New Kloosterman sum identities from the Helleseth-Zinoviev result on $Z_4$-linear Goethals codes

Minglong Qi · Shengwu Xiong

Abstract In the paper of Tor Helleseth and Victor Zinoviev (Designs, Codes and Cryptography, 17, 269-288(1999)), the number of solutions of the system of equations from $Z_4$-linear Goethals codes $G_4$ was determined and stated in Theorem 4. We found that Theorem 4 is wrong for $m$ even. In this note, we complete Theorem 4, and present a series of new Kloosterman sum identities deduced from Theorem 4. Moreover, we show that several previously established formulas on the Kloosterman sum identities can be rediscovered from Theorem 4 with much simpler proofs.

Keywords Kloosterman sum identities · $Z_4$-linear Goethals codes · nonlinear system of equations · exponential sums

Mathematics Subject Classification (2010) 11L05 · 11T23

1 Introduction

Let $m$ be a positive integer, $q = 2^m$, $F := \mathbb{F}_q$ be the finite field of $q$ elements, $F^* := F \setminus \{0\}$, and $F^{**} := F \setminus \{0, 1\}$. The well known Kloosterman sums [12] are defined by

$$K(a) = \sum_{x \in F^*} (-1)^{\text{Tr}(ax+1/x)}$$

where $a \in F^*$, and $\text{Tr}(\cdot)$ is the trace function of $F$ over $\mathbb{F}_2$.

Let $b, c \in F$. The problem of finding the coset weight distribution of $Z_4$-linear Goethals codes $G_4$, is transformed into solving the following nonlinear system of equations.
equations over $F$ [3]:

\[
\begin{align*}
  x + y + z + u &= 1 \\
  u^2 + xy + xz + xu + yz + yu + zu &= b^2 \\
  x^3 + y^3 + z^3 + u^3 &= c
\end{align*}
\]  

(2)

where $x, y, z$ and $u$ are pairwise distinct elements of $F$. The number of solutions of (2) (see p.284 of [3]), denoted by $\mu_2(b,c)$, is given by Theorem 4 of [3].

We found that Theorem 4 of [3], which gives the explicit evaluation of $\mu_2(b,c)$, is wrong for even $m$. It is obvious that the authors of [3] forgot to take account of the fact, that $\text{Tr}(1) = 1$ for $m$ odd and 0 for $m$ even, in the last step of the proof of Theorem 4. The following is the correct version of Theorem 4 of [3]:

**Theorem 1** Let $\mu_2(b,c)$ be the number of different 4-tuples $(x, y, z, u)$, where $x, y, z, u$ are pairwise distinct elements of $F$, which are solutions to the system (2) over $F$, where $b, c$ are arbitrary elements of $F$.

(1) If $m$ is odd and $\text{Tr}(c) = 1$ or $m$ is even and $\text{Tr}(c) = 0$, then

$$\mu_2(b,c) = \frac{1}{6} \left( q - 8 + (-1)^{\text{Tr}(b)} (K(k_1 k_2) - 3) \right).$$

(3)

(2) If $m$ is odd and $\text{Tr}(c) = 0$ or $m$ is even and $\text{Tr}(c) = 1$, then

$$\mu_2(b,c) = \frac{1}{6} \left( q - 2 - (-1)^{\text{Tr}(b)} (K(k_1 k_2) + 3) \right).$$

(4)

Where $k_1 = b^2 + c + 1$ and $k_2 = b^2 + b + c + \sqrt{c}$.

In this note, we will show that Theorem 4 of [3] implies not only a series of new Kloosterman sum identities, but almost all previously discovered formulas on the identities for Kloosterman sums, thanks to the following theorem which is a corollary of that theorem, too:

**Theorem 2** Let $b, c \in F$, $k_1 = b^2 + c + 1$ and $k_2 = b^2 + b + c + \sqrt{c}$. If $k_1 k_2 \neq 0$, then

$$K(k_1 k_2) = K(k_1 k_2 + k_2).$$

(5)

The idea is to affect a special value to $k_1$ or $k_2$ and then substitute them into (5) to arrive at a special Kloosterman sum identity. Let $b, c \in F$, and $n, k$ be rational numbers such that $b^n, b^k, c^n, c^k$ are elements of $F$. In the sequel, $k_1$ and $k_2$ are affected to the following values:

\[
\begin{align*}
  k_1 &\in \{ cb^n, b^2c^n, cb^n + b^k, b^2c^n + c^k \}, \\
  k_2 &\in \{ cb^n + \sqrt{c}, \sqrt{cb^n} + c, b^2c^n + b, bc^n + b^2 \}.
\end{align*}
\]  

(6)

The previously discovered formulas on the identities for Kloosterman sums are stated in the following theorem:

**Theorem 3** Let $a \in F^*$. Then
\(1\) \(K(a^3(a+1)) = K(a(a+1)^3)\) \[\text{(Helleseth-Zinoviev Formula I)}\].
\(2\) \(K(a^5(a+1)) = K((a+1)^5(a^4+a))\) \[\text{(Helleseth-Zinoviev Formula II)}\].
\(3\) \(K(a^8(a^4+a)) = K((a+1)^8(a^4+a))\) \[\text{(Hollmann-Xiang Formula)}\].
\(4\) \(K(a/(a+1)^4) = K(a^3/(a+1)^4)\) \[\text{(Shin-Kumar-Helleseth Formula)}\].

Note that Shin-Kumar-Helleseth Formula can be deduced from Helleseth-Zinoviev Formula I by the variable change \(a = b/(b+1)\). In this note, we will show that except for Helleseth-Zinoviev Formula II, every formula of Theorem 3 can be obtained from Theorem 4 of [3] with help of Theorem 2.

In Section 2, we at first prove Theorem 2 with help of Theorem 1 (Theorem 4 of [3]) and two lemmas of [5], treat in details some cases of (6) for \(k_1, k_2\) which bring us new Kloosterman sum identities, prove Helleseth-Zinoviev Formula and Hollmann-Xiang Formula, and finally generalize Shin-Kumar-Helleseth Formula.

### 2 New identities for Kloosterman sums

#### 2.1 Proof of Theorem 2

Before proving Theorem 2 we need several preliminary lemmas:

**Lemma 1 (1)** Let \(a \in F^\ast\). Then, \(K(a) = K(a^2)\).

**Lemma 2 (7)** Let \(a, b \in F\). Then,
\(1\) \(\text{Tr}(a) = \text{Tr}(a^2), \text{Tr}(a+b) = \text{Tr}(a) + \text{Tr}(b)\).
\(2\) \(\text{Tr}(1) = 1 \text{ if } m \text{ is odd, and } \text{Tr}(1) = 0 \text{ if } m \text{ is even}\).

The symmetry of the solutions of the nonlinear system (2) is characterized by the following two lemmas:

**Lemma 3 [5] Lemma 10** Let \(b, c\) be any elements of \(F\), where \(F\) has order \(2^m\). Let \(m\) be even. Let \(\mu_2(b,c)\) denote the number of solutions to system (2). Then the following symmetry conditions are valid:
\[\mu_2(b,c) = \mu_2(b+1,c)\] \[\text{(7)}\]
and
\[\mu_2(b,c) = \mu_2(b,c+1)\] \[\text{(8)}\]

**Lemma 4 [5] Lemma 11** Let \(b, c\) be any elements of \(F\), where \(F\) has order \(2^m\). Let \(m\) be odd. Let \(\mu_2(b,c)\) denote the number of solutions to system (2). Then the following symmetry conditions are valid:
\[\mu_2(b,c) + \mu_2(b+1,c) = \frac{1}{3} \times \begin{cases} (2^m - 2) & \text{if } \text{Tr}(c) = 0, \\ (2^m - 8) & \text{if } \text{Tr}(c) = 1, \end{cases}\] \[\text{(9)}\]
and
\[\mu_2(b,c) + \mu_2(b,c+1) = \frac{1}{3} \times \begin{cases} (2^m - 2) & \text{if } \text{Tr}(c) = 1, \\ (2^m - 8) & \text{if } \text{Tr}(c) = 0. \end{cases}\] \[\text{(10)}\]
Now, we are ready to prove Theorem 2. The idea of proof is to substitute the formulas for \( \mu_2(b, c) \) from Theorem 4 into the formulas of Lemma 4 for \( m \) even, and into the formulas of Lemma 4 for \( m \) odd.

**Proof (of Theorem 2)**

(1) Case for \( m \) even.

(a) Subcase that \( \text{Tr}(c) = 0 \).

Note that \( \text{Tr}(1) = 0 \) for \( m \) even by Lemma 2 and \( \text{Tr}(b + 1) = \text{Tr}(b) + \text{Tr}(1) = \text{Tr}(b) \). Let \( k_1^1 := (b + 1)^2 + c + 1 \) and \( k_2^1 := (b + 1)^2 + (b + 1) + c + \sqrt{c} \).

It is clear that \( k_1^1 = k_1 + 1, k_2^1 = k_2 \) and \( k_1^1 k_2^1 = k_1 k_2 + k_2 \), where \( k_1 = b^2 + c + 1 \) and \( k_2 = b^2 + b + c + \sqrt{c} \).

From (3) of Theorem 1, we have

\[
\mu_2(b + 1, c) = \frac{1}{6} (q - 8 + (-1)^{\text{Tr}(b+1)} (K(k_1^1 k_2^1) - 3))
\]

and,

\[
\mu_2(b, c) = \frac{1}{6} (q - 8 + (-1)^{\text{Tr}(b)} (K(k_1 k_2) - 3)).
\]

Theorem 2 follows from (11) of Lemma 3 for this subcase.

Let \( k_1^2 := b^2 + (c + 1) + 1, k_2^2 := b^2 + b + (c + 1) + \sqrt{c} + 1 \). It is clear that \( k_1^2 = k_1 + 1, k_2^2 = k_2 \) and \( k_1^2 k_2^2 = k_1 k_2 + k_2 \). Since \( \text{Tr}(c + 1) = \text{Tr}(c) = 0 \), from (3) of Theorem 1 we obtain

\[
\mu_2(b, c + 1) = \frac{1}{6} (q - 8 + (-1)^{\text{Tr}(b)} (K(k_1^2 k_2^2) - 3))
\]

and,

\[
\mu_2(b, c) = \frac{1}{6} (q - 8 + (-1)^{\text{Tr}(b)} (K(k_1 k_2) - 3)).
\]

Again, Theorem 2 follows from (11) of Lemma 3 for this subcase.

(b) Subcase that \( \text{Tr}(c) = 1 \).

For this subcase, we use (4) of Theorem 1 and (7) or (8) of Lemma 3 to prove Theorem 2 and omit the details due to limited space.

(II) Case for \( m \) odd.

For this case, we use (9) or (10) of Lemma 4 and Theorem 1 to prove Theorem 2 which is similar to the case for \( m \) even and omitted.

\[ \Box \]

2.2 New Kloosterman sum identities and the proof of Theorem 4

**Theorem 4** Let \( c \in F \), and \( n \) be a rational number such that \( c^n \) is an element of \( F \). If \( c^{4n} + 1 \neq 0 \), then

\[
K \left( \frac{(c^{n+1} + c^n)(c^{n+1} + 1)}{c^{4n} + 1} \right) = K \left( \frac{(c^{n+1} + c^n)(c^{n+1} + 1)}{c^{4n} + 1} \right). \quad (11)
\]
Let $k_1 = b^2 + c + 1 = b^2 c^n$. Then, $b^2 = (c + 1)/(c^n + 1)$, and $k_1 = (c^{n+1} + c^2)/(c^n + 1)$. Further, we can obtain

$$k_2 = b^2 + b + c + \sqrt{c} = \frac{c + 1}{c^n + 1} + \sqrt{\frac{c + 1}{c^n + 1} + c + \sqrt{c}};$$
$$k_2^2 = \frac{c^2 + 1}{c^{2n} + 1} + \frac{c + 1}{c^n + 1} + c^2 + c = \frac{(c^{n+1} + c^n)(c^{n+1} + 1)}{c^{2n} + 1},$$
$$(k_1 k_2)^2 = \frac{(c^{n+1} + c^n)(c^{n+1} + 1)}{c^{2n} + 1}; (k_1 k_2)^2 + k_2^2 = \frac{(c^{n+1} + c^n)(c^{n+1} + 1)^3}{c^{4n} + 1}.$$

The actual theorem follows from Lemma [1] and Theorem [2].

Let $L(n) := (c^{n+1} + c^n)(c^{n+1} + 1)/(c^{4n} + 1), R(n) := (c^{n+1} + c^n)(c^{n+1} + 1)^3/(c^{4n} + 1)$, then, $K(L(n)) = K(R(n))$. We now prove Helleseth-Zinoviev Formula I by Theorem [4].

**Proof** (of Helleseth-Zinoviev Formula I)

$$L(1) = \frac{(c^2 + c)^3(c^2 + 1)}{c^4 + 1} = \frac{c^3(c + 1)^5}{(c + 1)^4} = c^3(c + 1),$$
$$R(1) = \frac{(c^2 + c)(c^2 + 1)^3}{c^4 + 1} = \frac{c(c + 1)^7}{(c + 1)^4} = c(c + 1)^3.$$

Helleseth-Zinoviev Formula I follows from the case $K(L(1)) = K(R(1))$ of Theorem [4].

**Corollary 1** Let $c \in F$ such that the rational functions in $c$ occurring in the following formulas are valid. Then,

1. $K(c^b(c^2 + c + 1)/(c + 1)^4) = K(c^2(c^2 + c + 1)^3/(c + 1)^4),$
2. $K(c^3(c + 1)/(c^3 + c^4 + 1)) = K(c^3(c + 1)^3/(c^3 + c^4 + 1)),$
3. $K((c + 1)\delta(c^4 + c)) = K(c^3 + 1)^3),$
4. $K((c + 1)+(c^8 + c)) = K((c + 1)^4(c^8 + c)^3).$

**Proof** The first formula of Corollary [1] corresponds to the case $K(L(2)) = K(R(2))$ of Theorem [4], and the second formula to $K(L(3)) = K(R(3))$, which the proofs are analogous to that of Helleseth-Zinoviev Formula I and omitted. We now prove the third formula:

$$L(-1/4) = \frac{(c^{3/4} + c^{-1/4})^3(c^{3/4} + 1)}{c^{-1} + 1}, R(-1/4) = \frac{(c^{3/4} + c^{-1/4})(c^{3/4} + 1)^3}{c^{-1} + 1};$$
$$L(-1/4)^4 = \frac{(c^3 + c^{-1})^3(c^3 + 1)}{c^{-4} + 1} = \frac{(c^4 + 1)^3(c^4 + c)}{c^4 + 1} = (c + 1)^8(c^4 + c),$n
$$R(-1/4)^4 = \frac{(c^3 + c^{-1})(c^3 + 1)^3}{c^{-4} + 1} = \frac{(c^4 + 1)(c^4 + c)^3}{c^4 + 1} = c^3(c^4 + 1)^3.$$
The third formula follows from $K(L(-1/4)) = K(R(-1/4))$ of Theorem 4 and Lemma 1. The fourth formula arises from the case $K(L(1/4)) = K(R(1/4))$ and the fifth formula from $K(L(-1/8)) = K(R(-1/8))$, which the proofs are similar to Corollary 1 and omitted.

\[ \square \]

**Proof (of Hollmann-Xiang Formula)**

From Hellesef-Zinoviev Formula I, we obtain $K(c^3(c^3 + 1)^3) = K(c^8(c^3 + 1)) = \text{c}(c^8(c^4 + c))$. From the third formula of Corollary 1, we have $K((c + 1)^8(c^4 + c)) = K(c^3(c^3 + 1)^3) = K(c^8(c^4 + c))$.

Remark that Shin-Kumar-Helleseth Formula is the specific case $K(L(-2)) = K(R(-2))$ of Theorem 4 which we omit the proof.

2.3 New Kloosterman sum identities and the generalization of Shin-Kumar-Helleseth Formula

In this subsection, we establish several identities for Kloosterman sums which generalize Shin-Kumar-Helleseth Formula.

**Theorem 5** Let $b \in F$, and $n, k$ be rational numbers such that $b^n, b^k$ are elements of $F$. If $b^{4n} + 1 \neq 0$, then,

\[
K\left(\frac{(b^{n+2} + b^k + 1)(b^{n+2} + b^n + b^k)^3}{b^{4n} + 1}\right) = K\left(\frac{(b^{n+2} + b^k + 1)(b^{n+2} + b^n + b^k)^3}{b^{4n} + 1}\right).
\]

**Proof** Let $k_1 = b^2 + c + 1 = cb^n + b^k$, then $c = (b^k + b^2 + 1)/(b^n + 1)$. After an elementary algebraic computation over $\mathbb{F}_2$, we get

\[
\begin{align*}
  k_1^2 &= (b^{n+2} + b^n + b^k)^2/(b^{2n} + 1), \\
  k_2^2 &= (b^{n+2} + b^k + 1)(b^{n+2} + b^n + b^k)/(b^{2n} + 1), \\
  (k_1k_2)^2 &= (b^{n+2} + b^k + 1)(b^{n+2} + b^n + b^k)^3/(b^{4n} + 1), \\
  (k_1k_2)^2 + k_2^2 &= (b^{n+2} + b^k + 1)^3(b^{n+2} + b^n + b^k)/(b^{4n} + 1).
\end{align*}
\]

The actual theorem follows from Lemma 1 and Theorem 2.

\[ \square \]

We obtain the following corollaries by affecting particular values to $n, k$ in Theorem 5, which the proofs are similar to Corollary 1 and omitted.

**Corollary 2** Set $n = 1, k = 0$ in Theorem 5 Then

\[
K\left(\frac{b^3(b^3 + b + 1)^3}{(1+b)^4}\right) = K\left(\frac{b^3(b^3 + b + 1)}{(1+b)^4}\right).
\]

**Corollary 3** Set $n = 1, k = 2$ in Theorem 5 Then

\[
K\left(\frac{(b^3 + b^2 + 1)(b^3 + b^2 + b)^3}{(1+b)^4}\right) = K\left(\frac{(b^3 + b^2 + 1)(b^3 + b^2 + b)}{(1+b)^4}\right).
\]
Corollary 4  Set \( n = -1 \) in Theorem 5. Then
\[
K \left( \frac{(b^{k+1} + b^2 + b)(b^{k+1} + b^2 + 1)^3}{(1 + b)^4} \right) = K \left( \frac{(b^{k+1} + b^2 + b)(b^{k+1} + b^2 + 1)}{(1 + b)^3} \right).
\]

We can obtain analogous results as Theorem 4 and Theorem 5 if we affect one of remainder values from (5) to \( k_1 \) or \( k_2 \). For instance, set \( k_2 := b^2 + b + c + \sqrt{c} = b\sqrt{c} + c \), we obtain

Theorem 6  Let \( b \in F \), and \( n \) be rational number such that \( b^n \) is an element of \( F \). If \( b^{4n} + 1 \neq 0 \), then,
\[
K \left( \frac{(b^{n+1} + b^3)(b^{n+1} + b^n + b^2 + 1)^3}{b^{4n} + 1} \right) = K \left( \frac{(b^{n+1} + b^3)(b^{n+1} + b^n + b^2 + 1)}{b^{4n} + 1} \right).
\]

Proof  The proof for the actual theorem is similar to that of Theorem 4 and Theorem 5 and omitted.

Set \( n = 3 \) in the formula of Theorem 5, we obtain an interesting corollary which the proof is similar to Corollary 1 and omitted:

Corollary 5  Let \( b \in F \) such that \( b^8 + b^4 + 1 \neq 0 \). Then,
\[
K \left( \frac{(b^3 + b^2)(b^3 + b + 1)^3}{b^8 + b^4 + 1} \right) = K \left( \frac{(b^3 + b^2)(b^3 + b + 1)}{b^8 + b^4 + 1} \right).
\]

3 Conclusion

In this note, we obtained a series of new Kloosterman sum identities and rediscovered several previously found formulas with much simpler proof from Theorem 4 of [3]. The exception is that the formula, \( K(a^5(1 + a)) = K(a(1 + a)^5) \), we believe, could not be deduced from Theorem 4 of [3] and Theorem 2.

References

1. Carlitz, L.: Kloosterman sums and finite field extensions, Acta Arithmetica, 15(2), 179-193 (1969).
2. Charpin P., Helleseth T., Zinoviev V.: The divisibility modulo 24 of Kloosterman sums on \( GF(2^m) \), \( m \) odd, Journal of Combinatorial Theory, Series A, 144, 322-338 (2007).
3. Helleseth T., Zinoviev V.: On \( Z_4 \)-Linear Goethals Codes and Kloosterman Sums, Designs, Codes and Cryptography, 17, 269-288 (1999).
4. Helleseth T., Zinoviev V.: New Kloosterman sums identities over \( F_{2^m} \) for all \( m \), Finite Fields Their Appl., 9, 187-193 (2003).
5. Helleseth T., Zinoviev V.: On a new identity for Kloosterman sums and nonlinear system of equations over finite fields of characteristic 2, Discrete Math., 274, 109-124 (2004).
6. Hollmann Henk D.L., Xiang Q.: Kloosterman sums identities over \( F_{2^m} \) for all \( m \), Discrete Math., 279, 277-286 (2004).
7. Lidl R., Niederreiter H.: Finite Fields, Encyclopedia of Mathematics and Its Applications, 2nd ed., Cambridge University Press, Vol. 20 (1997).
8. Shin D.J., Kumar P.V., Helleseth T.: 3-Designs from the \( Z_4 \)-Goethals codes via a new Kloosterman sum identity, Des. Codes Cryptography, 28, 247-263 (2003).
9. Shin D.J., Sung W.J.: A new Kloosterman sum identity over \( F_{2^m} \) for odd \( m \), Discrete Math., 268, 337-341 (2003).