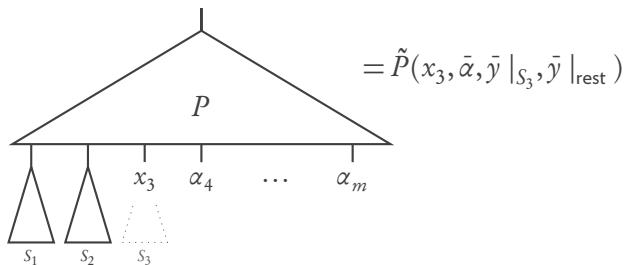
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



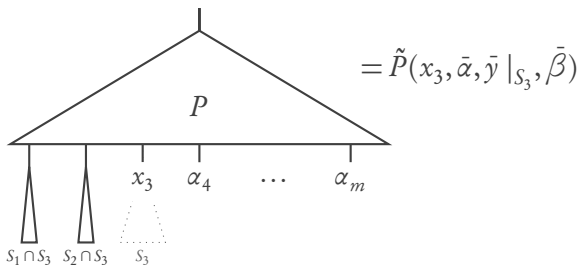
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



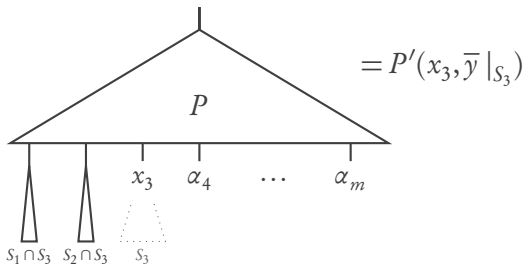
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



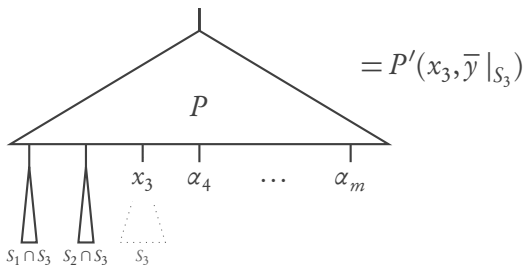
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

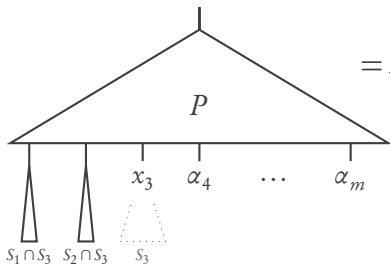
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$$(x_3 - Q) \text{ divides } P'$$

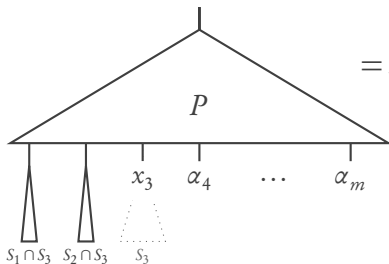
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has *small* circuits.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$(x_3 - Q)$ divides P' .

[Kaltofen, Bürgisser]:

Factors have small circuits.

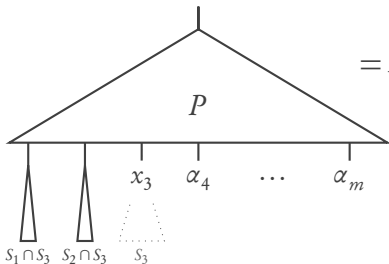
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has circuits of size $(s \cdot r \cdot d^r \cdot D)^{O(1)}$.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$(x_3 - Q)$ divides P' .

[Kaltofen, Bürgisser]:

Factors have small circuits.

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y} |_{S_1}), \dots, Q(\bar{y} |_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Suppose Q *does not* have circuits of size $(s \cdot r \cdot d^r \cdot D)^{O(1)}$.

Then, for any nonzero polynomial $P(x_1, \dots, x_m)$ of degree at most D and circuit size at most s , we have that $P(Q[\ell, k, r]) \neq 0$.

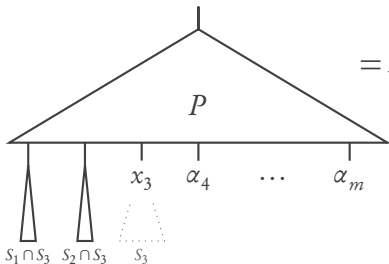
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has circuits of size $(s \cdot r \cdot d^r \cdot D)^{O(1)}$.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$(x_3 - Q)$ divides P' .

[Kaltofen, Bürgisser]:

Factors have small circuits.

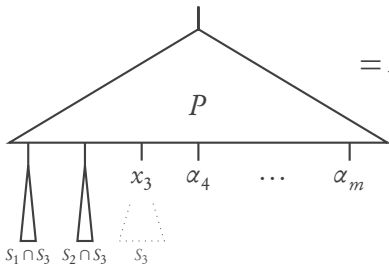
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has circuits of size $(s \cdot r \cdot d^r \cdot D)^{O(1)}$.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$(x_3 - Q)$ divides P' .

[Kaltofen, Bürgisser]:

Factors have small **circuits**.

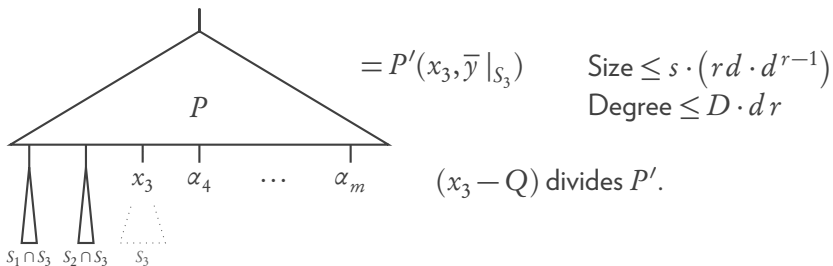
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has circuits of size $(s \cdot r \cdot d^r \cdot D)^{O(1)}$.



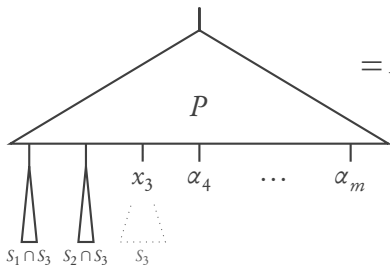
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kabanets-Impagliazzo])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s circuit. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then Q has circuits of size $(s \cdot r \cdot d^r \cdot D)^{O(1)}$.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$(x_3 - Q)$ divides P' .

$P'(0, \bar{y}|_{S_3})$ is a multiple of Q .
(after dividing by x_3 ; interpolation)

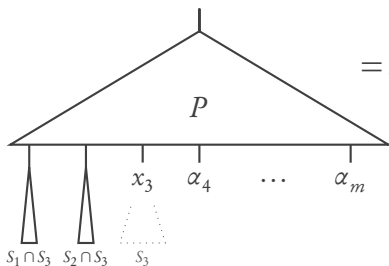
Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kumar-S-Tengse])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s formula. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then a low-degree multiple of Q has formulas of size $(s \cdot r \cdot d^r \cdot (D + 1))$.



$$= P'(x_3, \bar{y}|_{S_3})$$

$$\text{Size} \leq s \cdot (rd \cdot d^{r-1})$$

$$\text{Degree} \leq D \cdot dr$$

$(x_3 - Q)$ divides P' .

$P'(0, \bar{y}|_{S_3})$ is a multiple of Q .
(after dividing by x_3 ; interpolation)

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kumar-S-Tengse])

Let $P(x_1, \dots, x_m)$ is a nonzero polynomial of degree at most D that is computable by a size s formula. Suppose Q is a k -variate polynomial of ind. degree $< d$ such that $P(Q[\ell, k, r]) = 0$.

Then a low-degree multiple of Q has formulas of size $(s \cdot r \cdot d^r \cdot (D + 1))$.

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kumar-S-Tengse])

Suppose Q has the property that no multiple of Q of degree at most $D \cdot d^r$ has a formula of size $(s \cdot r \cdot d^r \cdot (D + 1))$.

Then, for any nonzero polynomial $P(x_1, \dots, x_m)$ of degree at most D and formula size at most s , we have that $P(Q[\ell, k, r]) \neq 0$.

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y}|_{S_1}), \dots, Q(\bar{y}|_{S_m}))$$

Lemma ([Kumar-S-Tengse])

Suppose Q has the property that no multiple of Q of degree at most $D \cdot d^r$ has a formula of size $(s \cdot r \cdot d^r \cdot (D + 1))$.

Then, for any nonzero polynomial $P(x_1, \dots, x_m)$ of degree at most D and formula size at most s , we have that $P(Q[\ell, k, r]) \neq 0$.

Corollary

Suppose Q vanishes on a hitting set for $\text{Formula}(k, d', s')$ with $d' = (D \cdot d^r)$ and $s' = s \cdot r \cdot d^r \cdot (D + 1)$. Then, if $P \in \text{Formula}(m, D, s)$, we have

$$P \neq 0 \iff P(Q[\ell, k, r]) \neq 0.$$

Hitting sets from lower bounds

$$Q[\ell, k, r] := (Q(\bar{y} |_{S_1}), \dots, Q(\bar{y} |_{S_m}))$$

Lemma ([Kumar-S-Tengse])

Suppose Q has the property that no multiple of Q of degree at most $D \cdot d r$ has a formula of size $(s \cdot r \cdot d^r \cdot (D + 1))$.

Then, for any nonzero polynomial $P(x_1, \dots, x_m)$ of degree at most D and formula size at most s , we have that $P(Q[\ell, k, r]) \neq 0$.

Corollary

Suppose Q vanishes on a hitting set for $\text{Formula}(k, d', s')$ with $d' = (D \cdot d r)$ and $s' = s \cdot r \cdot d^r \cdot (D + 1)$. Then, if $P \in \text{Formula}(m, D, s)$, we have

$$P \neq 0 \iff P(Q[\ell, k, r]) \neq 0.$$

From hitting sets for k -variate formulas, we obtain a hitting set for m -variate formulas.

Template for “Hardness to Randomness”



Template for “Hardness to Randomness”

Hyp: Given a k -variate polynomial Q that is s^c -hard.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

Template for “Hardness to Randomness”

Hyp: Given a k -variate polynomial Q that is s^c -hard.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

- ▶ Construct an (ℓ, k, r) -design $S_1, \dots, S_m \subseteq [\ell]$

Template for “Hardness to Randomness”

Hyp: Given a k -variate polynomial Q that is s^c -hard.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

▶ Construct an (ℓ, k, r) -design $S_1, \dots, S_m \subseteq [\ell]$

▶ Use the hardness of Q to argue that

$$0 \neq P \in \mathcal{C}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$$

Template for “Hardness to Randomness”

Hyp: Given a k -variate polynomial Q that is s^c -hard.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

▶ Construct an (ℓ, k, r) -design $S_1, \dots, S_m \subseteq [\ell]$

▶ Use the hardness of Q to argue that

$$0 \neq P \in \mathcal{C}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$$

▶ Brute-force on the polynomial $P(Q[\ell, k, r])$ to test if this is zero.

Template for “Hardness to Randomness”

Hyp: Hitting sets for $\mathcal{C}(\ell, s, s)$ for all $s \geq \ell$.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

▶ Construct an (ℓ, k, r) -design $S_1, \dots, S_m \subseteq [\ell]$

▶ Use the hardness of Q to argue that

$$0 \neq P \in \mathcal{C}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$$

▶ Brute-force on the polynomial $P(Q[\ell, k, r])$ to test if this is zero.

Template for “Hardness to Randomness”

Hyp: Hitting sets for $\mathcal{C}(\ell, s, s)$ for all $s \geq \ell$.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

- ▶ Construct an (ℓ, k, r) -design $S_1, \dots, S_m \subseteq [\ell]$
- ▶ Use **Hyp** to take a hitting set for $\mathcal{C}(\ell, s^c, s^c)$ to construct a **hard** k -variate polynomial Q .
- ▶ Use the hardness of Q to argue that

$$0 \neq P \in \mathcal{C}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$$

- ▶ Brute-force on the polynomial $P(Q[\ell, k, r])$ to test if this is zero.

Template for “Hardness to Randomness”

Hyp: Hitting sets for $\mathcal{C}(\ell, s, s)$ for all $s \geq \ell$.

Goal: Construct “better” hitting sets for $\mathcal{C}(m, s, s)$ for all $s \geq m$

- ▶ Construct an (ℓ, k, r) -design $S_1, \dots, S_m \subseteq [\ell]$
- ▶ Use **Hyp** to take a hitting set for $\mathcal{C}(\ell, s^c, s^c)$ to construct a **hard** k -variate polynomial Q .
- ▶ Use the hardness of Q to argue that

$$0 \neq P \in \mathcal{C}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$$

- ▶ $P(Q[\ell, k, r]) \in \mathcal{C}(\ell, s', s')$ for a small-ish s' . Use **Hyp** on it.

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

If Q is a k -variate polynomial ($k = 1000 \log m$) that is s^5 -hard, then we can do a variable reduction from m to $\ell = O(\log^2 m)$ that preserves nonzeroness.

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

If Q is a k -variate polynomial ($k = 1000 \log m$) that is s^5 -hard, then we can do a variable reduction from m to $\ell = O(\log^2 m)$ that preserves nonzeroness.

$P' = P(Q[\ell, k, r]) \in \mathcal{C}(\ell, s', s')$ for a small-ish s' .

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

If Q is a k -variate polynomial ($k = 1000 \log m$) that is s^5 -hard, then we can do a variable reduction from m to $\ell = O(\log^2 m)$ that preserves nonzeroness.

$P' = P(Q[\ell, k, r]) \in \mathcal{C}(\ell, s', s')$ for a small-ish s' .

Note: s' is already exponential in ℓ .

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

If Q is a k -variate polynomial ($k = 1000 \log m$) that is s^5 -hard, then we can do a variable reduction from m to $\ell = O(\log^2 m)$ that preserves nonzeroness.

$P' = P(Q[\ell, k, r]) \in \mathcal{C}(\ell, s', s')$ for a small-ish s' .

Note: s' is already exponential in ℓ . Hence, to apply this once more, we $k = O(\log \ell)$ variate polynomial that is $(s')^5 = \exp(\exp(k))$ -hard.

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

If Q is a k -variate polynomial ($k = 1000 \log m$) that is s^5 -hard, then we can do a variable reduction from m to $\ell = O(\log^2 m)$ that preserves nonzeroness.

$P' = P(Q[\ell, k, r]) \in \mathcal{C}(\ell, s', s')$ for a small-ish s' .

Note: s' is already exponential in ℓ . Hence, to apply this once more, we $k = O(\log \ell)$ variate polynomial that is $(s')^5 = \exp(\exp(k))$ -hard.

Unlike the boolean setting, we **can** find such polynomials of suitably large degree.

Why does bootstrapping work?

$0 \neq P \in \mathcal{C}(m, s, s)$ (think of $s = m^5$).

If Q is a k -variate polynomial ($k = 1000 \log m$) that is s^5 -hard, then we can do a variable reduction from m to $\ell = O(\log^2 m)$ that preserves nonzeroness.

$P' = P(Q[\ell, k, r]) \in \mathcal{C}(\ell, s', s')$ for a small-ish s' .

Note: s' is already exponential in ℓ . Hence, to apply this once more, we $k = O(\log \ell)$ variate polynomial that is $(s')^5 = \exp(\exp(k))$ -hard.

Unlike the boolean setting, we **can** find such polynomials of suitably large degree.

Thus, there is nothing stopping you from doing this again and again.

Plan



Plan

For all $s \geq n_0$:
PIT(n_0, s, s): $s^{n_0-0.01}$

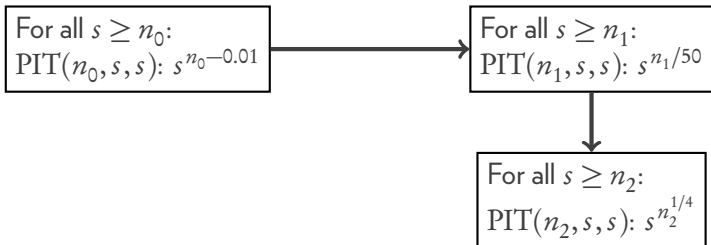
Plan

For all $s \geq n_0$:
PIT(n_0, s, s): $s^{n_0-0.01}$

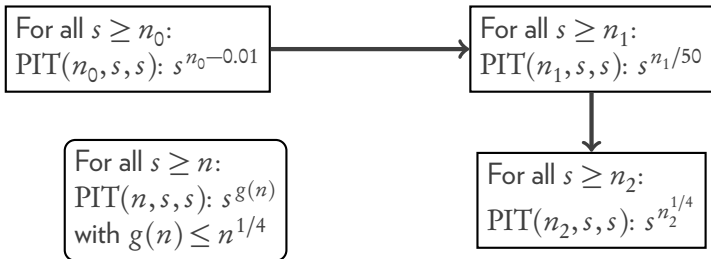


For all $s \geq n_1$:
PIT(n_1, s, s): $s^{n_1/50}$

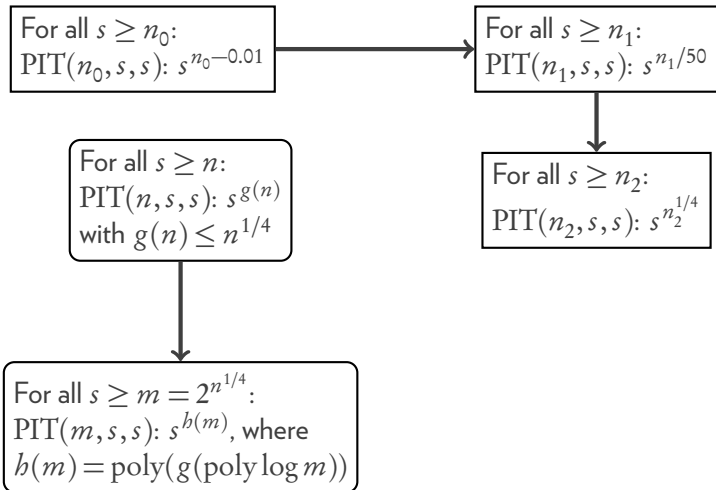
Plan



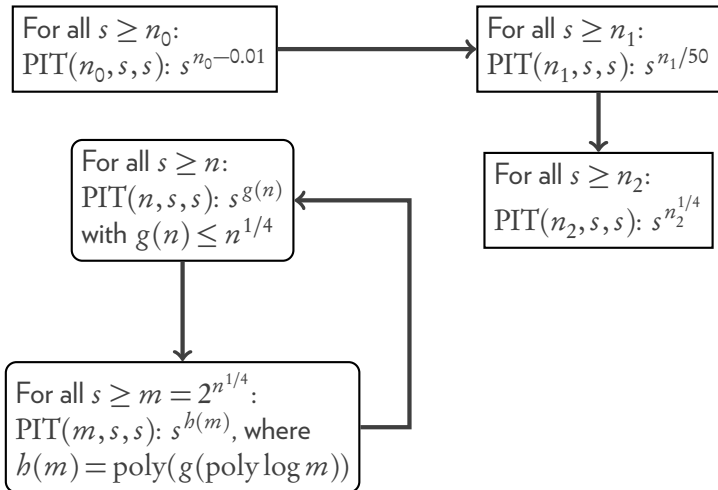
Plan



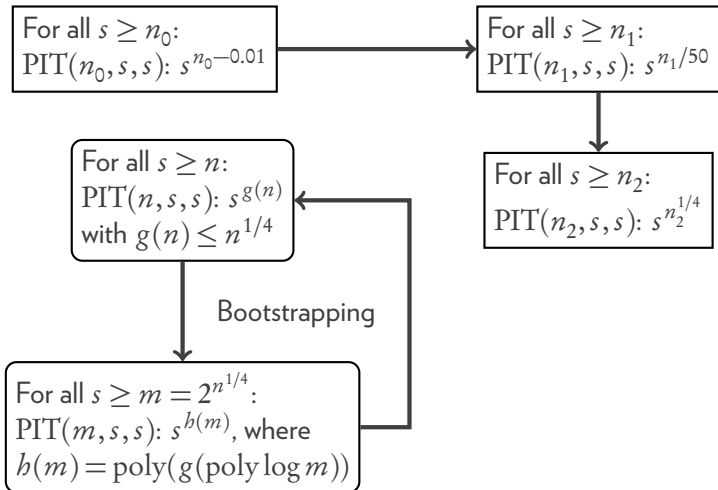
Plan



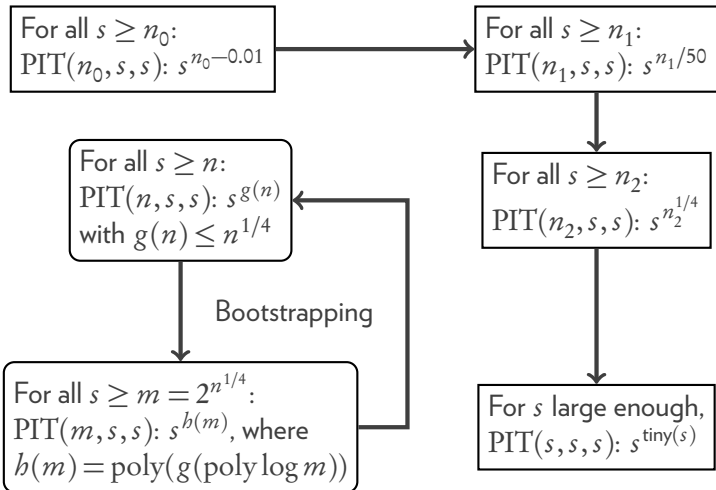
Plan



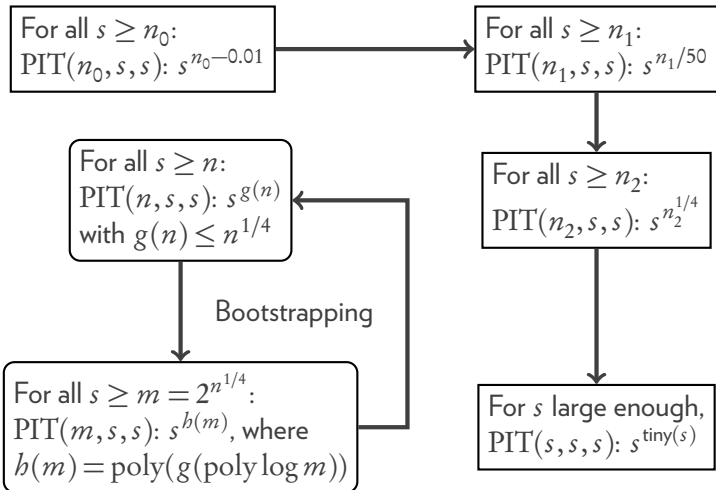
Plan



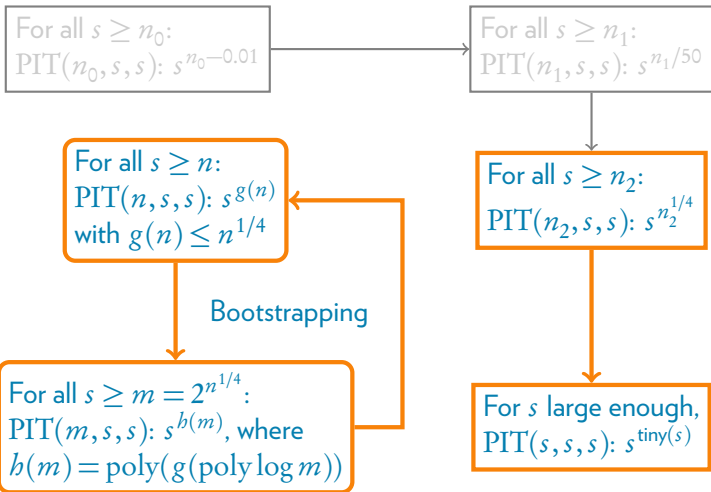
Plan



Plan



Plan



Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{n^{1/4}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20(g(n))^2$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{n^{1/4}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20(g(n))^2 = 20(\log^4 m)^2.$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{n^{1/4}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20(g(n))^2$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{2^{(1/4)n^{1/4}}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20^{1+2}(g(n))^4$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{c n^{1/4}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20^{1+2}(g(n))^4$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{c n^{1/4}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20^{1+2+4}(g(n))^8$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, for $m = 2^{c^{c^{c^{n^{1/4}}}}}$ and all $s \geq m$, we have an explicit hitting set for $\text{Formula}(m, s, s)$ of size at most

$$s^{h(m)}, \quad \text{with } h(m) \leq 20^{1+2+4+8} (g(n))^{16}$$

Bootstrapping Hitting Sets

Lemma (Bootstrapping slightly non-trivial hitting sets)

Let n be large enough ($n > 10^{10}$). Suppose, for all $s \geq n$, there is an explicit hitting set for $\text{Formula}(n, s, s)$ of size at most

$$s^{g(n)}, \quad \text{with } g(n) \leq \left(\frac{n^{1/4}}{10}\right).$$

Then, we have an explicit hitting set for $\text{Formula}(s, s, s)$ of size

$$s^{\exp(\exp(O(\log^* s)))}.$$

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{iddeg}(Q) < d := s^{5g(n)/k}$.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{iddeg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

Proof.

Q vanishes on a hitting set for $\text{Formula}(k, d', s')$ as

$$\begin{aligned}d' &= dDr = s^{5g(n)/k} \cdot s \cdot r \leq s^5, \\s' &= sr d^r (D + 1) \leq s^4 \cdot s^{5g(n) \cdot r/k} \leq s^5.\end{aligned}$$

Use the previous corollary.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

$P(Q[\ell, k, r])$ is a formula of size, degree at most $s \cdot s^{10g(n)} \leq s^{20g(n)}$.

Proof of the bootstrapping lemma

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n^{1/4}}{10}$.

Let $k = \sqrt{n}$, $\ell = n$ and $r = n^{1/4}$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = 2^{n^{1/4}}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

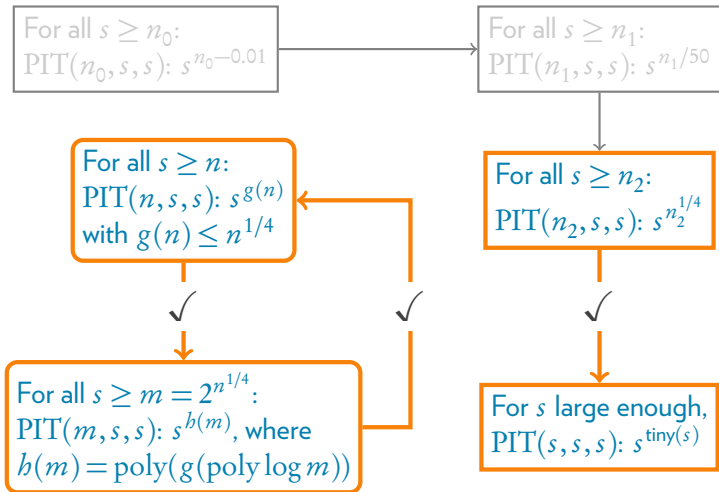
Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

$P(Q[\ell, k, r])$ is a formula of size, degree at most $s \cdot s^{10g(n)} \leq s^{20g(n)}$.

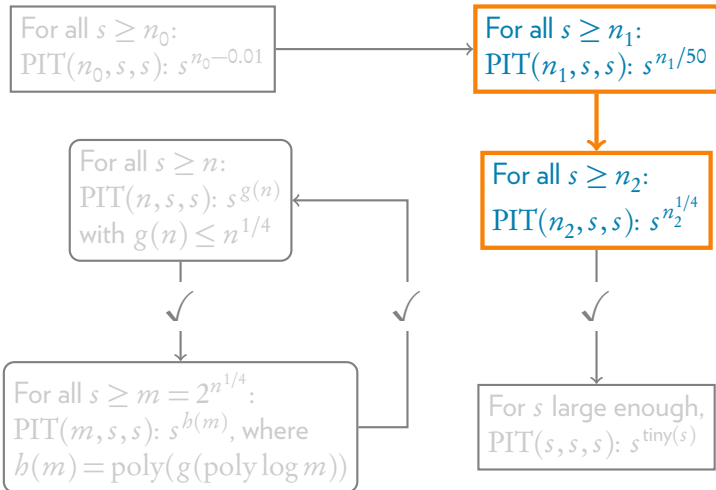
Using the hypothesis again, we get a hitting set of size $s^{20(g(n))^2}$ for $\text{Formula}(m, s, s)$.



Plan



Plan



Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

Proof.

Q vanishes on a hitting set for $\text{Formula}(k, d', s')$ as

$$d' = dDr = s^{5g(n)/k} \cdot s \cdot r \leq s^5,$$

$$s' = srdr(D+1) \leq s^4 \cdot s^{5g(n) \cdot r/k} \leq s^5.$$

Use the previous corollary.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{iddeg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

$P(Q[\ell, k, r])$ is a formula on $\ell = n^2$ variables of degree $s \cdot k \cdot s^{g(n)/k} \leq s^3$.

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{iddeg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

$P(Q[\ell, k, r])$ is a formula on $\ell = n^2$ variables of degree $s \cdot k \cdot s^{g(n)/k} \leq s^3$.

[O-DL-S-Z] lemma: hitting set of size $s^{3\ell}$

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{iddeg}(Q) < d := s^{5g(n)/k}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

$P(Q[\ell, k, r])$ is a formula on $\ell = n^2$ variables of degree $s \cdot k \cdot s^{g(n)/k} \leq s^3$.

[O-DL-S-Z] lemma: hitting set of size $s^{3\ell} \leq s^{(1/10) \cdot m^{1/4}}$

Déjà vu

Hyp: $s^{g(n)}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$, with $g(n) \leq \frac{n}{50}$.

Let $k = n$, $\ell = n^2$ and $r = 10$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = k^{10}$.

Using the hitting set H for $\text{Formula}(n, s^5, s^5)$ of size $s^{5g(n)}$, find Q vanishing on H such that:

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{5g(n)/k}$.

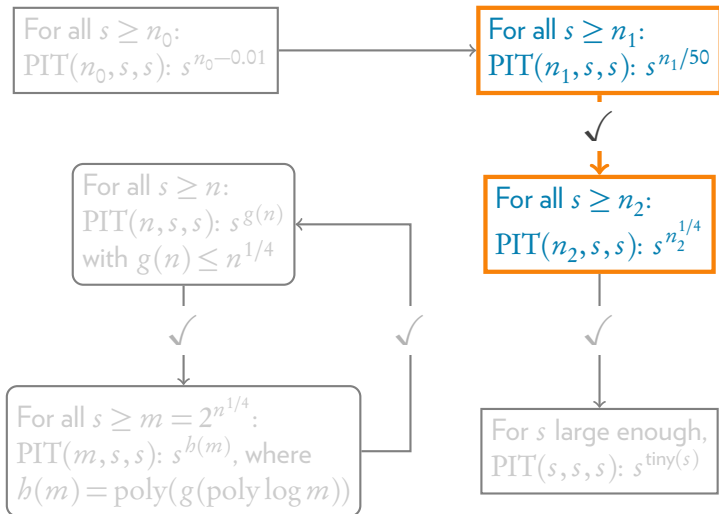
Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$.

$P(Q[\ell, k, r])$ is a formula on $\ell = n^2$ variables of degree $s \cdot k \cdot s^{g(n)/k} \leq s^3$.

[O-DL-S-Z] lemma: hitting set of size $s^{3\ell} \leq s^{(1/10) \cdot m^{1/4}}$



Plan



Plan

For all $s \geq n_0$:
PIT(n_0, s, s): $s^{n_0 - 0.01}$

For all $s \geq n_1$:
PIT(n_1, s, s): $s^{n_1/50}$

For all $s \geq n$:
PIT(n, s, s): $s^{g(n)}$
with $g(n) \leq n^{1/4}$

For all $s \geq n_2$:
PIT(n_2, s, s): $s^{n_2^{1/4}}$

For all $s \geq m = 2^{n^{1/4}}$:
PIT(m, s, s): $s^{h(m)}$, where
 $h(m) = \text{poly}(g(\text{poly log } m))$

For s large enough,
PIT(s, s, s): $s^{\text{tiny}(s)}$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$,

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot ((rd) \cdot d^{r-1}) \cdot (s + 1)$$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot ((rd) \cdot d^{r-1}) \cdot (s + 1)$$

Complexity to compute an $(r - 1)$ -variate polynomial of $\text{ideg } d$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot ((rd) \cdot d^{r-1}) \cdot (s+1)$$

Complexity to compute an $(r-1)$ -variate polynomial of $\text{ideg } d$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot ((rd) \cdot d^{r-1}) \cdot (s + 1)$$

Complexity to compute an univariate polynomial of degree d

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot 10d \cdot (s + 1)$$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot 10d \cdot (s + 1) \leq s^3 \cdot s^{300n-3}$$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Proof: If not, there is a nonzero multiple \tilde{Q} of Q , whose degree is at most $s \cdot (rd) \leq s^{300n}$, computable by a formula of size

$$s \cdot 10d \cdot (s + 1) \leq s^3 \cdot s^{300n-3} \leq s^{300n} \quad \dots \text{no way...}$$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

$P(Q[\ell, k, r])$ is a formula on $\ell = n^5$ variables.

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

$P(Q[\ell, k, r])$ is a formula on $\ell = n^5$ variables of degree $s \cdot k \cdot s^{300n-3} \leq s^{300n}$.

Déjà vu

Hyp: $s^{n-0.01}$ hitting sets for $\mathcal{C}(n, s, s)$, for any $s \geq n$.

Let $k = n$, $\ell = n^5$ and $r = 2$.

Let S_1, \dots, S_m be an (ℓ, k, r) -design with $m = \left(\frac{\ell}{k}\right)^r = n^8$.

Use the hitting set for $\text{Formula}(n, s^{300n}, s^{300n})$ to get

- ▶ Q is k -variate, and $\text{ideg}(Q) < d := s^{300(n-0.01)} = s^{300n-3}$.

Claim: $0 \neq P \in \text{Formula}(m, s, s) \implies P(Q[\ell, k, r]) \neq 0$

$P(Q[\ell, k, r])$ is a formula on $\ell = n^5$ variables of degree $s \cdot k \cdot s^{300n-3} \leq s^{300n}$.

[O-DL-S-Z] lemma: a hitting set of size $s^{300n \cdot n^5} \leq s^{m/50}$ for $\text{Formula}(m, s, s)$. □

Closing remarks



Closing remarks

- ▶ A similar statement also holds for bounded depth formulas, with some slack in depth between the hypothesis and conclusion.
-

Closing remarks

- ▶ A similar statement also holds for bounded depth formulas, with some slack in depth between the hypothesis and conclusion.
 - ▶ It is crucial that the exponent of s in the hypothesis is **independent** of s .
-

Closing remarks

- ▶ A similar statement also holds for bounded depth formulas, with some slack in depth between the hypothesis and conclusion.
- ▶ It is crucial that the exponent of s in the hypothesis is **independent** of s .

Question: Can saying something non-trivial from a hypothesis for just $s = \text{poly}(n)$ circuits?

Closing remarks

- ▶ A similar statement also holds for bounded depth formulas, with some slack in depth between the hypothesis and conclusion.
- ▶ It is crucial that the exponent of s in the hypothesis is **independent** of s .

Question: Can saying something non-trivial from a hypothesis for just $s = \text{poly}(n)$ circuits?

- ▶ To obtain the hitting set for $\mathcal{C}(s, s, s)$, the algorithm would use hitting sets for $\mathcal{C}(n_0, s', s')$ for **various** $s' \leq s^{\text{tiny}(s)}$.

Closing remarks

- ▶ A similar statement also holds for bounded depth formulas, with some slack in depth between the hypothesis and conclusion.
- ▶ It is crucial that the exponent of s in the hypothesis is **independent** of s .

Question: Can saying something non-trivial from a hypothesis for just $s = \text{poly}(n)$ circuits?

- ▶ To obtain the hitting set for $\mathcal{C}(s, s, s)$, the algorithm would use hitting sets for $\mathcal{C}(n_0, s', s')$ for **various** $s' \leq s^{\text{tiny}(s)}$.

Question: Is there a *hardness amplification* (à la [CILM]) in this setting?

Closing remarks

- ▶ A similar statement also holds for bounded depth formulas, with some slack in depth between the hypothesis and conclusion.
- ▶ It is crucial that the exponent of s in the hypothesis is **independent** of s .

Question: Can saying something non-trivial from a hypothesis for just $s = \text{poly}(n)$ circuits?

- ▶ To obtain the hitting set for $\mathcal{C}(s, s, s)$, the algorithm would use hitting sets for $\mathcal{C}(n_0, s', s')$ for **various** $s' \leq s^{\text{tiny}(s)}$.

Question: Is there a *hardness amplification* (à la [CILM]) in this setting?

`\end{document}`