Shallow Circuits with High-Powered Inputs

Pascal Koiran
LIP, Ecole Normale Supérieure de Lyon

Fall School of Logic and Complexity
Prague, September 2011

Two central problems of complexity theory

1. Arithmetic complexity of the permanent
   (Valiant's algebraic version of P versus NP).
2. Derandomization of Polynomial Identity Testing.

- Problems turn out to be related.
- Progress on one may lead to progress on other problem
  (approach to problem 1 advocated by Agrawal, 2005).

Valiant's model: $\mathrm{VP}_K = \mathrm{VNP}_K$?

- Complexity of a polynomial f measured by number $L(f)$ of arithmetic operations $(+,-,\times)$ needed to evaluate f:

  L(f) = size of smallest arithmetic circuit computing f.

- $(f_n) \in \mathrm{VP}$ if number of variables, $\deg(f_n)$ and $L(f_n)$ are polynomially bounded. For instance, $(X^{2^n}) \notin \mathrm{VP}$.
- $(f_n) \in \mathrm{VNP}$ if $f_n(\overline{x}) = \sum_{\overline{y}} g_n(\overline{x}, \overline{y})$

  for some $(g_n) \in \mathrm{VP}$
  (sum ranges over all boolean values of $\overline{y}$).
  If $\mathrm{char}(K) \neq 2$ the permanent is a VNP-complete family:

$$\mathrm{PER}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}.$$

Valiant's model: $\mathrm{VP}_K = \mathrm{VNP}_K$?

- Complexity of a polynomial f measured by number $L(f)$ of arithmetic operations (+,-,$\times$) needed to evaluate f:

  L(f) = size of smallest arithmetic circuit computing f.

- $(f_n) \in \mathrm{VP}$ if number of variables, $\deg(f_n)$ and $L(f_n)$ are polynomially bounded. For instance, $(X^{2^n}) \notin \mathrm{VP}$.

- $(f_n) \in \mathrm{VNP}$ if $f_n(\overline{x}) = \sum_{\overline{y}} g_n(\overline{x}, \overline{y})$

  for some $(g_n) \in \mathrm{VP}$
  (sum ranges over all boolean values of $\overline{y}$).
  If $\mathrm{char}(K) \neq 2$ the permanent is a VNP-complete family:

$$\mathrm{PER}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}.$$

Polynomial Identity Testing

Given polynomial f, decide whether $f \equiv 0$.
If given by an arithmetic circuit: ACIT problem.
Schwartz-Zippel Lemma:
Let $f \in K[X_1, \ldots, X_n]$ of degree d.
If $f \not\equiv 0$ and $X_1, \ldots, X_n$ drawn independently at random from $S \subseteq K$:

$$\Pr[f(X_1, \ldots, X_n) = 0] \leq d/|S|.$$

"Natural" intuition about ACIT:
no efficient deterministic algorithm exists
(because we haven't found any).

Polynomial Identity Testing

Given polynomial f, decide whether $f \equiv 0$.
If given by an arithmetic circuit: ACIT problem.
Schwartz-Zippel Lemma:
Let $f \in K[X_1, \ldots, X_n]$ of degree d.
If $f \not\equiv 0$ and $X_1, \ldots, X_n$ drawn independently at random from $S \subseteq K$:

$$\Pr[f(X_1, \ldots, X_n) = 0] \leq d/|S|.$$

"Natural" intuition about ACIT:
no efficient deterministic algorithm exists
(because we haven't found any).

Hardness versus randomness tradeoffs

Two roughly equivalent problems:

- derandomizing algorithms
- proving lower bounds.

For each problem we need **explicit constructions**.
From Kabanets-Impagliazzo (2004) :

- If ACIT can be derandomized:
  we have a lower bound for the permanent, or NEXP$\not\subset$P/poly.
- If we have a lower bound for the permanent:
  ACIT can be derandomized in subexponential time
  for circuits of logarithmic depth.

A possible approach to arithmetic circuit lower bounds ?
(Agrawal, 2005)

Hardness versus randomness tradeoffs

Two roughly equivalent problems:

- derandomizing algorithms
- proving lower bounds.

For each problem we need **explicit constructions**.
From Kabanets-Impagliazzo (2004) :

- If ACIT can be derandomized:
  we have a lower bound for the permanent, or NEXP$\not\subset$P/poly.
- If we have a lower bound for the permanent:
  ACIT can be derandomized in subexponential time
  for circuits of logarithmic depth.

A possible approach to arithmetic circuit lower bounds ?
(Agrawal, 2005)

Outline of the talk

1. Lower bounds from derandomization.
2. The real τ-conjecture.
3. An unconditional lower bound for the permanent.
4. Proof sketch for a result of Bürgisser's.

The black-box model

Only way to access f:

$$x \mapsto \boxed{\textbf{black box}} \to f(x).$$

Some problems studied in this model:
factorization, GCD, interpolation. . .
Two equivalent problems:

- derandomization of PIT in the black blox model.
- Construction of a *hitting set*.

A hitting set H for a family $\mathcal{F}$ of polynomials must contain for every $f \not\equiv 0$ in $\mathcal{F}$ a point x such that $f(x) \neq 0$.
Remark:
Hitting sets $\Rightarrow$ derandomization in (low-degree) circuit model.

Existence of small hitting sets

Recall from Schwartz-Zippel lemma:

$$\Pr[f(X_1, \ldots, X_n) = 0] \leq 1/2$$

if $|S| \geq 2d$.
Let $H = m$ random elements of S^n.
For $f \not\equiv 0$, $\Pr[f \equiv 0 \text{ on } H] \leq 1/2^m$.
Let $\mathcal{F}$ be a family of polynomials.
By union bound, H is *not* a hitting set with probability $\leq |\mathcal{F}|/2^m$:
take $m > \log |\mathcal{F}|$.
Remarks: same proof as RP $\subseteq$ P/poly (Adleman, 1978);
good bounds also for some infinite families $\mathcal{F}$
(Heintz-Schnorr, 1980).

Lower bounds from (univariate) hitting sets

Let $H = \{a_1, \ldots, a_k\}$ be a hitting set for $\mathcal{F}$, and

$$f(X) = \prod_{i=1}^{k}(X - a_i).$$

Then $f \notin \mathcal{F}$.
If H is explicit then f is explicit too!
Remarks:

1. This is a kind of indirect diagonalization.
2. Argument appears already in Heintz and Schnorr (1980).
3. Low-degree multivariate version in Agrawal (2005).
4. Our results are based on the univariate version.

Sums of products of sparse (univariate) polynomials

SPS polynomials are of the form $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$ where the f_{ij} are t-sparse.

Hardness versus randomness (informal statement): Efficient deterministic constructions of hitting sets for SPS polynomials imply that perm is hard for arithmetic circuits.

Remark: Polynomial size hitting sets exist by standard (probabilistic) arguments.

Benefits of univariate method:

1. Would lead to lower bounds for the permanent, instead of polynomials with PSPACE coefficients (i.e., in VPSPACE).
2. Leads to new versions of Shub and Smale's τ-conjecture.

Sums of products of sparse (univariate) polynomials

SPS polynomials are of the form $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$ where the f_{ij} are t-sparse.

Hardness versus randomness (informal statement): Efficient deterministic constructions of hitting sets for SPS polynomials imply that perm is hard for arithmetic circuits.

Remark: Polynomial size hitting sets exist by standard (probabilistic) arguments.

Benefits of univariate method:

1. Would lead to lower bounds for the permanent, instead of polynomials with PSPACE coefficients (i.e., in VPSPACE).
2. Leads to new versions of Shub and Smale's τ-conjecture.

Algebraic number generators

This is a sequence $(f_i)_{i\geq 1}$ of nonzero polynomials of $\mathbb{Z}[X]$:
$f_i(X) = \sum_\alpha a(\alpha, i)X^\alpha$ where

1. $\deg(f_i) \leq i^c$ and $|a(\alpha, i)| \leq 2^{i^c}$ for some constant c;
2. The $a(\alpha, i)$ can be computed *efficiently*, i.e.,

$$L(f) = \{(\alpha, i, j);\ \ \text{the } j\text{-th bit of } a(\alpha, i) \text{ is equal to } 1\}$$

is in P... or in P/poly ... or even in CH/poly.

Example: $L(f) \in \mathrm{P}$ for $f_i(X) = X - i$, $X^i - 1$ or $X^i - 2^i X + i^2 + 1$.
Remarks: A generator generates the roots of the f_i;
We will consider hitting sets made of the roots of an initial segment of the f_i.

Hardness versus randomness, formal statement

Consider a SPS polynomial

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$$

where the f_{ij} are t-sparse;
$\mathrm{size}(f)$ = number of monomials in this expression ($\leq kmt$).

Theorem: Let (f_i) be an algebraic number generator, and H_m the set of all roots of the polynomials f_i for all $i \leq m$. Assume that there exists a polynomial p such that $H_{p(s)}$ is a hitting set for SPS polynomials of size $\leq s$. Then Permanent does not have (constant free) arithmetic circuits of polynomial size.

Remark: More refined statement in ICS 2011 paper.

Hitting sets for sparse polynomials: roots of unity

Theorem [Bläser - Hardt - Lipton - Vishnoi'09]:
For the set polynomials $f \in \mathbb{C}[X]$ with at most t monomials, of degree at most d:
let H be the set of all p-th roots of unity for all $p \in \mathcal{P}$, where $\mathcal{P}$ is a set of at least $t \log d$ prime numbers.
Proof: If $f = 0$ on H then $f \equiv 0 \bmod (X^p - 1)$ for all $p \in \mathcal{P}$.
Fix monomial $a_i X^{\alpha_i}$ in f.
Then $p | (\alpha_j - \alpha_i)$ for some other monomial $a_j X^{\alpha_j}$.

(i) For fixed i, $< t$ choices for j.

(ii) For fixed i, j, at most $\log d$ choices for p.

Hitting sets for sparse polynomials: Descartes's rule

Observation:
For the set of polynomials $f \in \mathbb{R}[X]$ with at most t monomials, any set $H \subseteq \mathbb{R}_+^*$ with $|H| = t$ is a hitting set. Follows from:

Theorem [Descartes' rule without signs]:
f has at most $t-1$ positive real roots.
Proof: Induction on t. No positive root for $t = 1$.
For $t > 1$: let $a_\alpha X^\alpha =$ lowest degree monomial.
We can assume $\alpha = 0$ (divide by X^α if not). Then:

(i) f' has $t-1$ monomials $\Rightarrow \leq t-2$ positive real roots.
(ii) There is a positive root of f' between 2 consecutive positive roots of f (Rolle's theorem).

To generalize the observation to bigger classes of real polynomials: we need to bound the number of real roots.

Hitting sets for sparse polynomials: Descartes's rule

Observation:
For the set of polynomials $f \in \mathbb{R}[X]$ with at most t monomials, any set $H \subseteq \mathbb{R}_+^*$ with $|H| = t$ is a hitting set. Follows from:

Theorem [Descartes' rule without signs]:
f has at most $t-1$ positive real roots.
Proof: Induction on t. No positive root for $t = 1$.
For $t > 1$: let $a_\alpha X^\alpha$ = lowest degree monomial.
We can assume $\alpha = 0$ (divide by X^α if not). Then:

(i) f' has $t-1$ monomials $\Rightarrow \leq t-2$ positive real roots.
(ii) There is a positive root of f' between 2 consecutive positive roots of f (Rolle's theorem).

To generalize the observation to bigger classes of real polynomials: we need to bound the number of real roots.

Hitting sets for sparse polynomials: Descartes's rule

Observation:
For the set of polynomials $f \in \mathbb{R}[X]$ with at most t monomials, any set $H \subseteq \mathbb{R}_+^*$ with $|H| = t$ is a hitting set. Follows from:

Theorem [Descartes' rule without signs]:
f has at most $t-1$ positive real roots.
Proof: Induction on t. No positive root for $t=1$.
For $t > 1$: let $a_\alpha X^\alpha$ = lowest degree monomial.
We can assume $\alpha = 0$ (divide by X^α if not). Then:

(i) f' has $t-1$ monomials $\Rightarrow \leq t-2$ positive real roots.
(ii) There is a positive root of f' between 2 consecutive positive roots of f (Rolle's theorem).

To generalize the observation to bigger classes of real polynomials: we need to bound the number of real roots.

Hitting sets for sparse polynomials: Descartes's rule

Observation:
For the set of polynomials $f \in \mathbb{R}[X]$ with at most t monomials, any set $H \subseteq \mathbb{R}_+^*$ with $|H| = t$ is a hitting set. Follows from:

Theorem [Descartes' rule without signs]:
f has at most $t-1$ positive real roots.
Proof: Induction on t. No positive root for $t = 1$.
For $t > 1$: let $a_\alpha X^\alpha =$ lowest degree monomial.
We can assume $\alpha = 0$ (divide by X^α if not). Then:

(i) f' has $t-1$ monomials $\Rightarrow \leq t-2$ positive real roots.
(ii) There is a positive root of f' between 2 consecutive positive roots of f (Rolle's theorem).

To generalize the observation to bigger classes of real polynomials: we need to bound the number of real roots.

On the number of additions to compute specific polynomials

Model: multiplications are free.
Theorem [Borodin-Cook'76]:
If $f \in \mathbb{R}[X]$ is computable in k additions,
f has at most $\phi(k)$ real zeros.
ϕ is an explicit (astronomical) function.
Theorem [Grigoriev'82, Risler'85]: One can take $\phi(k) = 2^{(4k)^2}$.
Proof based on Khovanskii's theory of fewnomials.
Remark [Borodin-Cook'76, Shub-Smale]:
For some f the number of real zeros is $2^{\Omega(L(f))}$ (i.e. $\geq 2^{\Omega(k)}$).
Tau-conjecture [Shub-Smale'95]:
For constant-free circuits, the number of integer roots
is polynomially bounded.

On the number of additions to compute specific polynomials

Model: multiplications are free.

Theorem [Borodin-Cook'76]:
If $f \in \mathbb{R}[X]$ is computable in k additions,
f has at most $\phi(k)$ real zeros.
ϕ is an explicit (astronomical) function.

Theorem [Grigoriev'82, Risler'85]: One can take $\phi(k) = 2^{(4k)^2}$.
Proof based on Khovanskii's theory of fewnomials.

Remark [Borodin-Cook'76, Shub-Smale]:
For some f the number of real zeros is $2^{\Omega(L(f))}$ (i.e. $\geq 2^{\Omega(k)}$).

Tau-conjecture [Shub-Smale'95]:
For constant-free circuits, the number of integer roots
is polynomially bounded.

On the number of additions to compute specific polynomials

Model: multiplications are free.

Theorem [Borodin-Cook'76]:
If $f \in \mathbb{R}[X]$ is computable in k additions,
f has at most $\phi(k)$ real zeros.
ϕ is an explicit (astronomical) function.

Theorem [Grigoriev'82, Risler'85]: One can take $\phi(k) = 2^{(4k)^2}$.
Proof based on Khovanskii's theory of fewnomials.

Remark [Borodin-Cook'76, Shub-Smale]:
For some f the number of real zeros is $2^{\Omega(L(f))}$ (i.e. $\geq 2^{\Omega(k)}$).

Tau-conjecture [Shub-Smale'95]:
For constant-free circuits, the number of integer roots is polynomially bounded.

On the number of additions to compute specific polynomials

Model: multiplications are free.

Theorem [Borodin-Cook'76]:
If $f \in \mathbb{R}[X]$ is computable in k additions,
f has at most $\phi(k)$ real zeros.
ϕ is an explicit (astronomical) function.

Theorem [Grigoriev'82, Risler'85]: One can take $\phi(k) = 2^{(4k)^2}$.
Proof based on Khovanskii's theory of fewnomials.

Remark [Borodin-Cook'76, Shub-Smale]:
For some f the number of real zeros is $2^{\Omega(L(f))}$ (i.e. $\geq 2^{\Omega(k)}$).

Tau-conjecture [Shub-Smale'95]:
For constant-free circuits, the number of integer roots
is polynomially bounded.

Chebyshev polynomials

- Let T_n be the Chebyshev polynomial of order n:

$$\cos(n\theta) = T_n(\cos\theta).$$

  For instance $T_1(x) = x,\ T_2(x) = 2x^2 - 1$.
- T_n is a degree n polynomial with n real zeros on $[-1, 1]$.
- $T_{2^n}(x) = T_2(T_2(\cdots T_2(T_2(x))\cdots))$: n-th iterate of T_2.
  As a result $\tau(T_{2^n}) = O(n)$.

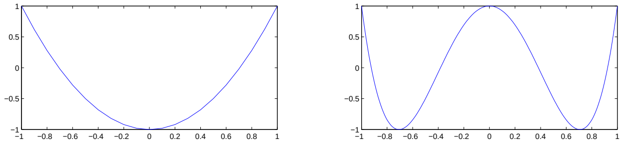

Figure: Plots of T_2 and T_4

Real τ-conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$, where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- Case $k = 1$ of the conjecture is obvious, $k = 2$ is open.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful ?

Real τ-conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$,
where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- Case $k = 1$ of the conjecture is obvious, $k = 2$ is open.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful ?

First ingredient: reduction to depth 4

Depth reduction theorem (Agrawal and Vinay, 2008):
Any multilinear polynomial in n variables with an arithmetic circuit of size $2^{o(n)}$ also has a depth four ($\Sigma\Pi\Sigma\Pi$) circuit of size $2^{o(n)}$.

Our polynomials are far from multilinear, but:

Depth-4 circuit with inputs of the form X^{2^i}, or constants *(Shallow circuit with high-powered inputs)*

$\Updownarrow$

Sum of Products of Sparse Polynomials

Second ingredient: Pochhammer-Wilkinson polynomials

$$PW_n(X) = \prod_{i=1}^{n}(X - i)$$

Theorem [Bürgisser'07-09]:
If the permanent is easy then PW_n has circuits of size $(\log n)^{O(1)}$.

How the proof does *not* go

Assume by contradiction that the permanent is easy.
Goal:
Show that SPS polynomials of size $2^{o(n)}$ can compute $\prod_{i=1}^{2^n}(X-i)$
$\Rightarrow$ contradiction with real τ-conjecture.

1. From assumption: $\prod_{i=1}^{2^n}(X-i)$ has circuits of polynomial in n (Bürgisser).
2. Reduction to depth 4 $\Rightarrow$ SPS polynomials of size $2^{o(n)}$.

What's wrong with this argument:

How the proof does *not* go

Assume by contradiction that the permanent is easy.

Goal:

Show that SPS polynomials of size $2^{o(n)}$ can compute $\prod_{i=1}^{2^n}(X-i)$
$\Rightarrow$ contradiction with real τ-conjecture.

1. From assumption: $\prod_{i=1}^{2^n}(X-i)$ has circuits of polynomial in n (Bürgisser).
2. Reduction to depth 4 $\Rightarrow$ SPS polynomials of size $2^{o(n)}$.

What's wrong with this argument:
No high-degree analogue of reduction to depth 4
(think of Chebyshev's polynomials).

How the proof goes (more or less)

Assume that the permanent is easy.
Goal:
Show that SPS polynomials of size $2^{o(n)}$ can compute $\prod_{i=1}^{2^n}(X-i)$
$\Rightarrow$ contradiction with real τ-conjecture.

1. From assumption: $\prod_{i=1}^{2^n}(X-i)$ has circuits of polynomial in n (Bürgisser).
2. Reduction to depth 4 $\Rightarrow$ SPS polynomials of size $2^{o(n)}$.

For step 2: need to use again the assumption that perm is easy.

A tractable special case
(joint work with B. Grenet, N. Portier and Y. Strozecki)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.

Theorem 1 (number of real roots):
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.

Proof method: Do an induction on k and use Rolle's theorem.
We have a sum of k terms: $f(X) = \sum_{i=1}^{k} T_i(X)$.
Taking the derivative of f/T_1 removes a term. $\square$

Theorem 2 (identity testing): For fixed k and m,
$f \equiv 0$ can be tested deterministically in polynomial-time.
Remark: The algorithm is non-black-box:
It executes the induction in Theorem 1.

A tractable special case
(joint work with B. Grenet, N. Portier and Y. Strozecki)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.
Theorem 1 (number of real roots):
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.
Proof method: Do an induction on k and use Rolle's theorem.
We have a sum of k terms: $f(X) = \sum_{i=1}^{k} T_i(X)$.
Taking the derivative of f/T_1 removes a term. □

Theorem 2 (identity testing): For fixed k and m,
$f \equiv 0$ can be tested deterministically in polynomial-time.
Remark: The algorithm is non-black-box:
It executes the induction in Theorem 1.

A tractable special case (joint work with B. Grenet, N. Portier and Y. Strozecki)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.
Theorem 1 (number of real roots):
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.
Proof method: Do an induction on k and use Rolle's theorem.
We have a sum of k terms: $f(X) = \sum_{i=1}^{k} T_i(X)$.
Taking the derivative of f/T_1 removes a term. $\square$

Theorem 2 (identity testing): For fixed k and m,
$f \equiv 0$ can be tested deterministically in polynomial-time.
Remark: The algorithm is non-black-box:
It executes the induction in Theorem 1.

A tractable special case
(joint work with B. Grenet, N. Portier and Y. Strozecki)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.
Theorem 1 (number of real roots):
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.
Proof method: Do an induction on k and use Rolle's theorem.
We have a sum of k terms: $f(X) = \sum_{i=1}^{k} T_i(X)$.
Taking the derivative of f/T_1 removes a term. $\square$

Theorem 2 (identity testing): For fixed k and m,
$f \equiv 0$ can be tested deterministically in polynomial-time.
Remark: The algorithm is non-black-box:
It executes the induction in Theorem 1.

A lower bound for restricted depth 4 circuits, or: the limited power of powering.

Consider representations of the permanent of the form:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X) \qquad (1)$$

where

- X is a $n \times n$ matrix of indeterminates.
- k and m are bounded, and the α_{ij} are of polynomial bit size.
- The f_j are polynomials in n^2 variables,
  with at most t monomials.

Theorem 3 (lower bound):
No such representation if t is polynomially bounded in n.
Remark: The point is that the α_{ij} may be nonconstant.
Otherwise, the number of monomials in (1) is polynomial in t.

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \qquad (2)$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x-i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and Theorem 1, P_n should have only $n^{O(1)}$ real roots. But P_n has 2^n integer roots!

Remark:

The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \tag{2}$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x - i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and Theorem 1, P_n should have only $n^{O(1)}$ real roots.
  But P_n has 2^n integer roots!

Remark:
The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \tag{2}$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x - i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and Theorem 1, P_n should have only $n^{O(1)}$ real roots.
  But P_n has 2^n integer roots!

Remark:
The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).

Bürgisser's result: a proof sketch (1/4)

Goal: If permanent is easy,

then $g_n(X) = \prod_{i=1}^{2^n-1}(X+i)$ has polynomial size circuits.

Remark: Using assumption, to show that a polynomial family is easy to compute we only have to put it in VNP.

Valiant's criterion: Let

$$f_n(x_1, \ldots, x_{p(n)}) = \sum_{i=0}^{2^{p(n)}-1} a_n(i) x_1^{i_1} \cdots x_{p(n)}^{i_{p(n)}}.$$

If $a : (1^n, i) \mapsto a_n(i) \in \{0, 1\}$ is in P/poly then $(f_n) \in \text{VNP}$.

Bürgisser's result: a proof sketch (1/4)

Goal: If permanent is easy,

then $g_n(X) = \prod_{i=1}^{2^n-1}(X+i)$ has polynomial size circuits.

Remark: Using assumption, to show that a polynomial family is easy to compute we only have to put it in VNP.

Valiant's criterion: Let

$$f_n(x_1,\ldots,x_{p(n)}) = \sum_{i=0}^{2^{p(n)}-1} a_n(i) x_1^{i_1} \cdots x_{p(n)}^{i_{p(n)}}.$$

If $a : (1^n, i) \mapsto a_n(i) \in \{0,1\}$ is in P/poly then $(f_n) \in \text{VNP}$.

Proof sketch (2/4)

The counting hierarchy: $C_0p = P$; $C_1P = PP$ where $A \in PP$ iff there exists a polynomial p and $B \in P$ such that for $|x| = n$:

$$x \in A \Leftrightarrow |\{y \in \{0,1\}^{p(n)};\ \langle x, y\rangle \in B\}| > 2^{p(n)-1}.$$

$C_2p = PP^{PP}$, $C_3P = PP^{C_2P}$,...

If the permanent is easy to compute then $CH \subseteq P/poly$ (asumes GRH if circuits can use arbitrary constants).

Proof sketch (2/4)

The counting hierarchy: $C_0p = P$; $C_1P = PP$ where $A \in PP$ iff there exists a polynomial p and $B \in P$ such that for $|x| = n$:

$$x \in A \Leftrightarrow |\{y \in \{0,1\}^{p(n)};\ \langle x, y\rangle \in B\}| > 2^{p(n)-1}.$$

$C_2p = PP^{PP}$, $C_3P = PP^{C_2P}, \ldots$
If the permanent is easy to compute then $CH \subseteq P/poly$ (asumes GRH if circuits can use arbitrary constants).

Proof sketch (3/4)

Expand product: $g_n(X) = \prod_{i=1}^{2^n-1}(X+i) = \sum_{\alpha=0}^{2^n-1} a_n(\alpha)X^\alpha$.

Binary expansion: $a_n(\alpha) = \sum_{i=0}^{2^{c.n}-1} a_n(i,\alpha)2^i$.

Hence:

$$\begin{aligned} g_n &= \sum_{\alpha=0}^{2^n-1}\sum_{i=0}^{2^{c.n}-1} a_n(i,\alpha)2^i X^\alpha \\ &= h_n(X^{2^0}, X^{2^1}, \ldots, X^{2^{n-1}}, 2^{2^0}, 2^{2^1}, \ldots, 2^{2^{c\cdot n-1}}) \end{aligned}$$

where $h_n(X_1,\ldots,X_n,Z_1,\ldots,Z_{c\cdot n})$ is the multilinear polynomial

$$\sum_\alpha \sum_i a_n(i,\alpha)X_1^{\alpha_1}\cdots X_{\cdot n}^{\alpha_{c\cdot n}} Z_1^{i_1}\cdots Z_{c\cdot n}^{i_{c\cdot n}}.$$

We would like to apply Valiant's criterion...

Proof sketch (3/4)

Expand product: $g_n(X) = \prod_{i=1}^{2^n-1}(X+i) = \sum_{\alpha=0}^{2^n-1} a_n(\alpha)X^\alpha$.

Binary expansion: $a_n(\alpha) = \sum_{i=0}^{2^{c.n}-1} a_n(i,\alpha)2^i$.

Hence:

$$\begin{aligned} g_n &= \sum_{\alpha=0}^{2^n-1}\sum_{i=0}^{2^{c.n}-1} a_n(i,\alpha)2^i X^\alpha \\ &= h_n(X^{2^0}, X^{2^1}, \ldots, X^{2^{n-1}}, 2^{2^0}, 2^{2^1}, \ldots, 2^{2^{c\cdot n-1}}) \end{aligned}$$

where $h_n(X_1, \ldots, X_n, Z_1, \ldots, Z_{c\cdot n})$ is the multilinear polynomial

$$\sum_\alpha \sum_i a_n(i,\alpha) X_1^{\alpha_1} \cdots X_{\cdot n}^{\alpha_{c\cdot n}} Z_1^{i_1} \cdots Z_{c\cdot n}^{i_{c\cdot n}}.$$

We would like to apply Valiant's criterion...

Proof sketch (3/4)

Expand product: $g_n(X) = \prod_{i=1}^{2^n-1}(X+i) = \sum_{\alpha=0}^{2^n-1} a_n(\alpha)X^\alpha$.

Binary expansion: $a_n(\alpha) = \sum_{i=0}^{2^{c.n}-1} a_n(i,\alpha)2^i$.

Hence:

$$\begin{aligned} g_n &= \sum_{\alpha=0}^{2^n-1}\sum_{i=0}^{2^{c.n}-1} a_n(i,\alpha)2^i X^\alpha \\ &= h_n(X^{2^0}, X^{2^1}, \ldots, X^{2^{n-1}}, 2^{2^0}, 2^{2^1}, \ldots, 2^{2^{c\cdot n-1}}) \end{aligned}$$

where $h_n(X_1,\ldots,X_n,Z_1,\ldots,Z_{c\cdot n})$ is the multilinear polynomial

$$\sum_\alpha\sum_i a_n(i,\alpha)X_1^{\alpha_1}\cdots X_{\cdot n}^{\alpha_{c\cdot n}} Z_1^{i_1}\cdots Z_{c\cdot n}^{i_{c\cdot n}}.$$

We would like to apply Valiant's criterion...

Proof sketch (4/4)

Recall: $h_n = \sum_\alpha \sum_i a_n(i,\alpha) X_1^{\alpha_1} \cdots X_n^{\alpha_n} Z_1^{i_1} \cdots Z_{c\cdot n}^{i_{c\cdot n}}$.
Theorem: The $a_n(i,\alpha)$ can be computed in CH (Bürgisser).
Proof: based on constant-depth threshold circuits
for iterated multiplication.□
From assumption: CH $\subseteq$ P/poly.
Hence $(h_n) \in$ VNP (Valiant's criterion), but VP $=$ VNP.
Substitution of powers 2^{2^i} and X^{2^j} in $h_n \Rightarrow$
polynomial size circuits for $\prod_{i=1}^{2^n-1}(X+i)$.□
Corollary:
Reduction to depth 4 for $h_n \Rightarrow$ SPS polynomial of size $2^{o(n)}$ for g_n.

Proof sketch (4/4)

Recall: $h_n = \sum_\alpha \sum_i a_n(i,\alpha) X_1^{\alpha_1} \cdots X_n^{\alpha_n} Z_1^{i_1} \cdots Z_{c\cdot n}^{i_{c\cdot n}}$.
Theorem: The $a_n(i,\alpha)$ can be computed in CH (Bürgisser).
Proof: based on constant-depth threshold circuits
for iterated multiplication.$\square$
From assumption: CH $\subseteq$ P/poly.
Hence $(h_n) \in$ VNP (Valiant's criterion), but VP $=$ VNP.
Substitution of powers 2^{2^i} and X^{2^j} in $h_n \Rightarrow$
polynomial size circuits for $\prod_{i=1}^{2^n-1} (X+i)$.$\square$

Corollary:
Reduction to depth 4 for $h_n \Rightarrow$ SPS polynomial of size $2^{o(n)}$ for g_n.

Proof sketch (4/4)

Recall: $h_n = \sum_\alpha \sum_i a_n(i,\alpha) X_1^{\alpha_1} \cdots X_n^{\alpha_n} Z_1^{i_1} \cdots Z_{c\cdot n}^{i_{c\cdot n}}$.
Theorem: The $a_n(i,\alpha)$ can be computed in CH (Bürgisser).
Proof: based on constant-depth threshold circuits
for iterated multiplication.$\square$
From assumption: CH $\subseteq$ P/poly.
Hence $(h_n) \in$ VNP (Valiant's criterion), but VP $=$ VNP.
Substitution of powers 2^{2^i} and X^{2^j} in $h_n \Rightarrow$
polynomial size circuits for $\prod_{i=1}^{2^n-1} (X+i)$.$\square$

Corollary:
Reduction to depth 4 for $h_n \Rightarrow$ SPS polynomial of size $2^{o(n)}$ for g_n.

To Be Done...

- Real τ-conjecture: prove or disprove.
- Some special cases:
  - $k = 2$: how many real solutions to $f_1 \cdots f_m = g_1 \cdots g_m$?
  - An even simpler question
    (courtesy of Arkadev Chattopadhyay):
    how many real solutions to $fg = 1$?
    Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.
- What about random polynomials ?
  Encouraging experimental results by Stefan Mengel.
- Instead of real roots, bound the number of p-adic roots ?

To Be Done...

- Real τ-conjecture: prove or disprove.
- Some special cases:
  - $k = 2$: how many real solutions to $f_1 \cdots f_m = g_1 \cdots g_m$?
  - An even simpler question
    (courtesy of Arkadev Chattopadhyay):
    how many real solutions to $fg = 1$?
    Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.
- What about random polynomials ?
  Encouraging experimental results by Stefan Mengel.
- Instead of real roots, bound the number of p-adic roots ?

To Be Done...

- Real τ-conjecture: prove or disprove.
- Some special cases:
  - $k = 2$: how many real solutions to $f_1 \cdots f_m = g_1 \cdots g_m$?
  - An even simpler question
    (courtesy of Arkadev Chattopadhyay):
    how many real solutions to $fg = 1$?
    Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.
- What about random polynomials ?
  Encouraging experimental results by Stefan Mengel.
- Instead of real roots, bound the number of p-adic roots ?

To Be Done...

- Real τ-conjecture: prove or disprove.
- Some special cases:
  - $k = 2$: how many real solutions to $f_1 \cdots f_m = g_1 \cdots g_m$?
  - An even simpler question
    (courtesy of Arkadev Chattopadhyay):
    how many real solutions to $fg = 1$?
    Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.
- What about random polynomials ?
  Encouraging experimental results by Stefan Mengel.
- Instead of real roots, bound the number of p-adic roots ?

To Be Done...

- Real τ-conjecture: prove or disprove.
- Some special cases:
  - $k = 2$: how many real solutions to $f_1 \cdots f_m = g_1 \cdots g_m$?
  - An even simpler question
    (courtesy of Arkadev Chattopadhyay):
    how many real solutions to $fg = 1$?
    Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.
- What about random polynomials ?
  Encouraging experimental results by Stefan Mengel.
- Instead of real roots, bound the number of p-adic roots ?

Constant-free version of Valiant's model

- Work with constant-free circuits (1 is the only constant).
- $(f_n) \in \mathsf{VP}^0$ if size and *formal degree* of circuits are polynomially bounded (Malod, 2003).
  Formal degree is an upper bound on $\deg(f_n)$:
  1. 1 for an input gate (variable or constant).
  2. Max of formal degrees of two inputs for $+, -$ gate.
  3. Sum of formal degrees for $\times$ gate.
- New goal: $\mathrm{PER}(X) \notin \mathsf{VP}^0$.