Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®
Discrete Mathematics 279 (2004) 277–286
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Kloosterman sum identities over $\mathbf{F}_{2^m}$

Henk D.L. Hollmann[a], Qing Xiang[b]

[a] *Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, Netherlands*
[b] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

Received 15 November 2002; received in revised form 20 March 2003; accepted 9 June 2003

Dedicated to Zhu Lie on the occasion of his 60th birthday

Abstract

We introduce Kloosterman polynomials over $\mathbf{F}_{2^m}$, and use these polynomials to prove three identities involving Kloosterman sums over $\mathbf{F}_{2^m}$.
Published by Elsevier B.V.

Keywords: Kloosterman sum; Kloosterman identity; Linearized polynomial; Trace

1. Introduction

For $m \geqslant 1$ an integer, we will write $\mathbf{F}_{2^m}$ to denote the finite (Galois) field with 2^m elements, and $\mathbf{F}_{2^m}^*$ to denote $\mathbf{F}_{2^m} \setminus \{0\}$. The (absolute) trace function $\mathrm{Tr} : \mathbf{F}_{2^m} \to \mathbf{F}_2$ is defined by $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{2^i}$. For $a, b \in \mathbf{F}_{2^m}$, the Kloosterman sum $K(a,b)$ is defined as

$$K(a,b) = \sum_{x \in \mathbf{F}_{2^m}^*} (-1)^{\mathrm{Tr}(ax+b/x)}. \tag{1}$$

When $a = 1$, we simply denote the sum $K(1,b)$ by $K(b)$. Note that $K(a,b) = K(ab)$ if $a \neq 0$. (Substitute $y = ax$ into (1).)

Our main aim in this note is to prove the following Kloosterman sum identities.

Theorem 1.1. *For all $b \in \mathbf{F}_{2^m}$, we have that*

(i) $K(b^3(b+1)) = K(b(b+1)^3)$;
(ii) $K(b^5(b+1)) = K(b(b+1)^5)$;

E-mail addresses: henk.d.l.hollmann@philips.com (H.D.L. Hollmann), xiang@math.udel.edu (Q. Xiang).

0012-365X/$ - see front matter Published by Elsevier B.V.
doi:10.1016/S0012-365X(03)00275-9

(iii) $K(b^8(b^4+b)) = K((b+1)^8(b^4+b))$.

The substitution $b=a/(a+1)$ shows that the first identity in Theorem 1.1 is equivalent to the following.

Corollary 1.2. *For all* $a \in \mathbf{F}_{2^m} \setminus \{1\}$, *we have that* $K(a/(a+1)^4) = K(a^3/(a+1)^4)$.

The identity in Corollary 1.2 is not new; it has been proved for odd m in [7,8]. Moreover, while preparing this note we learned that both the first and the second identity in Theorem 1.1 have been proved for all m in [3], and that all three identities together with three others seem to have been proved by using the theory of modular curves [4], following up work by Lahtonen and Ojala, see also [6].

It is interesting to note that the authors of [7] were led to the discovery of the identity in the above corollary in the process of constructing certain 3-designs from the $\mathbf{Z}_4$-Goethals code, while we were led to this identity in the study of certain pseudocyclic association schemes.

2. Preliminaries

For $e \in \mathbf{F}_2$, we define

$$\mathbf{T}_e = \{x \in \mathbf{F}_{2^m} \mid \mathrm{Tr}(x) = e\}.$$

In what follows, we will use some simple and well-known properties of the trace function. For convenience, we recapitulate these properties here. Complete proofs can be found in any book on finite fields, for example in [5].

Lemma 2.1. (i) *The map* Tr *is* $\mathbf{F}_2$*-linear and surjective*; *hence* $|\mathbf{T}_0| = |\mathbf{T}_1| = 2^{m-1}$.
(ii) *The map* $x \mapsto x^2 + x$ *maps* $\mathbf{F}_{2^m}$ *two-to-one onto* $\mathbf{T}_0$.

Note that since the trace map is linear, the set $\mathbf{T}_0$ is a hyperplane in $\mathbf{F}_{2^m}$ (when considered as an m-dimensional vector space over $\mathbf{F}_2$). As a consequence, $\sum_{x\in\mathbf{T}_e}(-1)^{\mathrm{Tr}(bx)} = 0$ for $b \neq 0, 1$, where $e \in \mathbf{F}_2$.

3. Kloosterman polynomials and Kloosterman sum identities

All three identities in Theorem 1.1 can be written in the form $K(ab) = K((a+1)b)$ for suitable a and b in $\mathbf{F}_{2^m}$. We will first derive an equivalent formulation of this type of identities. To this end, for $e \in \mathbf{F}_2$ we define

$$K_e(a,b) = \sum_{x\in\mathbf{T}_e, x\neq 0} (-1)^{\mathrm{Tr}(ax+b/x)}.$$

Lemma 3.1. *Let $a, b \in \mathbf{F}_{2^m}^*$ with $a \neq 1$. We have that $K(ab) = K((a+1)b)$ if and only if $K_1(a,b) = 0$.*

Proof. Observe that for $a \neq 0, 1$, the identity $K(ab) = K((a+1)b)$ is equivalent to $K(a,b) = K(a+1,b)$. Since $K(a,b) = K_0(a,b) + K_1(a,b)$, $K_0(a+1,b) = K_0(a,b)$ and $K_1(a+1,b) = -K_1(a,b)$, the lemma follows. □

Remark. We note that this lemma can be used to simplify the proof of the main theorems Theorem 1 in [8] and Theorem 1 in [3], while strengthening the results by removing a superfluous condition. Indeed, both Lemma 2 in [8] and Lemma 2 in [3] in fact state that $K_1(u,v) = 0$ for $u = f(a)/(f(a)+g(a))$ and $v = f(a)+g(a)$, where f and g are functions satisfying certain conditions (different in the two papers) and a is assumed to be contained in some domain D. The conclusion that $K(f(a)) = K(g(a))$ for $a \in D$ now follows immediately from Lemma 3.1, so the condition that $f(D) = g(D)$, which is present in Theorem 1 of both papers, is not required, and both proofs can be simplified.

Our proof of Theorem 1.1 crucially depends on permutation properties of certain polynomial functions. In order to introduce these functions, we need some definitions. Let m be a positive integer. For $c = c_{m-1} \cdots c_0$ in $\{0, 1, \ldots, 2^m - 1\}$ with digits $c_i \in \{0, 1\}$, define its *reverse* $\tilde{c} = c_1 \cdots c_{m-1} c_0$ (so that $\tilde{c}_i = c_{-i}$, with indices considered modulo m), and its *weight* $w(c) = \sum_{i=0}^{m-1} c_i$. Given such numbers c, d, we define the polynomial functions on $\mathbf{F}_{2^m}$

$$L_c(x) = \sum_{i=0}^{m-1} c_i x^{2^i}$$

and

$$L_{c,d}(x) = L_c(x) + L_d(x^{2^m-2}).$$

In the rest of the note, to simplify notation, we will usually write

$$L_{c,d}(x) = L_c(x) + L_d(1/x)$$

with the understanding that $L_{c,d}(0) = 0$. The function $L_{c,d} : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ is called a *Kloosterman polynomial function* (in short, Kloosterman polynomial) on $\mathbf{F}_{2^m}$ if $w(d)$ is even and $L_{c,d}$ is injective on $\mathbf{T}_1$ (that is, if $L_{c,d}(x) = L_{c,d}(y)$, and $x, y \in \mathbf{T}_1$, then $x = y$). Note that if $w(d)$ is even and $w(c) \equiv e \bmod 2$, then for any $x \in \mathbf{F}_{2^m}$, $\mathrm{Tr}(L_{c,d}(x)) = w(c)\mathrm{Tr}(x) + w(d)\mathrm{Tr}(1/x) = e\,\mathrm{Tr}(x)$, so $L_{c,d}$ is a Kloosterman polynomial if and only if $w(d)$ is even and $L_{c,d}$ maps $\mathbf{T}_1$ bijectively onto $\mathbf{T}_e$. The relationship between Kloosterman polynomials and Kloosterman sum identities is explained by the following theorem.

Theorem 3.2. *Let $c, d \in \{1, \ldots, 2^m - 1\}$ with $w(d)$ even. If $L_{c,d}$ is a Kloosterman polynomial on $\mathbf{F}_{2^m}$, then we have the Kloosterman sum identity*

$$K(L_{\tilde{c}}(z) L_{\tilde{d}}(z)) = K((L_{\tilde{c}}(z) + 1) L_{\tilde{d}}(z))$$

for all $z \in \mathbf{F}_{2^m}$ such that $L_{\tilde{c}}(z) \neq 0, 1$.

Proof. Since $L_{\tilde{c}}(0)=0$ and $L_{\tilde{c}}(1)=w(c)=0$ or 1 in $\mathbf{F}_{2^m}$, we only need to prove the theorem for $z\in\mathbf{F}_{2^m}\setminus\{0,1\}$ such that $L_{\tilde{c}}(z)\neq 0,1$. According to Lemma 3.1, we have to prove that $K_1(L_{\tilde{c}}(z),L_{\tilde{d}}(z))=0$. To this end, we note that for any $x\in\mathbf{F}_{2^m}^*$,

$$\begin{aligned}
\mathrm{Tr}(L_{\tilde{c}}(z)x+L_{\tilde{d}}(z)/x) &= \mathrm{Tr}\left(\sum_{i=0}^{m-1} c_i z^{2^{m-i}}x+\sum_{i=0}^{m-1} d_i z^{2^{m-i}}/x\right)\\
&= \sum_{i=0}^{m-1} c_i\mathrm{Tr}(z^{2^{m-i}}x)+\sum_{i=0}^{m-1} d_i\mathrm{Tr}(z^{2^{m-i}}/x)\\
&= \sum_{i=0}^{m-1} c_i\,\mathrm{Tr}(zx^{2^i})+\sum_{i=0}^{m-1} d_i\,\mathrm{Tr}(z/x^{2^i})\\
&= \mathrm{Tr}\left(\sum_{i=0}^{m-1} c_i zx^{2^i}+\sum_{i=0}^{m-1} d_i z/x^{2^i}\right)\\
&= \mathrm{Tr}(zL_{c,d}(x)).
\end{aligned}$$

Hence, if $w(c)=e$, we have that

$$\begin{aligned}
K_1(L_{\tilde{c}}(z),L_{\tilde{d}}(z)) &= \sum_{x\in\mathbf{T}_1}(-1)^{\mathrm{Tr}(L_{\tilde{c}}(z)x+L_{\tilde{d}}(z)/x)}\\
&= \sum_{x\in\mathbf{T}_1}(-1)^{\mathrm{Tr}(zL_{c,d}(x))}\\
&= \sum_{y\in\mathbf{T}_e}(-1)^{\mathrm{Tr}(zy)}\\
&= 0
\end{aligned}$$

and the theorem follows. □

In the next section, we will investigate Kloosterman polynomials in more detail.

4. A general approach to Kloosterman polynomials

We now discuss a general and systematic approach for proving that a given function $F(x)$ on $\mathbf{F}_{2^m}$ is injective on $\mathbf{T}_1$, the set of elements of trace one in $\mathbf{F}_{2^m}$. Let

$$D_F(x,y)=\frac{F(x)-F(y)}{x-y}$$

and suppose that $D_F(x,y)=F(x,y)/\lambda(x,y)$ for some polynomials $F,\lambda\in\mathbf{F}_{2^m}[x,y]$. We want to prove that the equation $D_F(x,y)=0$, or the equation $F(x,y)=0$ derived from it, has only zeroes $(x,y)\in\mathbf{F}_{2^m}^2$ with $x=y$ or with one of x,y in $\mathbf{T}_0$. A way that suggests

itself is to try to write $F(x, y)$ in the form

$$F(x, y) = yQ^2(x, y) + P(x, y)Q(x, y) + P(x, y)^2. \tag{2}$$

Indeed, in that case, the equation $F(x, y) = 0$ would imply that $Q(x, y) = P(x, y) = 0$ or, writing $R(x, y) = P(x, y)/Q(x, y)$, that $y = R(x, y)^2 + R(x, y) \in \mathbf{T}_0$. As a consequence, it would be sufficient to show that the equations $P(x, y) = 0 = Q(x, y)$ have no solutions in $\mathbf{T}_1^2$ with $x \neq y$, which is usually a much easier task.

The following observation is of help in actually *finding* an expression (2), if it exists. First, if $F(x, y)$ can indeed be written in the form (2), then by writing $y = z^2 + z$, we would have that

$$F(x, y) = (P(x, y) + zQ(x, y))(P(x, y) + (z + 1)Q(x, y)),$$

that is, there would be a factorisation

$$F(x, z^2 + z) = G(x, z)G(x, z + 1). \tag{3}$$

Conversely, if F has such a factorisation, then by writing $z^2 = z + y$, we derive $z^3 = z(1 + y) + y$, $z^4 = z + y^2 + y, \ldots$, and in general $z^i = A_i(y) + zB_i(y)$ for certain polynomials A_i and B_i, which allows us to write

$$G(x, z) = \sum_i G_i(x)z^i = \sum_i G_i(x)(A_i(y) + zB_i(y)) = P(x, y) + zQ(x, y),$$

where

$$P(x, y) = \sum_i G_i(x)A_i(y), \qquad Q(x, y) = \sum_i G_i(x)B_i(y);$$

therefore, such a factorisation would in turn produce an expression for $F(x, y)$ as in (2).

In the sequel, we will use these ideas to prove that certain functions from $\mathbf{F}_{2^m}$ to itself are Kloosterman polynomials. In each of these cases, we will simply produce polynomials $P(x, y)$ and $Q(x, y)$ such that (2) holds, followed by an analysis of the equations $Q(x, y) = P(x, y) = 0$ showing that they do not have a solution in $\mathbf{T}_1^2$ with $x \neq y$.

Theorem 4.1. *The functions*

(i) $L_{1,3}(x) = x + 1/x + 1/x^2$,
(ii) $L_{1,6}(x) = x + 1/x^2 + 1/x^4$, *and*
(iii) $L_{1,10}(x) = x + 1/x^2 + 1/x^8$

are Kloosterman polynomials on $\mathbf{F}_{2^m}$ *for all* m, *that is, they all map* $\mathbf{T}_1$ *bijectively to* $\mathbf{T}_1$.

Proof. Evidently, all three functions map $\mathbf{T}_e$ to $\mathbf{T}_e$ for $e = 0, 1$. So we only have to show that these functions are injective on $\mathbf{T}_1$. To do so, we will use the ideas explained above.

(i) In the first case, $F(x)=L_{1,3}(x)$. We have that $D_F(x,y)=(xy)^{-2}F(x,y)$ with

$$F(x,y)=(xy)^2+xy+x+y.$$

As is easily checked, we have an expression (2) for $F(x,y)$, with

$$P(x,y)=xy+1, \qquad Q(x,y)=x+1;$$

moreover, since $P(x,y)+(y+1)Q(x,y)=x+y$, we have $Q(x,y)=P(x,y)=0$ only if $x=y$ (in fact, if and only if $x=y=1$).

(ii) In the second case, $F(x)=L_{1,6}(x)$. We have that $D_F(x,y)=(xy)^{-4}F(x,y)$ with

$$F(x,y)=(xy)^4+(xy)^2(x+y)+(x+y)^3.$$

We again have an expression (2) for $F(x,y)$, now with

$$P(x,y)=(y^2+y)x^2+(y+1)x+y, \qquad Q(x,y)=x^2+x+y$$

as is easily checked. Moreover, if $Q(x,y)=0$ then obviously $y\in\mathbf{T}_0$.

(iii) Finally, in the third case, $F(x)=L_{1,10}(x)$. We have that $D_F(x,y)=(xy)^{-8}F(x,y)$ with

$$F(x,y)=(xy)^8+(xy)^6(x+y)+(x+y)^7.$$

It is not difficult to check that, this time, we have an expression (2) for $F(x,y)$, with

$$P(x,y)=(y^4+y^2+y)x^4+(y^3+y^2+y+1)x^3+yx^2+(y^3+y^2)x+y^3$$

and

$$Q(x,y)=(x+y)(x^3+(y^2+y+1)x^2+y^2).$$

To finish the proof in this case, we will show that $P(x,y)=0$ and $Q(x,y)=0$ imply that $x=y$. First, if $Q(x,y)=0$, then $x=y$ or $Q_1(x,y)=x^3+(y^2+y+1)x^2+y^2=0$. Now

$$P(x,y)+S(x,y)Q_1(x,y)=x^2(x+y)^4,$$

where

$$S(x,y)=x^3+(y^2+y+1)x^2+(y+1)x+y,$$

so if $Q_1(x,y)=0$ and $P(x,y)=0$, then $x=y$ or $x=0$; since $x=0$ implies $y=0$, we have $x=y$ in both cases. □

Proof of Theorem 1.1. All three identities are clearly true if $b=0$ or 1. So from now on, we assume that $b\neq 0,1$.

(i) According to Theorem 4.1, $L_{c,d}$ for $c=1$, $d=3$ is a Kloosterman polynomial. We have $\tilde{c}=1$ and $\tilde{d}=2^{m-1}+1$, so $L_{\tilde{c}}(z)=z$ and $L_{\tilde{d}}(z)=z^{2^{m-1}}+z$. Hence by Theorem 3.2 and taking $z=b^2$, we obtain that $K(b^2(b^2+b))=K((b^2+1)(b^2+b))$.

(ii) Similarly, $L_{c,d}$ for $c=1$, $d=6$ is a Kloosterman polynomial. Here $\tilde{c}=1$ and $\tilde{d}=2^{m-2}+2^{m-1}$, so $L_{\tilde{c}}(z)=z$ and $L_{\tilde{d}}(z)=z^{2^{m-1}}+z^{2^{m-2}}$. Again by Theorem 3.2 and taking $z=b^4$, we now obtain that $K(b^4(b^2+b))=K((b^4+1)(b^2+b))$.

(iii) Finally, $L_{c,d}$ for $c=1$, $d=10$ is a Kloosterman polynomial. Now $\tilde{c}=1$ and $\tilde{d}=2^{m-3}+2^{m-1}$, so $L_{\tilde{c}}(z)=z$ and $L_{\tilde{d}}(z)=z^{2^{m-1}}+z^{2^{m-3}}$. In this case Theorem 3.2, with $z=b^8$, implies that $K(b^8(b^4+b))=K((b^8+1)(b^4+b))$. □

The following result is just a reformulation of Theorem 1.1.

Theorem 4.2. *Let $x,y\in\mathbf{F}_{2^m}$. We have $K(x)=K(y)$ in the following cases.*

(i) $(x+y)^4=xy$,
(ii) $(x+y)^6=xy$,
(iii) $(x+y)^{13}=xy(x^3+y^3)$.

Proof. (i) We claim that $x=b^2(b^2+b)$ and $y=(b^2+1)(b^2+b)$ for some $b\in\mathbf{F}_{2^m}$ if and only if $(x+y)^4=xy$. Indeed, if x and y are of this form, then $x+y=b^2+b$ and $xy=(b^2+b)^4$, so the relation (i) follows. Conversely, suppose that $(x+y)^4=xy$. If also $x\neq y$, then taking $b^2=x/(x+y)$ indeed leads to $x=b^2(b^2+b)$, while if $x=y$, then $x=y=0$ so that taking $b=0$ works.

(ii) Similarly, we have that $x=b^4(b^2+b)$ and $y=(b^4+1)(b^2+b)$ if and only if $(x+y)^6=xy$. Here we should take b such that $b^4=x/(x+y)$ if $x\neq y$ and $b=0$ otherwise.

(iii) Finally, we have that $x=b^8(b^4+b)$ and $y=(b^8+1)(b^4+b)$ if and only if $(x+y)^{13}=xy(x^3+y^3)$. Now we should take b such that $b^8=x/(x+y)$ if $x\neq y$ and $b=0$ otherwise. □

For fixed m, there are many Kloosterman polynomials. For example, if $m=4$, we have the Kloosterman polynomials $L_{c,d}$ for the (c,d) pairs $(1,0)$, $(1,3)$, $(1,6)$, $(1,10)$, $(7,0)$, $(7,3)$, $(7,5)$, and $(7,9)$; for $m=5$, the pairs $(1,0)$, $(1,3)$, $(1,6)$, $(1,10)$, $(3,0)$, $(3,5)$, $(3,10)$, $(3,30)$, $(5,0)$, $(5,3)$, $(5,15)$, $(5,30)$, $(7,0)$, $(7,9)$, $(7,18)$, $(7,23)$, $(11,0)$, $(11,12)$, $(11,27)$, $(11,29)$, $(15,0)$, $(15,3)$, $(15,5)$, and $(15,17)$ all give rise to Kloosterman polynomials. Also note that if $L_{c,d}$ is a Kloosterman polynomial, then the same holds for $L_{c,d}^2$, $L_{c,d}^4$, etc. We have listed only one member from each such cycle.

However, we conjecture that all Kloosterman polynomials can be obtained from $L_{1,3}, L_{1,6}$, and $L_{1,10}$ in a way that will be explained below, and therefore do not produce other Kloosterman sum identities beyond the ones in Theorem 1.1. Let $m\geqslant 1$ be a positive integer. In what follows, we will use $f\circ g$ to denote the *composition* of the functions f and g from $\mathbf{F}_{2^m}$ to $\mathbf{F}_{2^m}$, that is, the function defined by $(f\circ g)(x)=f(g(x))$, for all $x\in\mathbf{F}_{2^m}$. For $a=a_{m-1}\cdots a_0$ and $b=b_{m-1}\cdots b_0$, define the *binary convolution* $c=a*b$ of a and b by letting

$$c_k=\sum_{i=0}^{m-1}a_ib_{k-i} \bmod 2,$$

where indices are considered modulo m. It is easily checked that, as a consequence of this definition, the linearized polynomials L_a and L_b satisfy $L_a \circ L_b = L_{a*b}$. Hence, we also have that

$$L_a \circ L_{c,d} = L_{a*c,a*d}.$$

Our next result clarifies when this operation produces a Kloosterman polynomial.

Lemma 4.3. *For $a = a_{m-1}a_{m-2}\cdots a_1a_0 \in \{0,1,\ldots,2^m-1\}$ with digits $a_i \in \{0,1\}$, let $L_a(x) = \sum_{i=0}^{m-1} a_i x^{2^i}$ be a linearized polynomial in $\mathbf{F}_2[x]$.*

(i) *The function $L_a : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ is injective on $\mathbf{T}_0$ if and only if L_a is injective on $\mathbf{T}_1$. This is the case if and only if one of the following hold*:
  (a) *$w(a)$ is odd and L_a has only one zero in $\mathbf{F}_{2^m}$ (so L_a is a permutation polynomial)*, or
  (b) *$w(a)$ is even, m is odd, and L_a has only zeroes $0,1$ in $\mathbf{F}_{2^m}$ (so L_a is two-to-one on $\mathbf{F}_{2^m}$)*.

(ii) *Let $w(d)$ be even. We have that $L_{a*c,a*d}$ is a Kloosterman polynomial on $\mathbf{F}_{2^m}$ if and only if both L_a and $L_{c,d}$ are Kloosterman polynomials on $\mathbf{F}_{2^m}$.*

Proof. (i) Let L_a be the linearized polynomial on $\mathbf{F}_{2^m}$ as in the statement of the lemma. Then the kernel $K = \{x \in \mathbf{F}_{2^m} \mid L_a(x) = 0\}$ is an $\mathbf{F}_2$-linear subspace of $\mathbf{F}_{2^m}$, say, of dimension k (so $|K| = 2^k$). Since $\mathbf{T}_0$ is an $(m-1)$-dimensional $\mathbf{F}_2$-subspace of $\mathbf{F}_{2^m}$, we have that either $K \subseteq \mathbf{T}_0$ or $|K \cap \mathbf{T}_0| = 2^{k-1}$. Next, we note that L_a is injective on $\mathbf{T}_0$ if and only if L_a is injective on $\mathbf{T}_1$ if and only if $K \cap \mathbf{T}_0 = \{0\}$. Combining these two observations, we see that the condition $K \cap \mathbf{T}_0 = \{0\}$ holds if and only if either (a) $k = 0$ (then necessarily also $L_a(1) = w(a) = 1$ and L_a is a permutation polynomial on $\mathbf{F}_{2^m}$), or (b) $k = 1$ and $K = \{0, b\}$ for some $b \in \mathbf{T}_1$. In the latter case, since $\mathrm{Tr}(L_a(x)) = w(a)\mathrm{Tr}(x)$, we must have that $w(a)$ is even, hence $L_a(1) = 0$ and so $b = 1 \in \mathbf{T}_1$, and therefore m is odd.

(ii) Obviously, $L_a \circ L_{c,d} = L_{a*c,a*d}$ can only be injective on $\mathbf{T}_1$ if $L_{c,d}$ itself is injective on $\mathbf{T}_1$, and in that case $L_a \circ L_{c,d}$ is injective on $\mathbf{T}_1$ if and only if L_a is injective on the image $\mathbf{T}_{w(c)} = L_{c,d}(\mathbf{T}_1)$ of $\mathbf{T}_1$ under $L_{c,d}$. Now the claim follows from part (i). □

Remark 1. It is well known and not difficult to prove that for $q = p^r$ with p prime, a linearized polynomial $L_a(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ in $\mathbf{F}_q[x]$ induces a permutation on $\mathbf{F}_{q^m}$ if and only if $\gcd(a(x), x^m - 1) = 1$ in $\mathbf{F}_q[x]$, where $a(x) = \sum_{i=0}^{m-1} a_i x^i$. (Indeed, by writing $x \in \mathbf{F}_{q^m}$ with respect to a normal basis of $\mathbf{F}_{q^m}$ we see that $L_a(x) = 0$ if and only if the circulant matrix A associated with $a = (a_{m-1}, \ldots, a_0)$ has an eigenvector in $\mathbf{F}_q^m$ with eigenvalue 0, and this leads to the stated condition.) Similarly, $L_a(x)$ has only zeroes 0 and 1 in $\mathbf{F}_{q^m}$ if and only if $\gcd(a(x), x^m - 1)$ divides $x - 1$.

Remark 2. We claim that the Kloosterman polynomials $L_{a*c,a*d}$ obtained in part (ii) of Lemma 4.3 do not produce new Kloosterman sum identities. To see this, consider a linearized polynomial L_a. Note that for all b we have that $L_{a*b} = L_{b*a}$ and $L_{\widetilde{a*b}} = L_{\tilde{a}*\tilde{b}}$. So we have that $L_{\widetilde{a*c}}(z) = L_{\tilde{c}}(L_{\tilde{a}}(z))$ and $L_{\widetilde{a*d}}(z)) = L_{\tilde{d}}(L_{\tilde{a}}(z))$ for all $z \in \mathbf{F}_{2^m}$ and,

as a consequence, the Kloosterman sum identity obtained by Theorem 1.1 from the Kloosterman polynomial $L_{a*c,a*d}$ is a special case of the identity obtained from $L_{c,d}$. In particular, since L_2 is a linearized Kloosterman polynomial, the squaring operation $L_{c,d} \mapsto L_{c,d}^2 = L_2 \circ L_{c,d}$ does not produce any new identities.

Example. For an application of the lemma, take for example $L_3(x) = x^2 + x$. Obviously, L_3 has only zeroes $0, 1$ in $\mathbf{F}_{2^m}$, so by Lemma 4.3, part (i), L_3 is a Kloosterman polynomial for odd m. Now apply Lemma 4.3, part (ii): we have that $L_3 \circ L_{1,3}(x) = L_3(x) + L_3(1/x + 1/x^2) = x^2 + x + 1/x + 1/x^4 = L_{3,5}$, and similarly, $L_3 \circ L_{1,6} = L_{3,10}$ and $L_3 \circ L_{1,10} = L_{3,30}$, so we get the following. The functions

(i) $L_{3,5}(x) = x^2 + x + 1/x + 1/x^4$,
(ii) $L_{3,10}(x) = x^2 + x + 1/x^2 + 1/x^8$,
(iii) $L_{3,30}(x) = x^2 + x + 1/x^2 + 1/x^4 + 1/x^8 + 1/x^{16}$

are Kloosterman polynomials on $\mathbf{F}_{2^m}$ for odd m.

Let $\mathscr{L}_m$ denote the collection of linearized polynomials on $\mathbf{F}_{2^m}$ with coefficients in $\mathbf{F}_2$ that are injective both on $\mathbf{T}_0$ and on $\mathbf{T}_1$ (that is, linearized Kloosterman polynomials). Either directly or as a consequence of part (ii) of Lemma 4.3, $\mathscr{L}_m$ is a group under composition. In particular, suppose that L_c is a Kloosterman polynomial. Then there is a b such that L_b is also a Kloosterman polynomial and $L_b \circ L_c = L_1$ (the identity map), that is, $L_b(L_c(x)) = x$ for all $x \in \mathbf{F}_{2^m}$. Hence by Lemma 4.3, we have that $L_{c,d}$ is a Kloosterman polynomial if and only if $L_b \circ L_{c,d} = L_{1,b*d}$ is a Kloosterman polynomial.

We can now make precise what we meant by our earlier remark that all Kloosterman polynomials can be obtained by the ones from Theorem 4.1. Based on extended computer experiments, we offer the following conjectures.

Conjecture 4.4. For all $m \geqslant 1$, we have that $L_{1,d}$ is a Kloosterman polynomial on $\mathbf{F}_{2^m}$ if and only if $d \in \{0, 3, 6, 10\}$.

Note that the "if"-part of this conjecture has been proved in Theorem 4.1. The "only if"-part of this conjecture should not be too difficult to prove since to do so it is only required to produce for each $d \notin \{0, 3, 6, 10\}$ two elements in $\mathbf{T}_1$ with the same image under $L_{1,d}$.

Conjecture 4.5. Let $m > 3$. If $L_{c,d}$ is a Kloosterman polynomial on $\mathbf{F}_{2^m}$, then L_c is in $\mathscr{L}_m$.

If Conjecture 4.5 is true, then *each* Kloosterman polynomial is of the form $L_a \circ L_{1,d}$ for some L_a in $\mathscr{L}_m$ and some Kloosterman polynomial $L_{1,d}$ on $\mathbf{F}_{2^m}$; if both Conjectures 4.5 and 4.4 are true, then each Kloosterman polynomial in fact arises from the three basic ones in Theorem 4.1. We remark that perhaps these conjectures can be proved (in a very indirect way, though) using the results from [3].

5. Discussion

Let p be a prime, and let $\xi_p = e^{2\pi i/p}$ be a primitive complex pth root of unity. For integer $r \geqslant 1$ and $a \in \mathbf{F}_{p^r}$, we define the Kloosterman sum

$$K(p^r, a) = \sum_{\substack{x,\, y \in \mathbf{F}_{p^r} \\ xy = a}} \xi_p^{\mathrm{Tr}(x+y)}.$$

Note that $K(2^r, a)$ equals the Kloosterman sum $K(a)$ on $\mathbf{F}_{2^r}$ as defined at the beginning of this paper. In general, these Kloosterman sums $K(p^r, a)$ tend to be distinct up to the action of $\mathrm{Gal}(\mathbf{F}_{p^r}, \mathbf{F}_p)$, see for example [1,2,9]. Indeed, the $p^r - 1$ Kloosterman sums $K(p^r, a)$, where $a \in \mathbf{F}_{p^r} \setminus \{0\}$, are conjectured to be all distinct up to the action of $\mathrm{Gal}(\mathbf{F}_{p^r}, \mathbf{F}_p)$ if and only if $p \geqslant 2r$ (with the exception of $p = 2$ and $r = 2$ or 3). Kloosterman sum identities for fields of characteristic p other than 2 would thus provide help in the lower bound part of this conjecture. The results here can indeed be generalised to fields of other characteristics. For example, if $p = 3$, then $x \mapsto x - 1/x + 1/x^3$ is injective outside $\mathbf{T}_0$ and, hence, we obtain the identity $K(3^r, b^3(b - b^3)) = K(3^r, (b^3 + 1)(b - b^3)) = K(3^r, (b^3 + 2)(b - b^3))$ for all r. We will report on this and on further results elsewhere.

Acknowledgements

We thank Dong-Joon Shin for providing us with preprints of [8,7]. While we were preparing this paper, we were informed by Tor Helleseth that he and Victor Zinoviev also have a proof of the first two Kloosterman sum identities for all m in [3]. He also informed us of the work in [4]. We thank both Tor Helleseth and Mika Kojo for making these preprints available to us, and Mika Kojo for discussions on [4] and for sharing some thoughts on the identity for $p = 3$. We are grateful to Sebastian Egner, Jack van Lint, and Ludo Tolhuizen for their comments on earlier versions.

References

[1] B. Fisher, Distinctness of Kloosterman sums, in: A. Adolphson, et al., (Eds.), p-Adic Methods in Number Theory and Algebraic Geometry, Contemporary Mathematics, Vol. 133, American Mathematical Society, Providence, 1992, pp. 81–102.
[2] B. Fisher, Kloosterman sums as algebraic integers, Math. Ann. 301 (1995) 485–505.
[3] T. Helleseth, V. Zinoviev, New Kloosterman sums identities over $\mathbf{F}_{2^m}$ for all m, Finite Fields Their Appl. 9 (2003) 187–193.
[4] M.R.S. Kojo, Modular curves and identities of classical Kloosterman sums, preprint.
[5] R. Lidl, H. Niederreiter, Finite Fields, 2nd Edition, Cambridge University Press, Cambridge, 1997.
[6] L. Ojala, Graduate Thesis, University of Turku, 2001.
[7] Dong-Joon Shin, P.V. Kumar, T. Helleseth, 3-Designs from the $\mathbf{Z}_4$-Goethals codes via a new Kloosterman sum identity, Des. Codes Cryptography 28 (2003) 247–263.
[8] Dong-Joon Shin, Wonjin Sung, A new Kloosterman sum identity over $\mathbf{F}_{2^m}$ for odd m, Discrete Math. 268 (2003) 337–341.
[9] Daqing Wan, Minimal polynomials and distinctness of Kloosterman sums, Finite Fields Their Appl. 1 (1995) 189–203.