Archivum Mathematicum

Nina Brandstätter; Arne Winterhof

Approximation of the discrete logarithm in finite fields of even characteristic by real polynomials

Archivum Mathematicum, Vol. 42 (2006), No. 1, 43--50

Persistent URL: http://dml.cz/dmlcz/107980

ARCHIVUM MATHEMATICUM (BRNO)
Tomus 42 (2006), 43 – 50

APPROXIMATION OF THE DISCRETE LOGARITHM IN FINITE FIELDS OF EVEN CHARACTERISTIC BY REAL POLYNOMIALS

NINA BRANDSTÄTTER AND ARNE WINTERHOF

Abstract. We obtain lower bounds on degree and additive complexity of real polynomials approximating the discrete logarithm in finite fields of even characteristic. These bounds complement earlier results for finite fields of odd characteristic.

1. Introduction

Put $q = p^r$ where p is a prime and r is a positive integer. Denote by $\mathbb{F}_q$ the finite field of order q. Moreover, let α be a defining element of $\mathbb{F}_q$, i.e., $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{r-1}\}$ is a (polynomial) basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. We order the elements $\xi_0, \xi_1, \dots, \xi_{q-1}$ of $\mathbb{F}_q$ in the following way,

$$\xi_k = k_1 + k_2\alpha + \ldots + k_r\alpha^{r-1}$$

if

$$k = k_1 + k_2p + \ldots + k_rp^{r-1}, \quad 0 \le k_1, k_2, \dots, k_r < p\,,$$

for $0 \le k \le q-1$. Let γ be a primitive element of $\mathbb{F}_q$. The *discrete logarithm* (or *index*) of a nonzero element $\xi \in \mathbb{F}_q$ to the base γ, denoted $\mathrm{ind}_\gamma(\xi)$, is the unique integer l with $0 \le l \le q-2$ such that $\xi = \gamma^l$. The *discrete logarithm problem* is to find a computationally feasible method for determining the discrete logarithm. The security of many public-key cryptosystems depends on the presumed intractability of the discrete logarithm problem (see e. g. [13]). This paper provides some theoretical support to this assumption of hardness of the discrete logarithm problem. In the monograph [22] (or its predecessor [21]) and the series of papers [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 25, 26] several results on the discrete logarithm problem supporting the assumption of its hardness were proven. In particular, in [22, Chapter 11] several results on the complexity of real polynomials approximating the discrete logarithm in the case $r = 1$ are given. In

2000 *Mathematics Subject Classification.* 11T24, 11T71, 94A60.
Key words and phrases. Discrete logarithm, polynomial approximation, character sums.
Received September 10, 2004.

the case $p > 2$ most of these results can be extended to arbitrary r in a rather straightforward way along the lines of [7, 8, 16, 25]. However, in the case $p = 2$ several new ideas are needed. For example for $p = 2$ we have no quadratic character and need a compensation. In this article we prove two results on approximation polynomials of the discrete logarithm in the case $q = 2^r$. In Section 3 we prove a lower bound on the additive complexity of an interpolation polynomial and in Section 4 we prove a lower bound on the degree of polynomials which determine the rightmost bit of the discrete logarithm in $\mathbb{F}_q$ for a large set of given data.

2. Preliminaries

The *additive complexity* $C_\pm(f)$ of a polynomial $f(X)$ is the smallest number of '+' and '−' signs necessary to write down this polynomial. In [17, 18] the number of different zeros of a real polynomial was estimated in terms of its additive complexity.

Lemma 1. *For a nonzero polynomial $f(X) \in \mathbb{R}[X]$ having N different real zeros we have*

$$C_\pm(f) \geq \left(\frac{1}{5}\log_2(N)\right)^{1/2},$$

where $\log_2(N)$ is the binary logarithm.

Put $\mathrm{e}_T(z) = \exp(2\pi i z/T)$.

Lemma 2. *For any integer $1 \leq N \leq T$ we have*

$$\sum_{u=1}^{T-1}\left|\sum_{n=0}^{N-1}\mathrm{e}_T(un)\right| \leq T\left(\frac{4}{\pi^2}\ln T + 0.8\right),$$

where $\ln T$ denotes the natural logarithm.

Proof. We have

$$\begin{aligned}\sum_{u=1}^{T-1}\left|\sum_{n=0}^{N-1}\mathrm{e}_T(un)\right| &= \sum_{u=1}^{T-1}\left|\frac{\sin(\pi N u/T)}{\sin(\pi u/T)}\right| \\ &\leq \frac{4}{\pi^2}T\ln T + 0.38T + 0.608 + 0.116\frac{\gcd(N,T)^2}{T}\end{aligned}$$

by [1, Theorem 1]. □

For the following bound on incomplete character sums see [24, Section 3, p. 469].

Lemma 3. *Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$ and $f(X) \in \mathbb{F}_q[X]$ a monic polynomial which is not an ordχ-th power and has m different zeros in its splitting field over $\mathbb{F}_q$. Then we have for any additive subgroup V of $\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$,*

$$\left|\sum_{\xi\in V}\chi(af(\xi))\right| \leq mq^{1/2}.$$

Lemma 4. *Let $q = 2^r$. Under the conditions of Lemma 3 we have*

$$\Big|\sum_{k=0}^{K-1} \chi(af(\xi_k))\Big| \le mrq^{1/2}\,, \qquad 1 \le K \le q\,.$$

Proof. The set $\{\xi_0, \dots, \xi_{K-1}\}$ can be written as union of at most r cosets of additive subgroups. Hence, the result follows by Lemma 3. □

3. Interpolation

In this section we deal with arbitrary finite fields but focus on small characteristic including characteristic 2.

Theorem 1. *Let $f(X) \in \mathbb{R}[X]$ be a polynomial such that*

$$\mathrm{ind}_\gamma(\xi_k) = f(k) \qquad \text{for all } k \in S$$

for a set $S \subseteq \{1, \dots, q-1\}$ of cardinality $|S| = q - 1 - s$. Then we have

$$\deg f \ge \frac{q/p - 1}{2} - s$$

and

$$C_\pm(f) \ge \Big(\frac{1}{20}\log_2\Big(\frac{q/p-1}{2} - s\Big)\Big)^{1/2} - 1\,.$$

Proof. Let R be the set of all $k \in S$ with $1 \le k \le \frac{q}{p} - 1$ such that

$$\mathrm{ind}_\gamma(\xi_k) = f(k) \quad \text{and} \quad \mathrm{ind}_\gamma(\xi_{kp}) = f(kp)\,.$$

Then we have $|R| \ge q/p - 1 - 2s$. For each $k \in R$ we have either

$$f(kp) = \mathrm{ind}_\gamma(\xi_{kp}) = \mathrm{ind}_\gamma(\alpha\xi_k) = \mathrm{ind}_\gamma(\xi_k) + \mathrm{ind}_\gamma(\alpha) = f(k) + \mathrm{ind}_\gamma(\alpha)$$

or

$$f(kp) = \mathrm{ind}_\gamma(\alpha\xi_k) = \mathrm{ind}_\gamma(\xi_k) + \mathrm{ind}_\gamma(\alpha) - q + 1 = f(k) + \mathrm{ind}_\gamma(\alpha) - q + 1\,.$$

Hence, at least one of the polynomials

$$h_\omega(X) = f(pX) - f(X) - \omega$$

with $\omega \in \{\mathrm{ind}_\gamma(\alpha), \mathrm{ind}_\gamma(\alpha) - q + 1\}$ has at least $|R|/2$ zeros. The polynomials $h_\omega(X)$ are not identically zero since $h_\omega(0) = -\omega \ne 0$ and it follows

$$\deg f \ge \deg h_\omega \ge \frac{q/p - 1}{2} - s\,.$$

Lemma 1 yields

$$C_\pm(h_\omega) \ge \Big(\frac{1}{5}\log_2\Big(\frac{q/p-1}{2} - s\Big)\Big)^{1/2}$$

and $C_\pm(h_\omega) \le 2C_\pm(f) + 2$ implies the result. □

Remarks. 1. For $p > 2$ we may also use the relation

$$\mathrm{ind}_\gamma(\xi_{2k}) \equiv \mathrm{ind}_\gamma(\xi_k) + \mathrm{ind}_\gamma(2) \bmod q-1$$

if $k = k_1 + k_2 p + \ldots + k_r p^{r-1}$ with $0 \le k_1, k_2, \ldots, k_r \le (p-1)/2$ to obtain

$$\deg f \ge \frac{((p+1)/2)^r - 1}{2} - s$$

and

$$C_\pm(f) \ge \left(\frac{1}{20} \log_2 \left(\frac{((p+1)/2)^r - 1}{2} - s\right)\right)^{1/2} - 1$$

which improves Theorem 1 for large p with respect to r. This approach works also for an arbitrary basis instead of a polynomial basis in the definition of the ξ_k.

2. For rational interpolation polynomials $f(X) \in \mathbb{Q}[X]$ we may also use the lower bound on the additive complexity of [19, 20] to improve Theorem 1.

4. Approximation

Now we restrict ourselves to the case of even characteristic and prove a result on polynomials which determine the rightmost bit of the discrete logarithm.

Theorem 2. *Let $q = 2^r$ with $r \ge 3$, $1 \le H \le q-1$, and let $f(X) \in \mathbb{R}[X]$ be such that for all k of a subset $S \subseteq \{1, \ldots, H\}$ of cardinality $|S| = H - s$ we have*

$$\begin{aligned} f(k) &\ge 0\,, \quad \textit{if} \quad \mathrm{ind}_\gamma(\xi_k) \quad \textit{is even,} \\ f(k) &< 0\,, \quad \textit{otherwise.} \end{aligned}$$

Then we have

$$\deg f \ge \frac{2}{9}(H-1) - 4.2r\; q^{1/2} \left(\frac{4}{\pi^2} \ln(q-1) + 0.8\right)^2 - 2s - 1\,.$$

Proof. Let χ be a primitive character of $\mathbb{F}_q$ and put $\eta := \chi(\gamma)^{-1}$. For $0 \le l \le q-2$ and $\xi \in \mathbb{F}_q^*$ we put

$$\psi_l(\xi) := \begin{cases} 1\,, & \text{if} \quad \xi = \gamma^l\,, \\ 0\,, & \text{otherwise,} \end{cases}$$

and

$$\psi(\xi) := \begin{cases} 1\,, & \text{if} \quad \xi = \gamma^{2m} \quad \text{with} \quad 0 \le m \le q/2 - 1\,, \\ -1\,, & \text{otherwise.} \end{cases}$$

Note that

$$\psi_l(\xi) = \frac{1}{q-1} \sum_{j=0}^{q-2} \eta^{jl} \chi^j(\xi)$$

and

$$\psi(\xi) = 2 \sum_{m=0}^{q/2-1} \psi_{2m}(\xi) - 1 \,.$$

Put

$$T := \{1 \leq k \leq H : k \text{ even and } \psi(\xi_k) \neq \psi(\xi_k + 1)\} \,.$$

For all $k \in T$ we have $\xi_{k+1} = \xi_k + 1$.
The number of $k \in T$ such that either $k \notin S$ or $k+1 \notin S$ is at most $2s+1$.
So we have $f(k)f(k+1) < 0$ for at least $|T| - 2s - 1$ different k. The polynomial f changes its sign at least $|T| - 2s - 1$ times and has at least so many zeros. So we have

$$\deg f \geq |T| - 2s - 1.$$

On the other hand we have

$$\begin{aligned} |T| &= -\sum_{k \in T} \psi(\xi_k)\psi(\xi_k + 1) \\ &= -\sum_{k=1}^{\lfloor H/2 \rfloor} \psi(\xi_{2k})\psi(\xi_{2k} + 1) + \lfloor H/2 \rfloor - |T| \,. \end{aligned}$$

Hence, with $\xi_{2k} = \alpha\xi_k$ for $0 \leq k \leq q/2 - 1$ we get

$$|T| = -\frac{1}{2} \sum_{k=1}^{\lfloor H/2 \rfloor} \psi(\alpha\xi_k)\psi(\alpha\xi_k + 1) + \frac{1}{2}\lfloor H/2 \rfloor \,.$$

Next we use

$$\psi(\xi)\psi(\xi+1) = 4 \sum_{m_1,m_2=0}^{q/2-1} \psi_{2m_1}(\xi)\psi_{2m_2}(\xi+1) - 2 \sum_{m=0}^{q/2-1} (\psi_{2m}(\xi) + \psi_{2m}(\xi+1)) + 1$$

and

$$\psi_{2m_1}(\xi)\psi_{2m_2}(\xi+1) = \frac{1}{(q-1)^2} \sum_{j_1,j_2=0}^{q-2} \eta^{2(j_1 m_1 + j_2 m_2)} \chi^{j_1}(\xi)\chi^{j_2}(\xi+1)$$

to get

$$\begin{aligned} |T| = -2 &\sum_{m_1,m_2=0}^{q/2-1} \sum_{k=1}^{\lfloor H/2 \rfloor} \psi_{2m_1}(\alpha\xi_k)\psi_{2m_2}(\alpha\xi_k + 1) \\ &+ \sum_{m=0}^{q/2-1} \sum_{k=1}^{\lfloor H/2 \rfloor} (\psi_{2m}(\alpha\xi_k) + \psi_{2m}(\alpha\xi_k + 1)) \end{aligned}$$

$$= \frac{-2}{(q-1)^2} \sum_{j_1,j_2=0}^{q-2} \sum_{m_1,m_2=0}^{q/2-1} \eta^{2(j_1m_1+j_2m_2)} \sum_{k=1}^{\lfloor H/2 \rfloor} \chi^{j_1}(\alpha\xi_k)\chi^{j_2}(\alpha\xi_k+1)$$
$$+ \frac{1}{q-1} \sum_{j=0}^{q-2} \sum_{m=0}^{q/2-1} \eta^{2jm} \sum_{k=1}^{\lfloor H/2 \rfloor} (\chi^j(\alpha\xi_k) + \chi^j(\alpha\xi_k+1)) .$$

The summand for $j_1 = j_2 = 0$ in the first sum,

$$\frac{-q^2}{2(q-1)^2} \lfloor H/2 \rfloor ,$$

and the summand for $j = 0$ in the second sum,

$$\frac{q}{q-1} \lfloor H/2 \rfloor ,$$

add to

$$t := \frac{(q-2)q}{2(q-1)^2} \lfloor H/2 \rfloor \geq \frac{2}{9}(H-1) , \qquad q \geq 4 .$$

So we have

$$\big||T| - t\big| \leq \frac{2}{(q-1)^2} \sum_{j_1,j_2=1}^{q-2} \Big| \sum_{m_1,m_2=0}^{q/2-1} \eta^{2(j_1m_1+j_2m_2)} \Big| \Big| \sum_{k=1}^{\lfloor H/2 \rfloor} \chi^{j_1}(\alpha\xi_k)\chi^{j_2}(\alpha\xi_k+1) \Big|$$
$$+ \Big| \frac{1}{q-1} - \frac{q}{(q-1)^2} \Big| \sum_{j=1}^{q-2} \Big| \sum_{m=0}^{q/2-1} \eta^{2jm} \Big| \Big| \sum_{k=1}^{\lfloor H/2 \rfloor} (\chi^j(\alpha\xi_k) + \chi^j(\alpha\xi_k+1)) \Big|$$
$$< 4rq^{1/2} \Big(\frac{4}{\pi^2} \ln(q-1) + 0.8 \Big)^2 + \frac{2r}{q-1} q^{1/2} \Big(\frac{4}{\pi^2} \ln(q-1) + 0.8 \Big)$$
$$< 4.2r \; q^{1/2} \Big(\frac{4}{\pi^2} \ln(q-1) + 0.8 \Big)^2$$

by Lemmas 2 and 4 and the result follows. □

For odd characteristic the knowledge of the rightmost bit of the discrete logarithm of an element ξ is equivalent to knowing if ξ is a square. In this case ψ defined in the proof of Theorem 2 is the quadratic character and we may apply character sum bounds of [23] much earlier. For even characteristic all elements of $\mathbb{F}_q$ are squares and ψ is not multiplicative.

Acknowledgment. The authors are supported by the Austrian Academy of Sciences and by the Austrian Science Fund (FWF) grant S8313.

References

[1] Cochrane, T., *On a trigonometric inequality of Vinogradov*, J. Number Theory **27** (1987), 9–16.

[2] Coppersmith, D. and Shparlinski, I., *On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping*, J. Cryptology **13** (2000), 339–360.

[3] Ding, C. and Helleseth, T., *On cyclotomic generator of order r*, Inform. Process. Lett. **66** (1998), 21–25.

[4] Kiltz, E. and Winterhof, A., *Polynomial interpolation of cryptographic functions related to Diffie-Hellman and discrete logarithm problem*, Discrete Appl. Math. **154** (2006), 326–336.

[5] Konyagin, S., Lange, T. and Shparlinski, I., *Linear complexity of the discrete logarithm*, Des. Codes Cryptogr. **28** (2003), 135–146.

[6] Lange, T. and Winterhof, A., *Polynomial interpolation of the elliptic curve and XTR discrete logarithm*, Lecture Notes in Comput. Sci. **2387** (2002), 137–143.

[7] Lange, T. and Winterhof, A., *Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by Boolean functions*, Acta Arith. **101** (2002), 223–229.

[8] Lange, T. and Winterhof, A., *Interpolation of the discrete logarithm in F_q by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$*, Discrete Appl. Math. **128** (2003), 193–206.

[9] Meidl, W. and Winterhof, A., *Lower bounds on the linear complexity of the discrete logarithm in finite fields*, IEEE Trans. Inform. Theory **47** (2001), 2807–2811.

[10] Meletiou, G. C., *Explicit form for the discrete logarithm over the field* $\mathrm{GF}(p,k)$, Arch. Math. (Brno) **29** (1993), 25–28.

[11] Meletiou, G. C., *Explicit form for the discrete logarithm over the field* $\mathrm{GF}(p,k)$, Bul. Inst. Politeh. Iaşi. Secţ. I. Mat. Mec. Teor. Fiz. **41(45)** (1995), 1–4.

[12] Meletiou, G. C. and Mullen, G. L., *A note on discrete logarithms in finite fields*, Appl. Algebra Engrg. Comm. Comput. **3** (1992), 75–78.

[13] Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. *Handbook of applied cryptography*, CRC Press, Boca Raton, FL 1997.

[14] Mullen, G. L. and White, D., *A polynomial representation for logarithms in* $\mathrm{GF}(q)$, Acta Arith. **47** (1986), 255–261.

[15] Niederreiter, H., *A short proof for explicit formulas for discrete logarithms in finite fields*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), 55–57.

[16] Niederreiter, H. and Winterhof, A., *Incomplete character sums and polynomial interpolation of the discrete logarithm*, Finite Fields Appl. **8** (2002), 184–192.

[17] Risler, J.-J., *Khovansky's theorem and complexity theory*, Rocky Mountain J. Math. **14** (1984), 851–853.

[18] Risler, J.-J., *Additive complexity of real polynomials*, SIAM J. Comp. **14** (1985), 178–183.

[19] Rojas, J. M., *Additive complexity and p-adic roots of polynomials*, Lecture Notes in Comput. Sci. **2369** (2002), 506–516.

[20] Rojas, J. M., *Arithmetic multivariate Descartes' rule*, Amer. J. Math. **126** (2004), 1–30.

[21] Shparlinski, I., *Number theoretic methods in cryptography. Complexity lower bounds*, Birkhäuser, Basel 1999.

[22] Shparlinski, I., *Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness*, Birkhäuser, Basel 2003.

[23] Winterhof, A., *Some estimates for character sums and applications*, Des. Codes Cryptogr. **22** (2001), 123–131.

[24] Winterhof, A., *Incomplete additive character sums and applications*, In: Jungnickel, D. and Niederreiter, H. (eds.): Finite fields and applications, 462–474, Springer, Heidelberg 2001.

[25] Winterhof, A., *Polynomial interpolation of the discrete logarithm*, Des. Codes Cryptogr. **25** (2002), 63–72.

[26] Winterhof, A., *A note on the linear complexity profile of the discrete logarithm in finite fields*, Progress Comp. Sci. Appl. Logic **23** (2004), 359–367.

Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenberger Strasse 69, A-4040 Linz, Austria
E-mail: nina.brandstaetteroeaw.ac.at,
arne.winterhofoeaw.ac.at