On the Values of Kloosterman Sums

Igor E. Shparlinski

***Abstract*—Given a prime p and a positive integer n, we show that the shifted Kloosterman sums**

$$\sum_{x \in \mathbb{F}_{p^n}} \psi(x + ax^{p^n-2}) = \sum_{x \in \mathbb{F}_{p^n}^*} \psi(x + ax^{-1}) + 1, \quad a \in \mathbb{F}_{p^n}^*$$

where ψ is a nontrivial additive character of a finite field $\mathbb{F}_{p^n}$ of p^n elements, do not vanish if a belongs to a small subfield $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. This complements recent results of P. Charpin and G. Gong which in turn were motivated by some applications to bent functions.

***Index Terms*—Bent functions, Kloosterman sums, Lucas and Lehmer numbers.**

I. Introduction

FOR a prime p and positive integer n, we consider Kloosterman sums

$$K_{p^n}(a) = \sum_{x \in \mathbb{F}_{p^n}^*} \psi(x + ax^{-1}), \quad a \in \mathbb{F}_{p^n}^*$$

where ψ is a nontrivial additive character of a finite field $\mathbb{F}_{p^n}$ of p^n elements (clearly, $K_{p^n}(a)$ does not depend on the choice of ψ).

Motivated by some applications to so-called *bent functions*, Charpin and Gong [1] have considered the question of characterising the set $\mathcal{V}_{p^n}$ of $a \in \mathbb{F}_{p^n}^*$, for which the shifted Kloosterman sum

$$\sum_{x \in \mathbb{F}_{p^n}} \psi(x + ax^{p^n-2}) = K_{p^n}(a) + 1$$

vanishes. That is, the set $\mathcal{V}_{p^n}$ is defined as follows:

$$\mathcal{V}_{p^n} = \{a \in \mathbb{F}_{p^n}^* : K_{p^n}(a) = -1\};$$

see also [2].

In particular, it is shown in [1] that if $p = 2$ and $n = 2m \geq 6$ is even then

$$\mathcal{V}_{2^n} \cap \mathbb{F}_{2^m} = \emptyset.$$

Here we obtain a general result which applies for any p and asserts that $\mathcal{V}_{p^n}$ does not contain elements from small subfields of $\mathbb{F}_{p^n}$ of relative degree bounded by some explicit function of p.

Manuscript received October 10, 2008. Current version published May 20, 2009. This work was supported in part by ARC under Grant DP0556431.

The author is with the Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (e-mail: igor@ics.mq.edu.au).

Communicated by L. M. G. M. Tolhuizen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2009.2018320

Theorem 1: For any $m < n/s_0(p)$ where

$$s_0(p) = \begin{cases} 15, & \text{if } p = 2, 3 \\ \max\left\{2^{p-1} - 1, 2000((p-1) \cdot \log(3(p-1)))^{12}\right\}, & \text{if } p \geq 5 \end{cases}$$

we have

$$\mathcal{V}_{p^n} \cap \mathbb{F}_{p^m} = \emptyset.$$

The proof is based on the classical representation of Kloosterman sums via the roots of the corresponding Zeta-function and results of Bilu, Hanrot, and Voutier [3] and Voutier [4] on primitive divisors of Lucas and Lehmer numbers, which in turn improve upon the classical result of Schinzel [5].

In particular, one of the goals of this paper is to exhibit some traditional number-theoretic techniques and results which have never been applied in the context of coding theory and cryptography.

Finally, we remark that Theorem 1 has been used by Lisoněk and Moisio [6] to make further progress on the structure of the set $\mathcal{V}_{p^n}$.

II. Preparations

We summarize the necessary properties of Kloosterman as follows (see [7, Theorem 11.8] and also the proof of [7, Lemma 11.21]).

Lemma 2: For any $a \in \mathbb{F}_{p^m}^*$, we define $\alpha_{p^m}(a)$ and $\beta_{p^m}(a)$ as the roots of the polynomial $T^2 - K_{p^m}(a)T + p^m \in \mathbb{R}[T]$. Then

$$K_{p^{ms}}(a) = \alpha_{p^m}(a)^s + \beta_{p^m}(a)^s.$$

We remark that in the formulation of Lemma 2 we have implicitly used the fact that the values of Kloosterman sums are real numbers, which easily follows from the identity

$$K_{p^n}(a) = \sum_{x \in \mathbb{F}_{p^n}^*} \psi(-x - ax^{-1}) = \overline{K_{p^n}(a)}.$$

Let $\mathbb{L}$ be an algebraic number field. Given two algebraic integers $\alpha, \beta \in \mathbb{L}$ and a positive integer k we say that $\alpha^k - \beta^k$ has a *primitive divisor* if there is a prime ideal $\mathbb{F}_p^*$ which divides $\alpha^k - \beta^k$ but does not divide $\alpha^h - \beta^h$ for $h = 1, \ldots, k-1$.

We now recall the following result of Voutier [4, Theorem 2].

Lemma 3: Suppose that α and β are algebraic integers of degree d over $\mathbb{Q}$ such that α/β is not a root of unity. Then $\alpha^k - \beta^k$ has a primitive divisor for every integer $k > k_0(d)$, where

$$k_0(d) = \max\left\{2(2^d - 1), 4000(d\log(3d))^{12}\right\}.$$

In the case where α and β are conjugated quadratic irrationalities a much better estimate has been given by Bilu, Hanrot, and Voutier [3]

Lemma 4: Suppose that α and β are algebraic integers such that $\alpha+\beta, \alpha\beta \in \mathbb{Z}$ and α/β is not a root of unity. Then $\alpha^k - \beta^k$ has a primitive divisor for every integer $k > 30$.

III. Proof of Theorem 1

Let $\zeta_p = \exp(2\pi i/p)$. Since any additive character ψ of $\mathbb{F}_{p^n}$ is of the form

$$\psi(z) = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(uz)}$$

for some $u \in \mathbb{F}_{p^n}$, where

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(w) = \sum_{j=0}^{n-1} w^{p^j}$$

is the trace of $u \in \mathbb{F}_{p^n}$ in $\mathbb{F}_p$, we see that

$$K_{p^n}(a) \in \mathbb{Q}(\zeta_p)$$

for all $a \in \mathbb{F}_{p^n}^*$. Furthermore, since $K_{p^n}(a) \in \mathbb{R}$, we have

$$K_{p^n}(a) \in \mathbb{K}_p$$

where

$$\mathbb{K}_p = \mathbb{Q}\left(\zeta_p + \zeta_p^{-1}\right) = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$$

is the maximal real subfield of $\mathbb{Q}(\zeta_p)$, which is of degree

$$[\mathbb{K}_p : \mathbb{Q}] = \frac{1}{2}[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \frac{p-1}{2}$$

over $\mathbb{Q}$, see [8, Ch. 2]. Therefore, $\alpha_{p^m}(a)$ and $\beta_{p^m}(a)$ belong to some quadratic extension $\mathbb{L}_{a,p^n}$ of $\mathbb{K}_p$. In particular, $\mathbb{L}_{a,p^n}$ is of degree

$$[\mathbb{L}_{a,p^n} : \mathbb{Q}] \le 2[\mathbb{K}_p : \mathbb{Q}] \le p-1 \tag{1}$$

over $\mathbb{Q}$.

Assume that for $a \in \mathbb{F}_{p^m}^* \subseteq \mathbb{F}_{p^n}^*$ we have

$$K_{p^n}(a) = -1.$$

Then by Lemma 2 we obtain

$$\alpha_{p^m}(a)^s + \beta_{p^m}(a)^s = -1 \tag{2}$$

where $s = n/m$. Suppose that $\beta_{p^m}(a)/\alpha_{p^m}(a) = \rho$ is a root of unity. We derive from (2) that

$$\alpha_{p^m}(a)^s(\rho^s + 1) = -1. \tag{3}$$

Since $\rho^s + 1 \in \mathbb{L}_{a,p^n}$ is an algebraic integer and $\alpha_{p^m}(a)\beta_{p^m}(a) = p^m$, we see that $\alpha_{p^m}(a)^s(\rho^s+1)$ is divisible by a prime ideal which divides p in $\mathbb{L}_{a,p^n}$. Hence (3) is impossible.

Therefore, $\beta_{p^m}(a)/\alpha_{p^m}(a)$ is not a root of unity. Furthermore, from the identity

$$\left(\alpha_{p^m}(a)^s + \beta_{p^m}(a)^s\right)\left(\alpha_{p^m}(a)^s - \beta_{p^m}(a)^s\right) = \alpha_{p^m}(a)^{2s} - \beta_{p^m}(a)^{2s}$$

we see that if (2) holds then $\alpha_{p^m}(a)^{2s} - \beta_{p^m}(a)^{2s}$ has no primitive divisor. Using the bound (1) and recalling Lemma 3, we obtain the desired result in the case of $p \ge 5$.

For $p = 2, 3$, we recall that $K_{p^n}(a) \in \mathbb{Z}$ (which follows from the well-known connection between Kloosterman sums and the number of points on elliptic curves, see [9]–[13]). Thus, in this case Lemma 4 applies and we conclude the proof.

IV. Remarks

We note that we have not tried to get the best possible results. Our goal has been to provide a short proof of the fact that $\mathcal{V}_{p^m}$ does not have elements from small subfields of $\mathbb{F}_{p^n}$, where the largest relative degree can be estimated in terms of p only. We have also exhibited a link between the distribution of values of Kloosterman sums and some classical number theory problems. It is quite possible that using the bound of linear forms in logarithms [14]–[16] one can improve our estimates. Such estimated underly the results of [3]–[5] but can probably be applied in a more direct way. We also remark that the result of Niederreiter [17] on the distribution of values of Kloosterman sums, which in turn is based on the quantitative form of the *Sato–Tate* conjecture due to Katz [18], immediately implies that

$$\#\mathcal{V}_{p^n} = O(p^{3n/4}). \tag{4}$$

Furthermore, for $p = 2, 3$, there is a direct link between Kloosterman sums and elliptic curves, see [9]–[13]. Thus, using bounds on the Kronecker class number in the same fashion in the bound of Lenstra [19, Proposition 1.9] on the number of isogenous elliptic curves one can probably derive that

$$\#\mathcal{V}_{p^n} = O\left(p^{n/2} n (\log n)^2\right) \tag{5}$$

for $p = 2, 3$. It is also plausible that using some results of Katz [18] one can improve (4) and obtain an analogue of (5) for any prime p.

Finally, we remark that in the case of fields of large characteristic, there are very general results of Fisher [20], [21] and Wan [22] on the structure of the value set and distinctness of multidimensional Kloosterman sums.

Acknowledgment

The author is grateful to Petr Lisoněk and Marko Moisio for interesting discussion and the careful reading of the manuscript.

References

[1] P. Charpin and G. Gong, "Hyperbent functions, Kloosterman sums and Dickson polynomials," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4230–4238, Sep. 2008.

[2] P. Lisoněk, "On the connection between Kloosterman sums and elliptic curves," in *Proc. SETA'08 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2008, vol. 5203, pp. 182–187.

[3] Y. Bilu, G. Hanrot, and P. M. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers," *J. Reine Angew. Math.*, vol. 539, pp. 75–122, 2001.

[4] P. M. Voutier, "Primitive divisors of Lucas and Lehmer sequences, II," *J. Théorie Nombres Bordeaux.*, vol. 8, pp. 251–274, 1996.

[5] A. Schinzel, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields," *J. Reine Angew. Math.*, vol. 268/269, pp. 27–33, 1974.

[6] P. Lisoněk and M. Moisio, "On Kloosterman zeros in subfields," in *Proc. Int. Workshop on Coding and Cryptography (WCC'09)*, Ullensvang, Norway, May 2009, to be published.
[7] H. Iwaniec and E. Kowalski, *Analytic Number Theory*. Providence, RI: Amer. Math. Soc., 2004.
[8] L. C. Washington, *Introduction to Cyclotomic Fields, Graduate Texts in Math*. New York: Springer-Verlag, 1997, vol. 83.
[9] P. A. Leonard and K. S. Williams, "Quartics over $\mathrm{GF}(2^n)$," in *Proc. Amer. Math. Soc.*, 1972, vol. 36, pp. 347–350.
[10] M. Moisio, "On the moments of Kloosterman sums and fibre products of Kloosterman curves," *Finite Fields Appl.*, vol. 14, pp. 515–531, 2008.
[11] M. Moisio, "Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm," *Acta Arith.*, vol. 132, pp. 329–350, 2008.
[12] M. Moisio and K. Ranto, "Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros," *Finite Fields Appl.*, vol. 13, pp. 922–935, 2007.
[13] M. Moisio and K. Ranto, "Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed," *Finite Fields Appl.*, vol. 14, pp. 798–815, 2008.
[14] N. Gouillon, "Explicit lower bounds for linear forms in two logarithms," *J. Théorie Nombres Bordeaux.*, vol. 18, pp. 125–146, 2006.
[15] M. Mignotte, "Linear forms in two and three logarithms and interpolation determinants," in *Diophantine Equantions*. New Delhi, India: Tata Inst. Fund. Studies, 2008, pp. 151–166.
[16] K. Yu, "Report on p-adic logarithmic forms," in *A Panorama of Number Theory or The View from Baker's Garden*. Cambridge, U.K.: Cambridge Univ. Press, 2002, pp. 11–25.
[17] H. Niederreiter, "The distribution of values of Kloosterman sums," *Arch. Math.*, vol. 56, pp. 270–277, 1991.
[18] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*. Princeton, NJ: Princeton Univ. Press, 1988.
[19] H. W. Lenstra, "Factoring integers with elliptic curves," *Ann. Math.*, vol. 126, pp. 649–673, 1987.
[20] B. Fisher, "Distinctness of Kloosterman sums," in *P-adic Methods in Number Theory and Algebraic Geometry*, ser. Contemporary Mathematics. Providence, RI: Amer. Math. Soc, 1992, vol. 133, pp. 81–102.
[21] B. Fisher, "Kloosterman sums as algebraic integers," *Math. Ann.*, vol. 301, pp. 485–505, 1995.
[22] D. Wan, "Minimal polynomials and distinctness of Kloosterman sums," *Finite Fields Appl.*, vol. 1, pp. 189–203, 1995.

Igor Shparlinski is a Professor at the Computing Department of Macquarie University, Sydney, Australia. His main areas of interest are number theory, finite fields, theoretic computer science ,and cryptography.

Prof. Shparlinski was awarded a Medal of the Australian Mathematical Society for his activities in the area of applications of number theory to computer science in 1996 . In 2006, for his achievements in mathematics and cryptography, he was elected to the Australian Academy of Science which consists of about 400 of Australia's top scientists, elected by their peers for their exceptional scientific contribution.