Lower Bounds for the Number of Zeros of Multivariate Polynomials over $GF[q]$

Dima Grigoriev
Steklov Mathematical Institute
Fontanka 27, St. Petersburg, Russia
and
Max-Planck Institute of Mathematics
5300 Bonn 1

Marek Karpinski *
Dept. of Computer Science
University of Bonn
5300 Bonn 1
and
International Computer Science Institute
Berkeley, California

Abstract

We prove lower bounds on the number of zeros of some classes of multivariate polynomials over $GF[q]$ in the function of the number of their terms only. The paper was motivated by some algebraic problems arising from the new randomized approximation techniques of [Karpinski, Luby 91] and [Karpinski, Lhotzky 91] for the number of zeros of polynomials over finite fields.

*Supported in part by the Leibniz Center for Research in Computer Science, by the DFG Grant KA 673/4-1 and by the SERC Grant GR-E 68297

1 Notation and Terminology

Let $f = \sum_I a_I X^I \in GF[q][X_1, \ldots, X_n]$ be t-sparse (the number of monomials bounded by t) polynomial with a nonempty set $G \subset GF[q]^n$ of zeros, denote by $|G|$ the number of zeros. Denote $g = f^{q-1}$. Then g ist at most t^{q-1}-sparse, more precisely $\begin{pmatrix} t+q-2 \\ q-1 \end{pmatrix}$-sparse (number of $q-1$ combinations of t distinct elements).

2 Lower bound for a number of terms in the case of a unique solution

Assume now that g (and also f) has a unique solution. We consider two cases.

2.1 The unique solution is $(0, \ldots, 0)$

For monomial $M = X_1^{i_1} \ldots X_n^{i_n}$ we denote by $supp(M) = \{X_j \mid i_j \neq 0\}$. We claim that for every nonempty set $J \in \{X_1, \ldots, X_n\}$ the monomial $M_J = \prod_{j \in J} X_j^{q-1}$ occurs in g. Assume the contrary and let M_{J_0} do not occur in g. Then

$$1 = \sum_{X_j \in GF[q]\,,\, j \in J_0} g(X_1, \ldots, X_n)|_{X_K = 0\,,\, K \notin J_0}\,.$$

But on the other hand the latter sum vanishes since the only monomial which could give a nonzero contribution in it is M_{J_0} taking into account that for $0 \leq l \leq q-1$

$$\sum_{X \in GF[q]} X^b = \begin{cases} 0 & (q-1) \neq l \\ -1 & (q-1) = l \end{cases}$$

This leads to a contradiction, therefore g contains at least $2^n - 1$ monomials.

2.2 All the coordinates of the unique solution are different from zero

Let us prove first that g does not contain any monomial M with $supp(M) \subsetneqq \{X_1, \ldots, X_n\}$ such that a power X_i^{q-1} occurs in M for a certain i.

Assume the contrary and let M contain the maximal set of powers $\{X_i^{q-1},\ i \in I\}$ for a given $supp(M)$. Consider all the monomials with $supp(M)$ containing the powers X_i^{q-1} for all $i \in I$. Denote the sum of all such monomials by $(\prod_{i\in I} X_i^{q-1})h$ where h is a polynomial in the variables from the set $\{X_j\ ,\ j \in J\} = supp(M) \setminus \{X_i\ ,\ i \in I\}$. There exist $\{x_j \in GF[q]\ ,\ j \in J\}$ such that $h\{x_j\ ,\ j \in J\} \neq 0$. Consider a sum

$$0 = \sum_{X_i \in GF[q]\ ,\ i\in I} g(X_1, \ldots, X_n)|_{X_s=0\ ,\ X_s \notin supp(M);\ X_j=x_j\ ,\ j\in J}$$

On the other hand the latter sum equals to $(\sum_{X_i\in GF[q]\ ,\ i\in I} (\prod_{i\in I} X_i^{q-1}))h(x_j, j \in J) \neq 0$. The obtained contradiction proves the statement.

Now we claim that g contains all the monomials M with the $supp(M) = \{X_1, \ldots, X_n\}$ such that M contains X_i^{q-1} for at least one i. Consider for example, all the monomials containing X_n^{q-1}. Denote by ξ a generator of the cyclic group $GF[q]^*$. Let $(\xi^{j_1^{(0)}}, \ldots, \xi^{j_n^{(0)}})$ be the unique root of g. For $1 \leq i_1, \ldots, i_{n-1} \leq q-1$ denote by $\alpha_{i_1,\ldots,i_{n-1}}$ the coefficient in the monomial $X_1^{i_1} \ldots X_{n-1}^{i^{n-1}} X_n^{q-1}$ in g. Then for any $1 \leq j_1, \ldots, j_{n-1} \leq q-1$ holds

$$\sum_{X_n\in GF[q]} g(X_1, \ldots, X_n)|_{X_1=\xi^{j_1},\ldots,X_{n-1}=\xi^{j_{n-1}}} = -\sum_{1\leq i_1,\ldots,i_{n-1}\leq q-1} \alpha_{i_1,\ldots,i_{n-1}} \xi^{i_1j_1+\ldots+i_{n-1}j_{n-1}}$$

by the proved above. Thus, the latter sums can be written (for different $j_1, \ldots, j_{n-1}$) as a product of the vector $(\alpha_{i_1,\ldots,i_n})_{1\leq i_1,\ldots,i_{n-1}\leq q-1}$ by $(q-1)^{n-1} \times (q-1)^{n-1}$ matrix A being a tensor product of $(n-1)$ copies of $(q-1) \times (q-1)$ matrix (ξ^{ij}) which is a Fourier transform matrix. This product equals to a vector having all zero coordinates except one coordinate equal to -1 (this coordinate corresponds to $j_1 = j_1^{(0)}, \ldots, j_{n-1} = j_{n-1}^{(0)}$). Thus, the vector $(\alpha_{i_1,\ldots,i_n})$ equals to a suitable row of the matrix A^{-1}, being a tensor product of $(n-1)$ copies of the matrix $-(\xi^{-ij})$, hence $\alpha_{i_1,\ldots,i_n} \neq 0$ for each $1 \leq i_1, \ldots, i_n \leq q-1$.

Thus, the number of monomials in g is at least $(q-1)^n - (q-2)^n \leq (q-1)^{n-1}$.

3 The general case of the unique root

Assume that $q > 2$. Suppose without loss of generality that for the unique root $(x_1, \ldots, x_n)$ of g holds $x_1 = \ldots = x_K = 0$, $x_{K+1} \neq 0, \ldots, x_n \neq 0$. Then considering polynomials $g|_{X_1=\ldots=X_K=0}$ and $g|_{X_{K+1}=x_{K+1},\ldots,X_n=x_n}$ and applying cases 2.2) und 2.1), respectively, we conclude that the number of monomials in g exceeds $\max\{(q-1)^{n-K-1}, 2^K - 1\} \geq 2^{n/2} - 1$.

Proof of the lower bound

If $|G| > 1$ there exists a coordinate $1 \leq i_1 \leq n$ whose value is not a constant on G. Fix a certain value x_{i_1} of X_{i_1} for which there are at most $\frac{1}{2}|G|$ solutions in G with this value. Continuing this process, fix $x_{i_1}, \ldots, x_{i_s}$ and after at most $s \leq \log_2 |G|$ steps we come to a unique solution. Applying 3. to a polynomial $g|_{X_{i_1}=x_{i_1},\ldots,X_{i_s}=x_{i_s}}$, we get a lower bound $2^{\frac{1}{2}(n-\log_2|G|)}$ for the number of monomials in g. Hence the initial polynomial f contains at least $2^{\frac{1}{2}((n-\log_2|G|)/(q-1)}$ monomials.

4 Upper bound for a number of roots of a t-sparse polynomial

Let $q = p^s$, where p is a prime. We construct a sequence of elements $a_0, \ldots, a_{N-1} \in GF[q]$ such that $\sum_{i \in I} a_i \neq 0$??? $\emptyset \neq I \subset \{1, \ldots, N\}$. For $s = 1$ we take $a_0 = \ldots = a_{p-2} = 1$. For $s > 1$ we take $N = s(P-1)$ and as $a_0, \ldots, a_{N-1}$ we take $(p-1)$ copies of each of s basic elements of $GF[q]$ over $GF[p]$.

Assume that we have already constructed a polynomial f_K over $GF[q]$ in N^K variables with the property that it has the unique zero root. For $0 \leq i < N$ denote by $f_{K,i}$ the polynomial in N_K variables $X_{iN^K+1}, X_{iN^K+2}, \ldots, X_{(i+1)N^K}$ obtained from f_K by replacing each variable X_j by X_{j+iN^K}. As f_{K+1} we take $\sum_{0 \leq i \leq N-1} a_i f_{K,i}^{q-1}$.

We claim that for the case $s = 1$ the number of monomials in f_K is close to the obtained lower bound. Namely, we prove by induction on K that the number of monomials in f_K is at most $2^{2(p-1)^{K-1} - \frac{1}{2}\log_2(p-1)}$. The base of induction for $K = 1$, then $f_1 = X_1^{p-1} + \ldots + X_{p-1}^{p-1}$ is

clear.

Inductive step: f_{K+1} has at most $(p-1)2^{2(p-1)^K-\frac{1}{2}(p-1)\log_2(p-1)} \leq 2^{2((p-1)^K-\frac{1}{2})\log_2(p-1)}$ monomials. Since f_K has $(p-1)^K$ variables, the obtained lower bound gives $2^{(p-1)^{K-1}}$.

For more than one roots take f_K and l more variables on which f_K does not depend. Then $|G| = p^l$, the lower bound is $2^{((p-1)^K+l-\log_2|G|)/(p-1)} = 2^{((p-1)^K-l(\log_2 p-1))/(p-1)}$. Thus, for $l < \frac{1}{2} \cdot \frac{(p-1)^K}{\log_2 p-1}$ this bound is also close to the bound in the constructed example. □

Acknowledgment. We are thankful to Mike Singer for a number of interesting discutions.

References

[KLM 89] Karp, R., Luby, M., Madras, N., "Monte-Carlo Approximation Algorithms for Enumeration Problems", *J. of Algorithms*, Vol. 10, No. 3, Sept. 1989, pp. 429-448.

[KL 91a] Karpinski, M., Luby, M., *Approximating the Number of Solutions of a GF*[2] *Polynomial*, Technical Report TR-90-025, International Computer Science Institute, Berkeley, 1990, in Proc. 2^{nd} ACM-SIAM SODA (1991), pp. 300-303.

[KL 91b] Karpinski, M., and Lhotzky, B., *An* (ϵ, δ)*-Approximation Algorithm for the Number of Zeros for a Multilinear Polynomial over GF*$[q]$, Technical Report TR-91-022, International Computer Science Institute, Berkeley, 1991.