ACTA ARITHMETICA
101.3 (2002)

Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by Boolean functions

by

TANJA LANGE (Essen) and ARNE WINTERHOF (Wien)

1. Introduction. Let $\mathbb{F}_q$ denote the finite field of order $q = p^r$ with a prime p and an integer $r \geq 1$. Let $\{\beta_0, \ldots, \beta_{r-1}\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and define ξ_k for $0 \leq k < q$ by

$$\xi_k = k_0\beta_0 + k_1\beta_1 + \ldots + k_{r-1}\beta_{r-1}$$

if

$$k = k_0 + k_1 p + \ldots + k_{r-1}p^{r-1} \quad \text{with } 0 \leq k_i < p \text{ for } 0 \leq i < r.$$

For $1 \leq K \leq p$ put

$$\mathcal{K}_K = \{k = k_0 + k_1 p + \ldots + k_{r-1}p^{r-1} \mid 0 \leq k_i < K \text{ for } 0 \leq i < r\}.$$

Consider the incomplete character sums $\sum_{k\in\mathcal{K}_K} \chi(f(\xi_k))$, where $f \in \mathbb{F}_q[x]$ and χ is a multiplicative character of $\mathbb{F}_q$. Excluding trivial cases we show in Section 2 that these sums are at most of the order of magnitude

$$(1) \qquad O(K^{1/2}p^{1/4}) \quad \text{if } r = 1 \quad \text{and} \quad O(K^{r-1}p^{1/2}) \quad \text{if } r \geq 2,$$

which improves previous results obtained with the standard method of Pólya and Vinogradov for K of the order of magnitude between $O(p^{1/2})$ and $O(p^{1/2}(\log(p))^2)$ if $r = 1$ and $O(p^{1/2}(\log(p))^{r/(r-1)})$ if $r \geq 2$.

If γ is a primitive element of $\mathbb{F}_q$ and $\xi \in \mathbb{F}_q$, $\xi \neq 0$, then $\xi = \gamma^l$ for some integer l with $0 \leq l \leq q-2$ and we say that l is the *discrete logarithm* (or *index*) of ξ to the base γ, denoted by $\mathrm{ind}_\gamma(\xi) = l$. For many practical purposes it would be sufficient to have an easily computable function which represents $\mathrm{ind}_\gamma(\xi)$ for almost all $\xi \neq 0$ or at least its rightmost bit, which is obviously 0 if ξ is a square in $\mathbb{F}_q$ and 1 if ξ is a non-square in $\mathbb{F}_q$ in the case of $p > 2$. To obtain a lower bound on the complexity of the discrete logarithm we investigate interpolating Boolean functions.

2000 *Mathematics Subject Classification*: 11T23, 11T71, 11Y16, 94A60, 94C10.

A Boolean function B can be represented as a multilinear polynomial over $\mathbb{F}_2$ and the *sparsity* (or *weight*) $\mathrm{spr}(B)$ of B is the number of non-zero coefficients of B. In the special case when $r = 1$ and $\beta_0 = 1$, i.e. $\xi_k = k$ for $0 \le k < p$, and $p > 2$, in Coppersmith and Shparlinski [1, Theorem 5] and Shparlinski [10, Theorem 6.1] it was shown that for a Boolean function $B(U_1, \ldots, U_s)$ of $s = \lfloor \log_2(p) \rfloor$ variables satisfying

$$B(u_1, \ldots, u_s) = \begin{cases} 0 & \text{if } k \text{ is a quadratic residue in } \mathbb{F}_p, \\ 1 & \text{if } k \text{ is a quadratic non-residue in } \mathbb{F}_p, \end{cases}$$

where $k = u_1 + \ldots + u_s 2^{s-1}$ with $u_j \in \{0,1\}$ for $1 \le j \le s$ and $1 \le k < 2^s$, we have

$$\mathrm{spr}(B) \ge 2^{-3/2} p^{1/4} (\log_2(p))^{-1/2} - 1. \tag{2}$$

Shparlinski mentioned in [10, p. 145] that using a "symmetrization" trick one can replace $p^{1/4}(\log_2(p))^{-1/2}$ by $p^{1/4}$ in (2) with a slightly worse constant. In Section 3 we extend the latter result to arbitrary r. The proof is based on the new estimate (1) for incomplete character sums.

2. A bound for incomplete character sums. Let χ be a non-trivial multiplicative character of $\mathbb{F}_q$ of order t, with the convention $\chi(0) = 0$, and let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not a tth power of a polynomial. Let v be the number of distinct roots of $f(x)$ in its splitting field over $\mathbb{F}_q$. First we recall Weil's bound for complete character sums.

LEMMA 1. *We have*

$$\Big| \sum_{\xi \in \mathbb{F}_q} \chi(f(\xi)) \Big| \le (v-1) q^{1/2}.$$

Proof. Lidl and Niederreiter [4, Theorem 5.41]. ∎

Now we prove a new bound for incomplete character sums.

THEOREM 1. *For $1 \le K < p$ we have*

$$\Big| \sum_{k \in \mathcal{K}_K} \chi(f(\xi_k)) \Big| < K^{r/2} (3v-1)^{1/2} q^{1/4} + r p^{1/2} K^{r-1}.$$

Proof. We modify the method used in Niederreiter and Shparlinski [7]. (See also Gutierrez, Niederreiter, and Shparlinski [3], Niederreiter and Shparlinski [6], and Niederreiter and Winterhof [8].) For any integer

$$m = m_0 + m_1 p + \ldots + m_{r-1} p^{r-1} \quad \text{with } 0 \le m_i < p \text{ for } 0 \le i < r$$

we have

$$\Big| \sum_{k \in \mathcal{K}_K} \chi(f(\xi_k)) - \sum_{k \in \mathcal{K}_K} \chi(f(\xi_k + \xi_m)) \Big| \le 2(m_0 + \ldots + m_{r-1}) K^{r-1}.$$

(We have $\xi_k + \xi_m \neq \xi_l$ for all $l \in \mathcal{K}_K$ only if at least one coordinate k_i of ξ_k satisfies $k_i + m_i \geq K$. The number of possible $k \in \mathcal{K}_K$ with this property is at most $(m_0 + \ldots + m_{r-1})K^{r-1}$. Similarly we can verify that the number of k with $\xi_k \neq \xi_l + \xi_m$ for all $l \in \mathcal{K}_K$ is at most $(m_0 + \ldots + m_{r-1})K^{r-1}$.) Then for any integer M with $1 \leq M \leq p$ we have

$$2 \sum_{m \in \mathcal{K}_M} (m_0 + \ldots + m_{r-1}) = rM^r(M-1)$$

and

$$M^r \Big| \sum_{k \in \mathcal{K}_K} \chi(f(\xi_k)) \Big| \leq W + rM^r(M-1)K^{r-1}, \tag{3}$$

where

$$W = \Big| \sum_{k \in \mathcal{K}_K} \sum_{m \in \mathcal{K}_M} \chi(f(\xi_k + \xi_m)) \Big| \leq \sum_{k \in \mathcal{K}_K} \Big| \sum_{m \in \mathcal{K}_M} \chi(f(\xi_k + \xi_m)) \Big|.$$

Using the Cauchy–Schwarz inequality we obtain

$$\begin{aligned} W^2 &\leq K^r \sum_{k \in \mathcal{K}_K} \Big| \sum_{m \in \mathcal{K}_M} \chi(f(\xi_k + \xi_m)) \Big|^2 \leq K^r \sum_{\xi \in \mathbb{F}_q} \Big| \sum_{m \in \mathcal{K}_M} \chi(f(\xi + \xi_m)) \Big|^2 \\ &= K^r \sum_{m, m' \in \mathcal{K}_M} \sum_{\xi \in \mathbb{F}_q} \chi(f(\xi + \xi_m) f(\xi + \xi_{m'})^{t-1}). \end{aligned}$$

Let $f(x) = \prod_{j=1}^{v} (x - \nu_j)^{c_j}$ be the factorization of $f(x)$ in its splitting field. Since $f(x)$ is not a tth power, there exists some h with $1 \leq h \leq v$ and $c_h \not\equiv 0 \bmod t$. If

$$\xi_m = \xi_{m'} + \nu_h - \nu_j \quad \text{for some } j \text{ with } 1 \leq j \leq v, \tag{4}$$

then the sum over ξ is estimated trivially by q. (There are at most v possible indices m' satisfying (4) for given m and h.) If $\xi_m \neq \xi_{m'} + \nu_h - \nu_j$ for all j with $1 \leq j \leq v$, then the polynomial $g(x) = f(x + \xi_m) f(x + \xi_{m'})^{t-1}$ is not a tth power and has at most $2v$ distinct zeros. Hence,

$$W^2 \leq K^r M^r vq + K^r M^{2r} (2v-1) q^{1/2}$$

by Lemma 1. Choosing $M = \lceil p^{1/2} \rceil$ we get

$$W^2 / M^{2r} < K^r (3v-1) q^{1/2}$$

and the assertion by (3). ∎

COROLLARY 1. *For $1 \leq K < p$ we have*

$$\Big| \sum_{k \in \mathcal{K}_K} \chi(f(\xi_k)) \Big| < \begin{cases} 2.2 K^{1/2} v^{1/2} p^{1/4} & \text{if } r = 1, \\ (3^{1/r} + r) K^{r-1} v^{1/r} p^{1/2} & \text{if } r \geq 2. \end{cases}$$

Proof. Since otherwise the bound is trivial we may assume that either $r = 1$ and $K \geq 4.84 p^{1/2}$ or $r \geq 2$ and $K \geq 3^{1/r} v^{1/r} p^{1/2}$. Then Theorem 1 yields for $r = 1$,

$$\Big|\sum_{k\in\mathcal{K}_K}\chi(f(\xi_k))\Big| < K^{1/2}v^{1/2}p^{1/4}(\sqrt{3}+K^{-1/2}p^{1/4}) < 2.2K^{1/2}v^{1/2}p^{1/4},$$

and for $r \geq 2$,

$$\Big|\sum_{k\in\mathcal{K}_K}\chi(f(\xi_k))\Big| < K^{r-1}v^{1/r}p^{1/2}(3^{1/2}K^{-r/2+1}v^{1/2-1/r}p^{r/4-1/2}+r)$$
$$\leq (3^{1/r}+r)K^{r-1}v^{1/r}p^{1/2},$$

which completes the proof. ∎

Remarks. 1. The standard method of Pólya and Vinogradov yields

$$\Big|\sum_{k\in\mathcal{K}_K}\chi(f(\xi_k))\Big| < vq^{1/2}(1+\log(p))^r \tag{5}$$

(see Davenport and Lewis [2, Theorem 1] for linear polynomials and Winterhof [11, Theorem 2] for arbitrary polynomials). Equation (5) is only non-trivial if K is at least of the order of magnitude $O(p^{1/2}\log(p))$. Theorem 1 is non-trivial if K is at least of the order of magnitude $O(p^{1/2})$ and it is better than (5) if K is at most of the order of magnitude $O(p^{1/2}(\log(p))^2)$ if $r = 1$ and $O(p^{1/2}(\log(p))^{r/(r-1)})$ if $r \geq 2$.

2. In [9, Theorem 3.1] Niederreiter and the second author showed that for any $1 \leq K < q$ we have

$$\Big|\sum_{k=0}^{K-1}\chi(f(\xi_k))\Big| < K^{1/2}(3v-1)^{1/2}q^{1/4}+q^{1/2}. \tag{6}$$

For $r = 1$ Theorem 1 and (6) coincide.

3. Interpolation by Boolean functions. In this section we give lower bounds for the sparsity and the degree of a Boolean function representing the rightmost bit of the discrete logarithm for almost all non-zero elements of $\mathbb{F}_q$.

Theorem 2. *Let $p > 2$. Put $s = \lfloor \log_2(p)\rfloor$, and let*

$$B(U_{11},\dots,U_{1s},\dots,U_{r1},\dots,U_{rs})$$

be a Boolean function satisfying

$$B(u_{11},\dots,u_{1s},\dots,u_{r1},\dots,u_{rs}) = \begin{cases} 0 & \text{if } \xi_k \text{ is a square in } \mathbb{F}_q,\\ 1 & \text{if } \xi_k \text{ is a non-square in } \mathbb{F}_q,\end{cases}$$

where $k_{i-1} = u_{i1}+u_{i2}2+\ldots+u_{is}2^{s-1}$ with $u_{ij}\in\{0,1\}$ for $1 \leq j \leq s$, $1 \leq i \leq r$, and $k \in \mathcal{K}_{2^s}\setminus\{0\}$. Then $\mathrm{spr}(B)$ is at least of the order of magnitude $O(q^{1/4})$, where the implied constant depends only on r.

Proof. Define the integer a by $2^a > (\mathrm{spr}(B)+1)^{1/r} \geq 2^{a-1}$ and put $\mathcal{M} = \{0,\ldots,2^a-1\}^r \setminus \{(0,\ldots,0)\}$. For each $\underline{m} = (m_1,\ldots,m_r) \in \mathcal{M}$ we consider the function

$$
\begin{aligned}
&B_{\underline{m}}(U_{11},\ldots,U_{1,s-a},\ldots,U_{r1},\ldots,U_{r,s-a})\\
&\qquad := B(U_{11},\ldots,U_{1,s-a},m_{11},\ldots,m_{1a},\ldots,U_{r1},\ldots,U_{r,s-a},m_{r1},\ldots,m_{ra}),
\end{aligned}
$$

where $m_i = m_{i1} + \ldots + m_{ia}2^{a-1}$ with $m_{ij} \in \{0,1\}$ for $1 \leq j \leq a$ and $1 \leq i \leq r$.

The number of distinct monomials in $U_{11},\ldots,U_{1,s-a},\ldots,U_{r1},\ldots,U_{r,s-a}$ occurring in all the $B_{\underline{m}}$ does not exceed $\mathrm{spr}(B)$. Since $|\mathcal{M}| = 2^{ar}-1 > \mathrm{spr}(B)$ we can find a non-trivial linear combination

$$
\sum_{\underline{m}\in\mathcal{M}} c_{\underline{m}} B_{\underline{m}}(U_{11},\ldots,U_{1,s-a},\ldots,U_{r1},\ldots,U_{r,s-a}) \quad \text{with } c_{\underline{m}} \in \mathbb{F}_2 \text{ for } \underline{m}\in\mathcal{M},
$$

which vanishes identically.

Let χ be the quadratic character of $\mathbb{F}_q$. By the condition of the theorem we have

$$
\chi(\xi_k) = (-1)^{B(u_{11},\ldots,u_{1s},\ldots,u_{r1},\ldots,u_{rs})} \quad \text{for } k \in \mathcal{K}_{2^s}\setminus\{0\}.
$$

Put $K = 2^{s-a}$. Then for $k = k_0 + k_1p + \ldots + k_{r-1}p^{r-1} \in \mathcal{K}_K$ we have

$$
\begin{aligned}
&\prod_{\underline{m}\in\mathcal{M}} \chi((k_0+m_1 2^{s-a})\beta_0 + \ldots + (k_{r-1}+m_r2^{s-a})\beta_{r-1})^{c_{\underline{m}}}\\
&\qquad\qquad = (-1)^{\sum_{\underline{m}\in\mathcal{M}} c_{\underline{m}}B_{\underline{m}}(u_{11},\ldots,u_{1,s-a},\ldots,u_{r1},\ldots,u_{r,s-a})} = 1
\end{aligned}
$$

and thus

$$
2^{(s-a)r} = \sum_{k\in\mathcal{K}_K} \chi\Big(\prod_{\underline{m}\in\mathcal{M}} ((k_0+m_12^{s-a})\beta_0 + \ldots + (k_{r-1}+m_r2^{s-a})\beta_{r-1})^{c_{\underline{m}}}\Big).
$$

Hence, for $r=1$ Corollary 1 yields

$$
2^{s-a} < 2.2\cdot 2^{s/2}p^{1/4}
$$

and thus

$$
2^a > 0.45\cdot 2^{s/2}p^{-1/4} \geq 0.31p^{1/4}.
$$

Hence,

$$
\mathrm{spr}(B) \geq 2^{a-1}-1 > 0.15p^{1/4}-1. \tag{7}
$$

For $r \geq 2$ Corollary 1 yields

$$
2^{(s-a)r} < (3^{1/r}+r)2^{(s-a)(r-1)}2^ap^{1/2}.
$$

Hence,

$$
2^{2a} > (3^{1/r}+r)^{-1}p^{-1/2}2^s \geq 2^{-1}(3^{1/r}+r)^{-1}p^{1/2}
$$

and thus

$$
(\mathrm{spr}(B)+1)^{1/r} \geq 2^{a-1} \geq 2^{-3/2}(3^{1/r}+r)^{-1/2}p^{1/4}, \tag{8}
$$

which yields the assertion. ∎

Using this bound we obtain the following bound on the degree of the Boolean function B.

COROLLARY 2. *Under the conditions of Theorem* 2 *for any* $r \geq 1$ *and any* $\varepsilon > 0$ *there exists a* $p_0(\varepsilon, r)$ *such that for all* $p \geq p_0$ *we have*

$$\deg(B) > (0.04 - \varepsilon)rs.$$

Proof. Put $n = \deg(B)$. Since otherwise the corollary is trivial we may suppose $2n \leq rs$. Obviously,

$$\operatorname{spr}(B) \leq \sum_{i=0}^{n} \binom{rs}{i} \leq 2^{rsH(n/(rs))}$$

by van Lint [5, Theorem 1.4.5], where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ for $0 < x \leq 1/2$ denotes the binary entropy function. Equations (7) and (8) yield

$$H\left(\frac{n}{rs}\right) \geq \frac{1}{4} + \frac{c}{s}$$

with a constant $c < 0$ depending only on r and thus

$$n \geq (\theta - \varepsilon)rs \quad \text{for } p \geq p_0,$$

where $\theta > 0.04$ denotes the solution of $H(x) = 1/4$. ∎

REMARKS. 1. Theorem 2 and Corollary 2 can be improved if 2 is a non-square in $\mathbb{F}_q$, i.e. if and only if $q \equiv \pm 3 \bmod 8$. Then we define $F(U_{11}, \ldots, U_{1,s-1}, \ldots, U_{r1}, \ldots, U_{r,s-1})$ by

$$\begin{aligned} F(U_{11}, \ldots, U_{1,s-1}, \ldots, U_{r1}, \ldots, U_{r,s-1}) \\ := B(U_{11}, \ldots, U_{1,s-1}, 0, \ldots, U_{r1}, \ldots, U_{r,s-1}, 0) \\ + B(0, U_{11}, \ldots, U_{1,s-1}, \ldots, 0, U_{r1}, \ldots, U_{r,s-1}). \end{aligned}$$

We have $F(u_{11}, \ldots, u_{1,s-1}, \ldots, u_{r1}, \ldots, u_{r,s-1}) = 1$ for every non-zero ξ_k with $k \in \mathcal{K}_{2^{s-1}}$ since exactly one of ξ_k and $2\xi_k$ is a square in $\mathbb{F}_q$. With $F(0, \ldots, 0) = 0$ (which does not depend on the ambiguous value of $B(0, \ldots, 0)$) we get

$$F(U_{11}, \ldots, U_{r,s-1}) = \prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s-1}} (1 + U_{ij}) + 1.$$

From the definition of F we have

$$\deg(B) \geq \deg(F) = r(s-1)$$

and

$$\operatorname{spr}(B) \geq \lceil 0.5\operatorname{spr}(F) \rceil = \lceil 0.5(2^{r(s-1)} - 1) \rceil = 2^{r(s-1)-1} \geq \frac{q}{2^{2r+1}}.$$

For $r = 1$ these results were derived by Shparlinski [10, Section 6].

2. In the same way as in the proof of Shparlinski [10, Theorem 6.2] one can use Corollary 2 to deduce a lower bound for the depth d of bounded fan-in Boolean circuits representing the rightmost bit of $\mathrm{ind}_\gamma(\xi_k)$ for all $k \in \mathcal{K}_{2^s} \setminus \{0\}$ in case of arbitrary r:

$$d \geq \log_2(rs) + O(1).$$

Acknowledgments. This paper was written during a visit of the first author to the Austrian Academy of Sciences. She wishes to thank Prof. H. Niederreiter and the Institute of Discrete Mathematics for hospitality and financial support.

References

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

[2] H. Davenport and D. J. Lewis, *Character sums and primitive roots in finite fields*, Rend. Circ. Mat. Palermo (2) 12 (1963), 129–136.

[3] J. Gutierrez, H. Niederreiter and I. E. Shparlinski, *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period*, Monatsh. Math. 129 (2000), 31–36.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997.

[5] J. H. van Lint, *Introduction to Coding Theory*, Springer, New York, 1982.

[6] H. Niederreiter and I. E. Shparlinski, *Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus*, Acta Arith. 92 (2000), 89–98.

[7] —, —, *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, Math. Comp. 70 (2001), 1569–1574.

[8] H. Niederreiter and A. Winterhof, *Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators*, Acta Arith. 93 (2000), 387–399.

[9] —, —, *Incomplete character sums over finite fields and polynomial interpolation of the discrete logarithm*, Finite Fields Appl., to appear.

[10] I. E. Shparlinski, *Number Theoretic Methods in Cryptography: Complexity Lower Bounds*, Birkhäuser, Basel, 1999.

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

Institute of Experimental Mathematics
University of Essen
Ellernstraße 29
D-45326 Essen, Germany
E-mail: lange@exp-math.uni-essen.de

Institute of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Wien, Austria
E-mail: arne.winterhof@oeaw.ac.at

Received on 3.8.2000
and in revised form on 17.5.2001 (3863)