Lower bounds for “explicit” and “non-explicit” polynomials

Sylvain Perifel (LIAFA, Paris)

Budapest – July 6, 2011

Introduction

- How many operations $+$ and $\times$ are necessary to compute a polynomial?
- Baur and Strassen (1983):
  $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ operations.

Introduction

- How many operations $+$ and $\times$ are necessary to compute a polynomial?
- Baur and Strassen (1983):
  $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ operations.
- Raz: no better lower bound for "explicit" polynomials?

Introduction

- How many operations $+$ and $\times$ are necessary to compute a polynomial?
- Baur and Strassen (1983):
  $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ operations.
- Raz: no better lower bound for "explicit" polynomials?
- Lower bounds for bad reasons:
  - $p(x_0, \ldots, x_s) = \sum_{i=0}^{s} x_i$ requires $\geq s$ operations;

Introduction

- How many operations $+$ and $\times$ are necessary to compute a polynomial?
- Baur and Strassen (1983):
  $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ operations.
- Raz: no better lower bound for "explicit" polynomials?
- Lower bounds for bad reasons:
  - $p(x_0, \ldots, x_s) = \sum_{i=0}^{s} x_i$ requires $\geq s$ operations;
  - $p(x) = x^{2^s}$ requires $\geq s$ operations;

Introduction

- How many operations $+$ and $\times$ are necessary to compute a polynomial?
- Baur and Strassen (1983):
  $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ operations.
- Raz: no better lower bound for "explicit" polynomials?
- Lower bounds for bad reasons:
  - $p(x_0, \ldots, x_s) = \sum_{i=0}^{s} x_i$ requires $\geq s$ operations;
  - $p(x) = x^{2^s}$ requires $\geq s$ operations;
  - $p(x) = \sum_{i=1}^{s} \alpha_i x^i$, where the α_i are algebraically independent, requires $\geq s$ operations.

Introduction

- How many operations $+$ and $\times$ are necessary to compute a polynomial?

- Baur and Strassen (1983):
  $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^d$ requires $\Omega(n \log d)$ operations.

- Raz: no better lower bound for "explicit" polynomials?

- Lower bounds for bad reasons:
  - $p(x_0, \ldots, x_s) = \sum_{i=0}^{s} x_i$ requires $\geq s$ operations;
  - $p(x) = x^{2^s}$ requires $\geq s$ operations;
  - $p(x) = \sum_{i=1}^{s} \alpha_i x^i$, where the α_i are algebraically independent, requires $\geq s$ operations.

  Remark: in the computations, arbitrary constants from $\mathbb{C}$ can be used.

Precise question

For all s, find an explicit polynomial:

- $p \in \mathbb{Z}[x]$ (one variable);
- coefficients in $\{0, 1\}$;
- degree polynomial in s

such that computing p requires $\geq s$ operations.

Precise question

For all k, find an explicit family of polynomials (p_n):

- $p_n \in \mathbb{Z}[x]$ (one variable);
- coefficients of p_n in $\{0, 1\}$;
- degree of p_n polynomial in n

such that computing p_n requires $\geq n^k$ operations.

Precise question

For all k, find an explicit family of polynomials (p_n):

- $p_n \in \mathbb{Z}[x]$ (one variable);
- coefficients of p_n in $\{0, 1\}$;
- degree of p_n polynomial in n

such that computing p_n requires $\geq n^k$ operations.

Remarks:

- example of a family (p_n): $\quad p_n(x) = \sum_{i=0}^{n} x^i$;
- arbitrary constants from $\mathbb{C}$ can be used.

Precise question

For all k, find an explicit family of polynomials (p_n):

- $p_n \in \mathbb{Z}[x]$ (one variable);
- coefficients of p_n in $\{0, 1\}$;
- degree of p_n polynomial in n

such that computing p_n requires $\geq n^k$ operations.

Remarks:

- example of a family (p_n): $\quad p_n(x) = \sum_{i=0}^{n} x^i$;
- arbitrary constants from $\mathbb{C}$ can be used.

$\rightarrow$ What does “explicit” mean?

Outline

1. Non-explicit polynomials

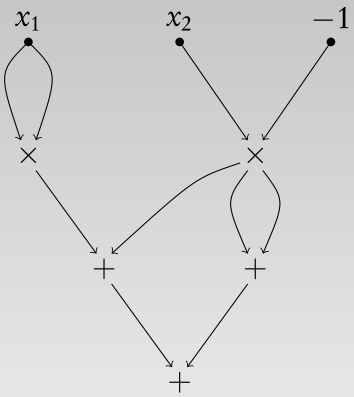
2. Explicit polynomials

Outline

1. Non-explicit polynomials

2. Explicit polynomials

Arithmetic circuits



- Directed acyclic graph
- Inputs labeled x_i or $\alpha \in \mathbb{C}$
- Gates labeled $+$ or $\times$
- One output
- Size = number of vertices
  = number of operations
- Aka SLP
  (straight-line program)

Lipton and Schnorr

Based on works of Strassen (1974) and Lipton (1975):

Theorem (Schnorr, 1978)

For all k, there exist polynomials $p_n(x)$:

- one variable x;
- coefficients in $\{0, 1\}$;
- degree $O(n^{2k})$

such that p_n has no circuits of size $\leq n^k$
(even using arbitrary constants from $\mathbb{C}$).

Idea of the proof

- The coefficients of $p(x)$ are polynomials in the "description" of the circuit for p

Idea of the proof

- The coefficients of $p(x)$ are polynomials in the "description" of the circuit for p
- thus there exists a polynomial H_s such that:

  if $p(x) = \sum_{i=0}^{d} \alpha_i x^i$ is computed by a circuit of size s

  then $H_s(\alpha_0, \ldots, \alpha_d) = 0$.

Idea of the proof

- The coefficients of $p(x)$ are polynomials in the "description" of the circuit for p
- thus there exists a polynomial H_s such that:

  if $p(x) = \sum_{i=0}^{d} \alpha_i x^i$ is computed by a circuit of size s

  then $H_s(\alpha_0, \ldots, \alpha_d) = 0$.
- Hence, if $(\beta_0, \ldots, \beta_d)$ is not a root of H_s,

  then $p(x) = \sum_i \beta_i x^i$ does not have circuits of size s. $\square$

Expliciteness

- Existence result: non explicit.
- Coefficients computable in exponential time.

Expliciteness

- Existence result: non explicit.
- Coefficients computable in exponential time.

- Expliciteness: coefficients computable efficiently

$\rightarrow$ Can we do better than exponential time?

Outline

1. Non-explicit polynomials

2. Explicit polynomials

Expliciteness

Family of polynomials $p_n(x) = \sum_{i=0}^{n^k} \alpha_i x^i$,
coefficients $\alpha_i \in \{0, 1\}$.

- Strongest notion of expliciteness:
  $i \mapsto \alpha_i$ computable in time polynomial in n

Expliciteness

Family of polynomials $p_n(x) = \sum_{i=0}^{n^k} \alpha_i x^i$,
coefficients $\alpha_i \in \{0, 1\}$.

- Strongest notion of expliciteness:
  $i \mapsto \alpha_i$ computable in time polynomial in n
- Other notion of interest: coefficients in $\sharp\mathsf{P}$

  $\to$ polynomial in "uniform-VNP^0"
  = the complexity of the permanent:

$$\operatorname{per}_n(x_{1,1}, \ldots, x_{n,n}) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

Diagonalisation

Can we use diagonalisation?

Diagonalisation

Can we use diagonalisation?

Problem: arbitrary constants from $\mathbb{C}$!
(no counting argument possible)

Idea: go to finite fields.

THEOREM (Koiran 1996, Bürgisser 2000)

Assuming GRH,

if a system of polynomial equations with integer coefficients has a solution over $\mathbb{C}$

then it has a solution over $\mathbb{Z}/r\mathbb{Z}$ for "small" r.

(if $\#\text{eq} = 2^n$, $\#\text{var} = n$, coef$\leq 2^{2^n}$ and degree$\leq 2^n$ then $r \leq 2^{n^c}$)

Application

- Polynomial $p(x) = \sum \alpha_i x^i$ computed by a circuit C with constants $\beta_1, \ldots, \beta_m$: $\quad C(x, \bar{\beta}) = p(x)$
- The system: equations in $\bar{y}$

$$C(i, \bar{y}) = p(i) \quad \text{for } 0 \leq i \leq 2^n$$

Application

- Polynomial $p(x) = \sum \alpha_i x^i$ computed by a circuit C with constants $\beta_1, \ldots, \beta_m$: $\quad C(x, \bar{\beta}) = p(x)$
- The system: equations in $\bar{y}$

$$C(i, \bar{y}) = p(i) \quad \text{for } 0 \leq i \leq 2^n$$

- Solution over $\mathbb{C}$ (the constants $\bar{\beta}$) $\Longrightarrow$ solution over $\mathbb{Z}/r\mathbb{Z}$
- the new constants $\bar{\gamma}$ are now $\in \{0, \ldots, r-1\}$ and the values $C(i, \bar{\gamma})$ coincide with $p(i)$ for $i \in \{0, \ldots, 2^n\}$.

Application

- Polynomial $p(x) = \sum \alpha_i x^i$ computed by a circuit C
  with constants $\beta_1, \dots, \beta_m$: $\quad C(x, \bar{\beta}) = p(x)$
- The system: equations in $\bar{y}$

$$C(i, \bar{y}) = p(i) \quad \text{for } 0 \leq i \leq 2^n$$

- Solution over $\mathbb{C}$ (the constants $\bar{\beta}$) $\Longrightarrow$ solution over $\mathbb{Z}/r\mathbb{Z}$
- the new constants $\bar{\gamma}$ are now $\in \{0, \dots, r-1\}$ and
  the values $C(i, \bar{\gamma})$ coincide with $p(i)$ for $i \in \{0, \dots, 2^n\}$.
- Counting argument:
  existence of a polynomial with no circuits of size n^k.

Complexity

- Computing the coefficients $\bar{\alpha}$ in PH:

$$\exists \bar{\alpha} \quad \forall r,\ \forall C,\ \forall \bar{\gamma} \in \mathbb{Z}/r\mathbb{Z} \quad C(x, \bar{\gamma}) \not\equiv \sum \alpha_i x^i.$$

- "Almost" in $\sharp$P due to Toda's theorem (PH $\subseteq$ P$^{\sharp\mathsf{P}}$)

Complexity

- Computing the coefficients $\bar{\alpha}$ in PH:

$$\exists \bar{\alpha} \quad \forall r,\ \forall C,\ \forall \bar{\gamma} \in \mathbb{Z}/r\mathbb{Z} \quad C(x, \bar{\gamma}) \not\equiv \sum \alpha_i x^i.$$

- "Almost" in $\sharp$P due to Toda's theorem ($\mathsf{PH} \subseteq \mathsf{P}^{\sharp\mathsf{P}}$)

$\rightarrow$ Can we make it really in $\sharp$P?