COMPLEXITY OF COMPUTATION OF POLYNOMIALS

S. B. GASHKOV, I. S. SERGEEV
Lomonosov Moscow State University
PTK conference (Nizhny Novgorod, 2011)

I. CLASSIC RESULTS

i.1 Computation of real polynomials in the complete arithmetic basis $A = \{+,\times,\boldsymbol{R}\}$

To compute a polynomial of degree n, there are sufficient:

n additive operations

$n/2+O(1)$ multiplications

$\Omega(n^{1/2})$ nonscalar operations

These bounds are tight (Motzkin, Pan, Belaga 1950s; Paterson, Stockmeyer 1973)

I. CLASSIC RESULTS

i.2 Method to compute a polynomial by $n/2+O(\log n)$ multiplications (due to Winograd)

Idea: let $f(x)$ be a monic polynomial of degree $2^{k+1} - 1$

Then, $$f(x) = (x^{2^k} + a)\, f_0(x) + f_1(x), \qquad (1)$$

where $f_0(x), f_1(x)$ are monic polynomials of degree $2^k - 1$

Apply (1) to $f_0(x), f_1(x)$ etc.

Verify: (a) necessary powers $x^{2^k}, x^{2^{k-1}}, \dots, x^2$ may be computed by k multiplications (via an addition chain);

(b) after they are computed, any intermediate polynomial of degree $2^m - 1$ can be computed by $2^{m-1} - 1$ multiplications (obvious from (1))

I. CLASSIC RESULTS

i.3 Method to compute a polynomial by $2n^{1/2}$ nonscalar multiplications

Idea: represent a polynomial $f(x)$ of degree $rs - 1$ as

$$f(x) = (\ldots((f_0(x)\, x^r + f_1(x))\, x^r + \ldots)\, x^r + f_{s-1}(x), \qquad (2)$$

(Horner's scheme) where $f_k(x)$ are polynomials of degree $r - 1$

(a) powers $x^2, x^3, \ldots, x^r$ are computable by $r - 1$ nonscalar multiplications; polynomials $f_k(x)$ are obtained as linear combinations of these powers;

(b) to finalize computations according to (2), it suffices to implement $s - 1$ more multiplications by x^r

I. CLASSIC RESULTS

i.4 Efficient lower bounds

In 70-90s, Straßen and his students (von zur Gathen, Heintz, Schnorr, Stoß, Baur, Halupczok, and also Sieveking, van de Wiele) constructed "explicit" polynomials of almost maximal possible complexity. Usually, the coefficients of such polynomials are algebraically independent real numbers or rapidly growing rational numbers. Examples of hard-to-compute polynomials:

$$\sum p_i^{1/2} x^i \qquad \sum 2^{2^i} x^i \qquad \sum i^r x^i$$

Here: $p_i \in \boldsymbol{P}$, $r \in \boldsymbol{Q} / \boldsymbol{Z}$

I. CLASSIC RESULTS

i.5 *Kronecker substitution*

$$x_i = x^{2^i}$$

implements a one-to-one correspondence between single variable polynomials of degree $2^n - 1$ and *multilinear* (i.e. linear in every variable) polynomials of n variables.

Thus, if $f(x)$ corresponds to $g(x_0, \dots, x_{n-1})$, then

$$L(f) \le L(g) + n - 1$$

II. MONOTONE COMPLEXITY

ii.1 Consider monotone polynomials, i.e. those with nonnegative real coefficients, and the complexity of computation over the monotone arithmetic basis $A_+ = \{+, \times, \boldsymbol{R}_+\}$. Important problem is to construct hard-to-compute polynomials with coefficients 0, 1.

ii.2 Subexponential lower bounds

The first supepolynomial lower bound was obtained for the characteristic polynomial of a k-clique in a graph:

$$CL_{n,k} = \sum_{1 \le i_1 < \ldots < i_k \le n} \prod_{1 \le s < t \le k} x_{i_s, i_t}$$

$$L_+(CL_{n,k}) \ge C_n^k - 1\,, \quad \text{in particular,} \quad L_+(CL_{n,n/2}) \ge 2^{n/2-o(n)}$$

Schnorr 1976

II. MONOTONE COMPLEXITY

Besides Schnorr, size $2^{\Omega(n)}$ lower bounds for various multilinear polynomials of $n^{O(1)}$ variables were obtained by Valiant, Jerrum, Snir in 80s

ii.3 Exponential lower bounds

$2^{n/2} - 1$	Kasim-Zade 1983
$\Omega(2^{2n/3})$	Gashkov 1987
$2^{n-o(n)}$	Gashkov, Sergeev 2010

(further in more details)

III. THIN SETS METHOD

iii.1 *DEF*. A subset M of a commutative semigroup $(G, +)$ is (k, l)-thin, where $k \leq l$, if for any subsets $A, B \subset G$ satisfying $|A|=k$ and $|B|=l$, it holds that

$$A \times B = \{ a+b \mid a \in A, b \in B \} \not\subset M$$

In the case $k=l$, the shortening k-thin is used.

Example: Subset $\{0, 1, 3\} \subset (\mathbf{Z}_7, +)$ is 2-thin

DEF. Let f be a polynomial in n variables. Then

mon $f \subset (\mathbf{N} \cup \{0\})^n$ is a set of vectorial degrees of its monomials.

III. THIN SETS METHOD

iii.2 MAIN THEOREM

Let $k \geq 1$, and mon f be a (k, l)-thin subset in $(\boldsymbol{N} \cup \{0\})^n$,

$L_+(f)$ – additive monotone complexity of f,

$L_\times(f)$ – multiplicative monotone complexity of f,

$\alpha(k)$ – maximal number of boolean vectors of length $k - 1$, neither of them is a disjunction of some others.

Set $h = \min \{ (k-1)^3, (l-1)^2 \}$.

Then: (i) $L_+(f) \geq h^{-1} \, |\, \mathrm{mon}\, f \,| - 1$

(ii) $L_\times(f) \geq C_{k,l} \, |\, \mathrm{mon}\, f \,|^{\alpha(k)/(2\alpha(k)-1)} - n - 2$

In particular, $L_\times(f) = \Omega(|\, \mathrm{mon}\, f \,|^{2/3})$ for $k=l=2$

and $L_\times(f) = \Omega(|\, \mathrm{mon}\, f \,|^{3/5})$ for $k=l=3$.

These bounds are tight — Gashkov 1987

III. THIN SETS METHOD

iii.3 Examples of dense 2- and 3-thin sets

1. 2-thin subsets in $\boldsymbol{Z}_n$ of size $\sim n^{1/2}$:

<u>*V.E. Alexeev set*</u> 1979:

Let $n=p(p-1)$, $p\in\boldsymbol{P}$, ζ be a generator of the multiplicative group of the field $\boldsymbol{Z}_p$. Then

$M = \{ s_i \mid i = 0, \dots, p\text{-}2 \}$, where $s_i \equiv i \bmod (p\text{-}1)$, $s_i \equiv \zeta^i \bmod p$

<u>*Singer set*</u> 1938:

Let $n=q^2+q+1$, q be a prime power, θ be a primitive element in the field $GF(q^3)$. Denote $GF(q) = \{ \zeta_1, \dots, \zeta_q \}$. Then

$$M = \{0\} \cup \{ s_i \mid \theta^{s_i} / (\theta + \zeta_i) \in GF(q),\ i=1, \dots, q \}$$

III. THIN SETS METHOD

DEF. $E_m = \{ 0, \dots, m\text{-}1 \}$.

2. 2-thin subsets $E_m{}^n$ of size $\sim m^{n/2}$:

Let $q = p^k$, $p \in \boldsymbol{P} \setminus \{2\}$. Then

$$M = \{ (x, x^2) \mid x \in GF(q) \} \subset GF(q^2) \to E_p{}^{2k}$$

Lindström set 1969: Let $q = 2^k$. Then

$$M = \{ (x, x^3) \mid x \in GF(q) \} \subset GF(q^2) \to E_2{}^{2k}$$

3. 3-thin subsets $E_m{}^n$ of size $\sim m^{2n/3}$:

Brown set 1966:

Let $q = p^k$, $p \in \boldsymbol{P} \setminus \{2\}$, γ be a quadratic nonresidue in $GF(q)$. Then

$$M = \{ (x, y, z) \mid x^2 + y^2 + z^2 = -\gamma,\ x, y, z \in GF(q) \} \subset GF(q^3) \to E_p{}^{3k}$$

III. THIN SETS METHOD

iii.4 Corollaries for the complexity of polynomials

There is an explicit polynomial f in n variables of degree at most $m - 1$ in each variable, such that (under some restrictions on m and n)

$$L_+(f) \geq (1 - o(1))m^{n/2} \qquad L_\times(f) \geq (2 - o(1))m^{n/3}$$

(if mon f is an appropriate 2-thin set), or

$$L_+(f) \geq (1/8 - o(1))m^{2n/3} \qquad L_\times(f) \geq (2^{-4/5} - o(1))m^{2n/5}$$

(if mon f is an appropriate 3-thin set)

(in examples by Schnorr and Kasim-Zade: 2-thin sets)

III. THIN SETS METHOD

Fact (Erdös, Spencer 1974): any (k, l)-thin subset $M \subset E_m^{\ n}$ has cardinality $O_{k,\,l}(m^{n(1-1/k)})$

iii.5 Thin sets of extreme density

Kollár-Rónyai-Szabó set 1996:

In the group $(GF(q^t), +)$, the set of elements of the norm 1

$$M = \{\, x \mid x^{(q^t-1)/(q-1)} = 1,\ x \in GF(q^t) \,\}$$

is a $(t, t!+1)$-thin subset of cardinality $(q^t - 1)/(q - 1)$.

III. THIN SETS METHOD

iii.6 LEMMA 1

Let $\psi_{s,\,t,\,m}: E_m^{\,st} \to E^{\,s}_{(2m\text{-}1)^t}$ be one-to-one mapping:

$$\psi_{s,\,t,\,m}(\ \dots,\ a_{it},\ \dots,\ a_{it+t\text{-}1},\ \dots\ ) = (\ \dots,\ [\ a_{it},\ \dots,\ a_{it+t\text{-}1}\ ]_{2m\text{-}1},\ \dots\ ) \quad *$$

If $M \subset E_m^{\,st}$ is a (k, l)-thin subset, then

$\psi_{s,\,t,\,m}(M) \subset E^{\,s}_{(2m\text{-}1)^t}$ is also (k, l)-thin subset.

* $[\ a_k,\ \dots,\ a_0\ ]_m = (\dots(a_k\, m + a_{k\text{-}1})m + \dots\ )m + a_0$ (representation of a number in the numeric system with base m)

III. THIN SETS METHOD

iii.7 MAIN COROLLARY (from the main theorem and technical theorem 1)

Let $m \geq 2$ and $n \geq 1$. There exists an explicit polynomial f in n variables of degree at most $m - 1$ in each variable, such that as $m^n \to \infty$,

$$L_+(f) \geq m^{n(1 - o(1))} \qquad L_\times(f) \geq m^{n(1/2 - o(1))}$$

Both bounds are tight in the form they are written.

IV. MONOTONE AND NONMONOTONE COMPLEXITY

iv.1 Examples of separations: complexity $L(f)$ over the complete basis $A = \{+,\times,\boldsymbol{R}\}$ vs the complexity $L_M(f)$ over the monotone basis $A_+ = \{+,\times,\boldsymbol{R}_+\}$

f – multilinear polynomials in n variables:

$L(f) = n^{O(1)}$ $\quad L_M(f) \geq c^{\,n^{1/2}}$ — Valiant 1979

$L(f) = n^{O(1)}$ $\quad L_M(f) \geq c^{\,n}$ — Kasim-Zade 1983

$L_M(f) \,/\, L(f) = n^{\Omega(1)}$ $\quad \deg f = 3$ — Schnorr 1976

$L_M(f) \,/\, L(f) \geq 2^{n(1/2-o(1))}$ — Gashkov, Sergeev 2010

$L_M(f) \,/\, L(f) = n^{1-o(1)}$ $\quad \deg f = 2$ — Gashkov, Sergeev 2010

IV. MONOTONE AND NONMONOTONE COMPLEXITY

iv.2 One more way to build a thin set

DEF. A boolean matrix is (k, l)-thin, if it does not contain all-1 submatrices of size $k \times l$

LEMMA 2

Let $M_1 = \{ a_1, \ldots, a_r \}$ and $M_2 = \{ b_1, \ldots, b_r \}$ be k-thin subsets of $E_m^{\ n}$, and $(\mu_{i,j})$ be an l-thin matrix of size $r \times r$. Then,

(i) $$M = \{ (a_i , b_j) \mid \mu_{i,j} = 1 \} \subset E_m^{\ 2n}$$

(ii) $$M = \{ a_i + (2m-1)\, b_j \mid \mu_{i,j} = 1 \} \subset E^{\ n}_{\ m2}$$

– $((k-1)(l-1)+1)$-thin subsets

Property: $L(f_M) \le L(f_{a_1}, \ldots, f_{a_r}, f_{b_1}, \ldots, f_{b_r}) + L(\mu_{i,j}) + O(\log m)$, where $M = \mathrm{mon}\, f_M$, and $L(\mu_{i,j})$ is the complexity of a linear map

IV. MONOTONE AND NONMONOTONE COMPLEXITY

COROLLARY (from lemma 1 and the construction by Kóllar, Rónyai, Szabó)

There is an explicit $n^{o(1)}$-thin circulant matrix of size $n \times n$ and weight $n^{2-o(1)}$

COROLLARY (from lemma 2)

Let f be a polynomial with coefficients 0 and 1 such that $M = \mathrm{mon}\, f$. Let $(\mu_{i,j})$ be a $r^{\,o(1)}$ –thin circulant matrix, and $k = r^{\,o(1)}$, and either $n \log m = r^{\,o(1)}$, or $\deg f = r^{\,o(1)}$. Then,

$$L_M(f)=\Omega(r^{\,2-o(1)}) \qquad\qquad L(f) \le r^{\,1+o(1)}$$

IV. MONOTONE AND NONMONOTONE COMPLEXITY

iv.3 COROLLARY (on the monotone/nonmonotone complexity separation)

Let $m \geq 2$ and $n \geq 1$. There exists an explicit polynomial f in n variables of degree at most $m - 1$ in each variable, such that as $m^n \to \infty$,

$$L_M(f) \,/\, L(f) \geq m^{\,n\,(1/2\,-\,o(1))}$$

iv.4 Example of a polynomial of degree 2

Пусть $(\mu_{i,j})$ be a $n^{o(1)}$-thin circulant matrix of size $n \times n$ and weight $n^{2-o(1)}$. Define

$$f = \sum_{1 \leq i < j \leq n} \mu_{i,j}\, x_i\, y_j$$

Then, $L_M(f) \,/\, L(f) = n^{1-o(1)}$