Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Finite Fields and Their Applications 14 (2008) 823–833

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

New Kloosterman sum identities and equalities over finite fields

Xiwang Cao [a,b,1], Henk D.L. Hollmann [c], Qing Xiang [d,*,2]

[a] *School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, PR China*
[b] *State Key Laboratory of Information Security, Beijing 100049, PR China*
[c] *Philips Research Labs, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands*
[d] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

Received 7 November 2007; revised 6 February 2008

Available online 18 April 2008

Communicated by Gary L. Mullen

Abstract

We present some general equalities between Kloosterman sums over finite fields of arbitrary characteristics. In particular, we obtain an explicit Kloosterman sum identity over finite fields of characteristic 3.

Keywords: Kloosterman polynomial; Kloosterman sum; Permutation polynomial

1. Introduction

Let p be a prime, $\mathbb{F}_{p^m}$ be the finite field with p^m elements, and $\mathbb{F}^*_{p^m} = \mathbb{F}_{p^m} \setminus \{0\}$. The *absolute trace* $\mathrm{Tr}: \mathbb{F}_{p^m} \to \mathbb{F}_p$ is defined by $\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{m-1}}$ for $x \in \mathbb{F}_{p^m}$. For future use, define $\mathrm{T}_i = \{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}(x) = i\}$, where $i \in \mathbb{F}_p$. For $a, b \in \mathbb{F}_{p^m}$, the (classical) *Kloosterman sum* $K(a, b)$ is defined by

* Corresponding author.
E-mail addresses: xwcao@nuaa.edu.cn (X. Cao), henk.d.l.hollman@philips.com (H.D.L. Hollmann), xiang@math.udel.edu (Q. Xiang).

[1] Research supported in part by NNSF of PR China 10771100.
[2] Research supported in part by NSF Grant DMS 0701049.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.02.002

$$K(a,b)=\sum_{x\in\mathbb{F}_{p^m}^*}\omega^{\mathrm{Tr}(ax+\frac{b}{x})},$$

where ω is a fixed complex primitive pth root of unity. To simplify notation, we simply write $K(b)$ for $K(1,b)$. It is easy to see that $K(a,b)=K(ab)$ for all $a\in\mathbb{F}_{p^m}^*$, and $K(b)=K(b^p)$ for all $b\in\mathbb{F}_{p^m}$.

Kloosterman sums have been studied extensively in number theory. They also found many applications in coding theory and design theory [6,8]. In general, the Kloosterman sums $K(b)$, $b\in\mathbb{F}_{p^m}^*$, tend to be distinct up to the action of $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$, see for example [1,2], and [10]. Indeed, it was conjectured in [10, p. 191] that the (p^m-1) Kloosterman sums $K(b)$, $b\in\mathbb{F}_{p^m}^*$, are distinct up to the action of $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ if $p\geqslant 2m$. A weaker version of this conjecture was proved in [10]. However, when p is small compared with m, there exist nontrivial equalities of the form $K(a)=K(b)$, where $b\neq a^{p^i}$ for any $i\in\{1,2,\ldots,m-1\}$. It turns out that when $p=2$ there even exist nontrivial *identities* between Kloosterman sums, of the type $K(f(c))=K(f(c+1))$ for certain functions f. As far as we know, all known identities of this type are over finite fields of characteristic 2 (cf. [9,3,4]). We briefly review these results.

Let $c\in\{0,1,\ldots,p^m-1\}$. Write $c=c_{m-1}p^{m-1}+\cdots+c_1p+c_0$, where $c_i\in\{0,1,2,\ldots,p-1\}$. We will often simply write $c=c_{m-1}c_{m-2}\cdots c_0$. Define the *reverse* of $c=c_{m-1}c_{m-2}\cdots c_0$ as $\tilde{c}=c_1\cdots c_{m-1}c_0$ (so that $\tilde{c_i}=c_{-i}$, where the indices are read modulo m). The *weight* of c is defined as $w(c)=\sum_{i=0}^{m-1}c_i$. Given two integers $c=c_{m-1}c_{m-2}\cdots c_0$ and $d=d_{m-1}d_{m-2}\cdots d_0$ in $\{0,1,\ldots,p^m-1\}$, we define a polynomial over $\mathbb{F}_{p^m}$ as follows:

$$L_{c,d}(X)=\sum_{i=0}^{m-1}c_iX^{p^i}+\sum_{i=0}^{m-1}d_iX^{(p^m-2)p^i}\in\mathbb{F}_{p^m}[X].$$

Following [4], we call $L_{c,d}(X)$ a *Kloosterman polynomial over* $\mathbb{F}_{p^m}$ if the function $L_{c,d}:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ induced by $L_{c,d}(X)$ is a bijection from T_i to $\mathrm{T}_{i'}$ for all $i=1,2,\ldots,p-1$, where $i'\in\mathbb{F}_p$ depends on i and $L_{c,d}(X)$.

When $p=2$, Hollmann and Xiang [4] proved the following results.

Lemma 1.1. *Let $L_c(X)=\sum_{i=0}^{m-1}c_iX^{2^i}\in\mathbb{F}_2[X]$, and $L_d(X)=\sum_{i=0}^{m-1}d_iX^{2^i}\in\mathbb{F}_2[X]$ with $w(d)$ even. If $L_{c,d}(X)=L_c(X)+L_d(X^{2^m-2})$ is a Kloosterman polynomial over $\mathbb{F}_{2^m}$, then the following identity holds*:

$$K\big(L_{\tilde{c}}(b)L_{\tilde{d}}(b)\big)=K\big(\big(L_{\tilde{c}}(b)+1\big)L_{\tilde{d}}(b)\big),$$

for all $b\in\mathbb{F}_{2^m}$ satisfying $L_{\tilde{c}}(b)\neq 0,1$.

As an application of Lemma 1.1, the following identities were proved by constructing certain specific Kloosterman polynomials over $\mathbb{F}_{2^m}$.

Theorem 1.2. *For every $b\in\mathbb{F}_{2^m}\backslash\mathbb{F}_2$, the following identities hold*:

$$K\big(b^3(1+b)\big)=K\big(b(1+b)^3\big),\tag{1.1}$$

$$K\big(b^5(1+b)\big)=K\big(b(1+b)^5\big),\tag{1.2}$$

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

Remark 1.3. The identities (1.1) and (1.2) were first proved in [3]. Prior to [3], (1.1) was proved in [9] for all odd m. All three identities and a few more were obtained by Kojo [5] by using modular curves of genus zero.

In this note, we will prove some general Kloosterman sum equalities over finite fields of arbitrary characteristics, including some explicit nontrivial ones in characteristic 3. We also obtain an explicit Kloosterman sum identity in characteristic 3 that was announced previously in [4]. We first give a definition.

Definition 1.4. Let $f:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ be a function. For $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$, $u\in\mathbb{F}_p$, and $i\in\mathbb{F}_p^*$, we define

$$N_f(b,u;i)=\left|\left\{x\in \mathrm{T}_i \;\middle|\; \mathrm{Tr}\big(bf(x)\big)=u\right\}\right|.$$

Given $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$, we say that f is *b-balanced* if $N_f(b,u;i)=p^{m-2}$ for all $u\in\mathbb{F}_p$ and all $i\in\mathbb{F}_p^*$. Furthermore we say that f is *globally balanced* if f is b-balanced for all $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$.

With this definition, we have

Theorem 1.5. *Let $L_c(X)=\sum_{i=0}^{m-1}c_iX^{p^i}\in\mathbb{F}_p[X]$, $L_d(X)=\sum_{i=0}^{m-1}d_iX^{p^i}\in\mathbb{F}_p[X]$, and $L_{c,d}(X)=L_c(X)+L_d(X^{p^m-2})$. If the function $L_{c,d}:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ induced by $L_{c,d}(X)$ is b-balanced for some $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$ such that $L_{\tilde c}(b)\notin\mathbb{F}_p$, then for all $u\in\mathbb{F}_p$, the following equality holds*:

$$K\big(L_{\tilde c}(b)L_{\tilde d}(b)\big)=K\big(\big(L_{\tilde c}(b)+u\big)L_{\tilde d}(b)\big).$$

Corollary 1.6. *Let $L_c(X)=\sum_{i=0}^{m-1}c_iX^{p^i}\in\mathbb{F}_p[X]$, $L_d(X)=\sum_{i=0}^{m-1}d_iX^{p^i}\in\mathbb{F}_p[X]$, and $L_{c,d}(X)=L_c(X)+L_d(X^{p^m-2})$. If the function $L_{c,d}:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ induced by $L_{c,d}(X)$ is globally balanced, then for all $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$ such that $L_{\tilde c}(b)\notin\mathbb{F}_p$ and all $u\in\mathbb{F}_p$, the following identity holds*:

$$K\big(L_{\tilde c}(b)L_{\tilde d}(b)\big)=K\big(\big(L_{\tilde c}(b)+u\big)L_{\tilde d}(b)\big).$$

Corollary 1.7. *Let $L_c(X)=\sum_{i=0}^{m-1}c_iX^{p^i}\in\mathbb{F}_p[X]$ and $L_d(X)=\sum_{i=0}^{m-1}d_iX^{p^i}\in\mathbb{F}_p[X]$. If $L_{c,d}(X)=L_c(X)+L_d(X^{p^m-2})$ is a Kloosterman polynomial over $\mathbb{F}_{p^m}$, then for all $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$ such that $L_{\tilde c}(b)\notin\mathbb{F}_p$ and all $u\in\mathbb{F}_p$, the following identity holds*:

$$K\big(L_{\tilde c}(b)L_{\tilde d}(b)\big)=K\big(\big(L_{\tilde c}(b)+u\big)L_{\tilde d}(b)\big).$$

Theorem 1.8. *With notation as above, we have for all $b\in\mathbb{F}_{3^m}\setminus\mathbb{F}_3$,*

$$K\big(b^3,b-b^3\big)=K\big(b^3+1,b-b^3\big)=K\big(b^3-1,b-b^3\big).$$

The proofs of these results will be given in Section 3. We make some preparations in Section 2.

2. Preliminaries

We first state the well-known Hilbert's theorem 90. A proof of this result can be found in many places, for example in [7, p. 56].

Lemma 2.1 *(Hilbert's theorem 90). Let* $\alpha \in \mathbb{F}_{p^m}$. *Then* $\mathrm{Tr}(\alpha) = 0$ *if and only if there exists an element* $\beta \in \mathbb{F}_{p^m}$ *such that* $\alpha = \beta^p - \beta$.

The following lemma will be useful in our discussion.

Lemma 2.2. *Let* $a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$. *Then there exists an element* $x \in \mathrm{T}_0$ *such that* $\mathrm{Tr}(ax) \neq 0$.

Proof. Assume to the contrary that for all $x \in \mathrm{T}_0$, one has $\mathrm{Tr}(ax) = 0$. Then viewed as polynomials over $\mathbb{F}_{p^m}$,

$$aX + a^p X^p + \cdots + a^{p^{m-1}} X^{p^{m-1}} = a^{p^{m-1}} \prod_{u \in \mathrm{T}_0} (X - u).$$

By the definition of T_0, we also have

$$X + X^p + \cdots + X^{p^{m-1}} = \prod_{u \in \mathrm{T}_0} (X - u),$$

as polynomials over $\mathbb{F}_{p^m}$. Hence we obtain

$$aX + a^p X^p + \cdots + a^{p^{m-1}} X^{p^{m-1}} = a^{p^{m-1}} \left(X + X^p + \cdots + X^{p^{m-1}}\right),$$

which implies that $a = a^p$, i.e., $a \in \mathbb{F}_p$, contradicting the choice of a. □

As a consequence of Lemma 2.2, we have

Corollary 2.3. *With notation as above, we have*

$$\sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(ax)} = 0, \quad \textit{for all } a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p \textit{ and for all } i \in \mathbb{F}_p.$$

Proof. Let $a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$. By Lemma 2.2, there is an element $x_0 \in \mathrm{T}_0$ such that $\omega^{\mathrm{Tr}(ax_0)} \neq 1$. We have

$$\omega^{\mathrm{Tr}(ax_0)} \sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(ax)} = \sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(a(x+x_0))} = \sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(ax)}. \tag{2.1}$$

Since $\omega^{\mathrm{Tr}(ax_0)} \neq 1$, we deduce from (2.1) the desired result. □

For future use, we define for $a, b \in \mathbb{F}_{p^m}^*$ and $i \in \mathbb{F}_p$,

$$K_i(a, b) = \sum_{x \in \mathrm{T}_i,\, x \neq 0} \omega^{\mathrm{Tr}(ax + \frac{b}{x})}.$$

Similar to Lemma 3.1 in [4], we have the following lemma.

Lemma 2.4. *Let $a \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$ and $b \in \mathbb{F}_{p^m}$. Then*

$$K_i(a,b) = 0, \quad \forall i \in \mathbb{F}_p^*,$$

if and only if $K(ab) = K((a+u)b)$ for all $u \in \mathbb{F}_p$.

Proof. Since $a \notin \mathbb{F}_p$, we see that for $u \in \mathbb{F}_p^*$, $K(ab) = K((a+u)b)$ is equivalent to $K(a,b) = K(a+u,b)$. Now

$$\begin{aligned} K(a+u,b) &= \sum_{x \in \mathbb{F}_{p^m}^*} \omega^{\mathrm{Tr}((a+u)x+\frac{b}{x})} \\ &= \sum_{x \in \mathrm{T}_0 \setminus \{0\}} \omega^{\mathrm{Tr}((a+u)x+\frac{b}{x})} + \sum_{x \in \mathbb{F}_{p^m}^* \setminus \mathrm{T}_0} \omega^{\mathrm{Tr}((a+u)x+\frac{b}{x})} \\ &= K_0(a,b) + \sum_{i=1}^{p-1} \omega^{ui} K_i(a,b), \end{aligned}$$

$$K(a,b) = K_0(a,b) + \sum_{i=1}^{p-1} K_i(a,b).$$

If $K_i(a,b) = 0$ for $i = 1, 2, \ldots, p-1$, then we have $K(a+u,b) = K(a,b) = K_0(a,b)$, for all $u \in \mathbb{F}_p^*$. Conversely, if for all $u \in \mathbb{F}_p^*$, $K(a+u,b) = K(a,b)$, then

$$\sum_{i=1}^{p-1} \omega^{ui} K_i(a,b) = \sum_{i=1}^{p-1} K_i(a,b), \quad \forall u \in \mathbb{F}_p^*.$$

Adding the above equations, we have

$$-\sum_{i=1}^{p-1} K_i(a,b) = (p-1) \sum_{i=1}^{p-1} K_i(a,b).$$

Therefore $\sum_{i=1}^{p-1} K_i(a,b) = 0$. Hence $K_i(a,b)$ satisfy the following homogeneous linear system:

$$\sum_{i=1}^{p-1} \omega^{ui} K_i(a,b) = 0, \quad \forall u \in \mathbb{F}_p^*.$$

The coefficient matrix of this linear system is clearly nonsingular. Hence $K_i(a,b) = 0$ for all $i = 0, 1, \ldots, (p-1)$. The proof is complete. □

3. Proofs of the main theorems

We first prove several properties of b-balanced functions.

Proposition 3.1. *Let $f:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ be a function, $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$, and let ω be a primitive pth root of unity. Then f is b-balanced if and only if*

$$\sum_{x\in \mathrm{T}_i}\omega^{\mathrm{Tr}(bf(x))}=0\quad \textit{for all } i\in\mathbb{F}_p^*.$$

Proof. Clearly we have

$$\sum_{x\in \mathrm{T}_i}\omega^{\mathrm{Tr}(bf(x))}=\sum_{u=0}^{p-1}N_f(b,u;i)\omega^u.$$

Therefore $\sum_{x\in \mathrm{T}_i}\omega^{\mathrm{Tr}(bf(x))}=0$ if and only if

$$\sum_{u=0}^{p-1}N_f(b,u;i)\omega^u=0. \tag{3.1}$$

Noting that the minimal polynomial of ω over the field of rational numbers is $1+X+X^2+\cdots+X^{p-1}$, we see from (3.1) that

$$N_f(b,u;i)=N_f(b,v;i)\quad \text{for all } u\neq v\in\mathbb{F}_p.$$

Now noting that $\sum_{u=0}^{p-1}N_f(b,u;i)=p^{m-1}$, we have $N_f(b,u;i)=p^{m-2}$ for all $u\in\mathbb{F}_p$.

The converse is obvious. The proof of the proposition is complete. □

Proposition 3.2. *Let $f:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ be a function. If for every $i\in\mathbb{F}_p^*$, $f|_{\mathrm{T}_i}$ is a one-to-one map from T_i to $\mathrm{T}_{i'}$ for some $i'\in\mathbb{F}_p^*$, then f is globally balanced.*

Proof. If the map f is a one-to-one map from T_i to $\mathrm{T}_{i'}$, where $i,i'\in\mathbb{F}_p^*$, then by Corollary 2.3, for all $b\in\mathbb{F}_{p^m}\setminus\mathbb{F}_p$, we have

$$\sum_{x\in \mathrm{T}_i}\omega^{\mathrm{Tr}(bf(x))}=\sum_{y\in \mathrm{T}_{i'}}\omega^{\mathrm{Tr}(by)}=0.$$

Hence the result now follows from Proposition 3.1. □

The next corollary gives the relationship between Kloosterman polynomials and globally balanced maps.

Corollary 3.3. *If $L_{c,d}(X)$ is a Kloosterman polynomial over $\mathbb{F}_{p^m}$, then the function $L_{c,d}:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ induced by $L_{c,d}(X)$ is globally balanced.*

The proof of Corollary 3.3 is immediate from the definition of Kloosterman polynomial and Proposition 3.2. We are now ready to give the proof of Theorem 1.5.

Proof of Theorem 1.5. By Lemma 2.4, if we can show that

$$K_i\big(L_{\tilde{c}}(b), L_{\tilde{d}}(b)\big) = 0$$

for all $i \in \mathbb{F}_p^*$, then the conclusion of the theorem will follow. Indeed, for $i \in \mathbb{F}_p^*$ we have,

$$\begin{aligned}
K_i\big(L_{\tilde{c}}(b), L_{\tilde{d}}(b)\big) &= \sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(L_{\tilde{c}}(b)x + \frac{L_{\tilde{d}}(b)}{x})} \\
&= \sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(\sum_{j=0}^{m-1} c_j b^{p^{m-j}} x + \sum_{j=0}^{m-1} d_j b^{p^{m-j}}/x)} \\
&= \sum_{x \in \mathrm{T}_i} \omega^{\sum_{j=0}^{m-1} c_j \mathrm{Tr}(b^{p^{m-j}} x) + \sum_{j=0}^{m-1} d_j \mathrm{Tr}(b^{p^{m-j}}/x)} \\
&= \sum_{x \in \mathrm{T}_i} \omega^{\sum_{j=0}^{m-1} c_j \mathrm{Tr}(b x^{p^j}) + \sum_{j=0}^{m-1} d_j \mathrm{Tr}(b/x^{p^j})} \\
&= \sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(b L_{c,d}(x))}.
\end{aligned}$$

If $L_{c,d}$ is b-balanced, by Proposition 3.1, we have $\sum_{x \in \mathrm{T}_i} \omega^{\mathrm{Tr}(b L_{c,d}(x))} = 0$. Now the theorem follows from Lemma 2.4. The proof is complete. □

Corollary 1.6 follows immediately from Theorem 1.5. Combining Corollaries 3.3 and 1.6, we obtain Corollary 1.7. In order to prove Theorem 1.8, we first construct an explicit Kloosterman polynomial over $\mathbb{F}_{3^m}$.

Lemma 3.4. *For every positive integer m, the polynomial* $L_{1,5}(X) = X - X^{3^m-2} + X^{3(3^m-2)}$ *is a Kloosterman polynomial over* $\mathbb{F}_{3^m}$.

We will present two proofs of this lemma. The first proof shows that the systematic way of proving such results as developed in [4] (see, for example, the proof of Theorem 4.1 in [4]) works here too. The second proof is a simple direct proof.

The first proof of Lemma 3.4. It is obvious that $\mathrm{Tr}(L_{1,5}(x)) = \mathrm{Tr}(x)$ for all $x \in \mathbb{F}_{3^m}$. Let

$$L_{1,5} : x \mapsto x - x^{3^m-2} + x^{3(3^m-2)}$$

be the map from $\mathbb{F}_{3^m}$ to itself induced by $L_{1,5}(X)$. We will show that $L_{1,5}$ is a bijection from T_i to T_i for $i = 1$ and 2.

If there exist $x, y \in \mathrm{T}_i$, $i = 1$ or 2, $x \neq y$, such that

$$L_{1,5}(x) = L_{1,5}(y),$$

then

$$F(x,y) := x^3y^3 + x^2y^2 - (x-y)^2 = 0. \tag{3.2}$$

Since $\mathrm{Tr}(x) = \mathrm{Tr}(y)$ and $x \neq y$, there exists an element $z \in \mathbb{F}_{3^m}$ such that $y = z^3 - z + x$, $z \notin \mathbb{F}_3$. Let

$$P(x,z) := x^2 + \left(z^3 - z\right)x - \left(z^2 + z\right).$$

Then it follows from (3.2) that

$$P(x,z)P(x,z+1)P(x,z-1) = 0.$$

So $P(x,z) = 0$, or $P(x,z+1) = 0$, or $P(x,z-1) = 0$. We will only consider the case where $P(x,z) = 0$ since the substitution $z \mapsto z-1$ (respectively $z \mapsto z+1$) changes $P(x,z+1)$ (respectively $P(x,z-1)$) into $P(x,z)$. Therefore, we assume that $x \in \mathrm{T}_i$ ($i = 1$ or 2) is a solution of the quadratic polynomial

$$P(X,z) = X^2 + \left(z^3 - z\right)X - \left(z^2 + z\right). \tag{3.3}$$

The discriminant of (3.3) is $z(z+1)(z^2+z+2)^2$. It follows that $z(z+1) = \delta^2$ for some $\delta \in \mathbb{F}_{3^m}$. Hence $x = (z^3 - z) \pm (\delta^3 - \delta)$. It follows that $\mathrm{Tr}(x) = 0$, contradicting the assumption that $x \in \mathrm{T}_i$, $i = 1$ or 2. The proof of the lemma is complete. □

The 2nd proof of Lemma 3.4. Let $\alpha \in \mathrm{T}_i$, where $i = 1$ or 2. If there exists $x \in \mathrm{T}_i$ such that $x - 1/x + 1/x^3 = \alpha$, then

$$x^4 - \alpha x^3 - x^2 + 1 = 0.$$

Therefore in order to prove the lemma, we only need to show that the polynomial $X^4 - \alpha X^3 - X^2 + 1 \in \mathbb{F}_{3^m}[X]$ has at most one solution in $\mathbb{F}_{3^m}$.

Assume to the contrary that the above polynomial has two solutions $a, b \in \mathbb{F}_{3^m}$. We have

$$X^4 - \alpha X^3 - X^2 + 1 = (X-a)(X-b)\left(X^2 + AX + B\right)$$

where $A, B \in \mathbb{F}_{3^m}$. Comparing the coefficients of X^3, X^2 and so on, we have

$$A - (a+b) = -\alpha, \tag{3.4}$$

$$ab - (a+b)A + B = -1, \tag{3.5}$$

$$abA - (a+b)B = 0, \tag{3.6}$$

$$abB = 1. \tag{3.7}$$

From (3.7), we find that $B = 1/ab$. From (3.6), we find that $A = \frac{a+b}{a^2b^2}$. Multiplying both sides of (3.5) by $\frac{(a+b)}{ab}$, we find that

$$A + (a+b) = \frac{(a+b)^3}{a^3b^3} - \frac{(a+b)}{ab}.$$

Table 1
Traces of the elements of $\mathbb{F}_{27}^*$

i	β^i	Tr	i	β^i	Tr	i	β^i	Tr	i	β^i	Tr	i	β^i	Tr
0	100	0	1	010	0	2	001	2	3	210	0	4	021	2
5	212	1	6	111	2	7	221	2	8	202	1	9	110	0
10	011	2	11	211	2	12	201	2	13	200	0	14	020	0
15	002	1	16	120	0	17	012	1	18	121	2	19	222	1
20	112	1	21	101	2	22	220	0	23	022	1	24	122	1
25	102	1												

Therefore $\mathrm{Tr}(A) = -\mathrm{Tr}(a+b)$. Now from (3.4), we see that $\mathrm{Tr}(A) = \mathrm{Tr}(\alpha)$, which by assumption is nonzero. It follows that $a+b \neq 0$. Now rewrite (3.5) as

$$ab + a^2b^2 + a^3b^3 = (a+b)^2. \tag{3.8}$$

Noting that (3.8) can be rewritten as $(a+b)^2 = ab(ab-1)^2$, we have

$$A = \frac{a+b}{a^2b^2} = \frac{(ab-1)^4}{(a+b)^3} = \frac{ab-1}{a+b} - \frac{(ab-1)^3}{(a+b)^3}.$$

Therefore $\mathrm{Tr}(A) = 0$, contradicting our assumption that $\mathrm{Tr}(\alpha) \neq 0$. The proof is complete. □

We are now ready to give the proof of Theorem 1.8.

Proof of Theorem 1.8. Let $L_1(X) = X$ and $L_5(X) = -X + X^3$. Then $L_{\tilde{1}}(X) = X$ and $L_{\tilde{5}}(X) = -X + X^{3^{m-1}}$. If $b \in \mathbb{F}_{3^m} \setminus \mathbb{F}_3$, then $L_{\tilde{1}}(b) = b \notin \mathbb{F}_3$. By Lemma 3.4, $L_{1,5}(X)$ is a Kloosterman sum polynomial over $\mathbb{F}_{3^m}$. It follows from Theorem 1.5 that

$$K\big(b, -b + b^{3^{m-1}}\big) = K\big(b+1, -b + b^{3^{m-1}}\big) = K\big(b-1, -b + b^{3^{m-1}}\big).$$

Substituting b by b^3 yields the desired result. □

Finally we present an example to illustrate that there exist $c, d \in \{0, 1, \ldots, p^m - 1\}$ and $b \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$ such that $L_{c,d}$ is b-balanced but $L_{c,d}(X)$ is not a Kloosterman polynomial.

Example 3.5. Let β be a primitive element of $\mathbb{F}_{3^3}$ satisfying $\beta^3 - \beta + 1 = 0$. The elements of $\mathbb{F}_{27}$ together with their traces are listed in Table 1.

Let

$$E_1 = \{5, 8, 15, 17, 19, 20, 23, 24, 25\}, \qquad E_2 = \{2, 4, 6, 7, 10, 11, 12, 18, 21\}.$$

Then $\beta^j \in \mathrm{T}_i$ if and only if $j \in E_i$, for $i = 1, 2$ and $j = 1, 2, \ldots, 25$.

Let $L_c(X) = X$, $L_d(X) = -X^9$, where $c = 1$ and $d = 18$. Then $L_{\tilde{c}}(X) = X$, $L_{\tilde{d}}(X) = -X^3$, and $L_{c,d}(X) = X - X^{-9}$. Taking $b = \beta^{14}$, one can easily check that

$$\big(\mathrm{Tr}\big(bL_{c,d}(x)\big) \big| x \in \mathrm{T}_1\big) = (2, 2, 0, 0, 1, 1, 1, 0, 2),$$
$$\big(\mathrm{Tr}\big(bL_{c,d}(x)\big) \big| x \in \mathrm{T}_2\big) = (0, 0, 2, 2, 2, 0, 1, 1, 1).$$

Therefore, $L_{c,d}(X)$ is b-balanced.

Table 2
b-Balanced functions of the form $L_{1,d}(x) = x + k_1 x^{-25} + k_2 x^{25*3} + k_3 x^{25*9}$ on $\mathbb{F}_{27}$

$(k_1k_2k_3)$	b	$(k_1k_2k_3)$	b	$(k_1k_2k_3)$	b	$(k_1k_2k_3)$	b	$(k_1k_2k_3)$	b
(100)	NO	(120)	–	(011)	$\pm\beta$	(221)	$-\beta$	(112)	NO
(200)	$\pm\beta$	(220)	NO	(111)	–	(002)	$-\beta$	(212)	β
(010)	NO	(001)	NO	(211)	NO	(102)	–	(022)	NO
(110)	$\pm\beta$	(101)	β	(021)	–	(202)	NO	(122)	$\pm\beta$
(210)	GB	(201)	–	(121)	NO	(012)	–	(222)	–
(020)	$-\beta$								

Now, we have $L_{\tilde{c}}(b)L_{\tilde{d}}(b) = \beta + 2\beta^2 = \beta^{17}$, $L_{\tilde{c}}(b)L_{\tilde{d}}(b) + L_{\tilde{d}}(b) = 2 + 2\beta + 2\beta^2 = \beta^{19}$. By Theorem 1.5, we have

$$K\left(L_{\tilde{c}}(b)L_{\tilde{d}}(b)\right) = K\left(\left(L_{\tilde{c}}(b) + 1\right)L_{\tilde{d}}(b)\right),$$

that is, $K(\beta^{17}) = K(\beta^{19})$. (In fact, $K(\beta^{17}) = K(\beta^{19}) = 2$.)

Note that β^{17} is not conjugate to β^{19}, hence this equation represents a nontrivial result.

Putting $b' = \beta^2$, one can check that

$$\left(\mathrm{Tr}\left(b' L_{c,d}(x)\right) \middle| x \in \mathrm{T}_1\right) = (2, 1, 0, 0, 2, 2, 1, 2, 1),$$
$$\left(\mathrm{Tr}\left(b' L_{c,d}(x)\right) \middle| x \in \mathrm{T}_2\right) = (0, 0, 1, 2, 2, 1, 2, 1, 2).$$

Therefore, $L_{c,d}$ is not b'-balanced. Thus $L_{c,d}$ is not globally balanced and so it is not a Kloosterman polynomial.

In Table 2 we list all polynomials of the form $L_{1,d}(X) = X + k_1X^{25} + k_2X^{25*3} + k_3X^{25*9}$ with k_1, k_2, k_3 in $\mathbb{F}_3$, indicating whether the induced functions $L_{1,d} : \mathbb{F}_{27} \to \mathbb{F}_{27}$ are globally balanced (GB), b-balanced for some b's (we list the cycleleaders that produce nontrivial equations), or not balanced (NO).

From Table 2, we see that there is only one Kloosterman polynomial of the form $L_{1,d}(X) = X + k_1X^{25} + k_2X^{25*3} + k_3X^{25*9}$ with k_1, k_2, k_3 in $\mathbb{F}_3$. However, there are many b-balanced functions induced by polynomials of this form. From Theorem 1.5, we can obtain many equalities between Kloosterman sums by using b-balanced functions, and many of these are nontrivial.

The behavior in Table 2 appears to be typical for finite fields of characteristic $p = 3$. For other values of p the situation seems to be different. We did further computations for the case $p = 5$, $m = 3$, covering all polynomials $L_{c,d}(X)$, and for the cases $p = 5$, $m \leqslant 5$, $p = 7$, $m \leqslant 4$, and $p = 11$, $m = 3$, covering all polynomials $L_{1,d}(X)$. Unfortunately, except for the case $p = 5$, $m = 5$, all b-balanced functions $L_{c,d}$ that we found turn out to satisfy $L_{\tilde{d}}(b) = 0$; in the case $p = 5$, $m = 5$, we found various b-balanced functions $L_{1,d}$ for which $L_{\tilde{d}}(b) \neq 0$ (for example $L_{1,9}(x)$), however none of these produced a nontrivial Kloosterman equality. More extensive computations are needed to draw further conclusions; but at present we cannot rule out the possibility that no nontrivial Kloosterman equalities can be produced by this method for $p \geqslant 5$.

References

[1] B. Fisher, Distinctness of Kloosterman sums, in: A. Adolphson, et al. (Eds.), p-Adic Methods in Number Theory and Algebraic Geometry, in: Contemp. Math., vol. 133, Amer. Math. Soc., Providence, 1992, pp. 81–102.

[2] B. Fisher, Kloosterman sums as algebraic integers, Math. Ann. 301 (1995) 485–505.
[3] Tor Helleseth, Victor Zinoviev, New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, Finite Fields Appl. 9 (2003) 187–193.
[4] Henk D.L. Hollmann, Qing Xiang, Kloosterman sum identities over $\mathbb{F}_{2^m}$, Discrete Math. 279 (2004) 277–286.
[5] Mika R.S. Kojo, Modular curves and identities of classical Kloosterman sums, personal communication.
[6] G. Lachaud, J. Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractristique 2 (Kloosterman sums, elliptic curves and cyclic codes in characteristic 2), C. R. Acad. Sci. Paris Sér. I Math. 305 (1987) 881–883 (in French).
[7] R. Lidl, H. Niederreiter, Finite Fields, second ed., Cambridge Univ. Press, 1997.
[8] Dong-Joon Shin, P. Vijay Kumar, Tor Helleseth, 3-Designs from the $\mathbb{Z}_4$-Goethals codes via a new Kloosterman sum identity, Des. Codes Cryptogr. 28 (2003) 247–263.
[9] Dong-Joon Shin, Wonjin Sung, A new Kloosterman sum identity over $\mathbb{F}_{2^m}$ for odd m, Discrete Math. 268 (2003) 337–341.
[10] D. Wan, Minimal polynomials and distinctness of Kloosterman sums, Finite Fields Appl. 1 (1995) 189–203.