Designs, Codes and Cryptography, 30, 325–343, 2003

Cyclic Relative Difference Sets and their *p*-Ranks

DAVID B. CHANDLER chandler@math.udel.edu
Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

QING XIANG xiang@math.udel.edu
Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

Communicated by: A. Pott

Received May 2, 2001; Revised May 17, 2002; Accepted May 29, 2002

Abstract. By modifying the constructions in Helleseth et al. [10] and No [15], we construct a family of cyclic $((q^{3k}-1)/(q-1), q-1, q^{3k-1}, q^{3k-2})$ relative difference sets, where $q = 3^e$. These relative difference sets are "liftings" of the difference sets constructed in Helleseth et al. [10] and No [15]. In order to demonstrate that these relative difference sets are in general new, we compute p-ranks of the classical relative difference sets and 3-ranks of the newly constructed relative difference sets when $q = 3$. By rank comparison, we show that the newly constructed relative difference sets are never equivalent to the classical relative difference sets, and are in general inequivalent to the affine GMW difference sets.

Keywords: affine GMW difference set, Gauss sum, relative difference set, Singer difference set, Stickelberger's theorem, Teichmüller character

AMS Classification: 05B10, 11T24

1. Introduction

Let G be a finite (multiplicative) group of order mn, and let N be a normal subgroup of order n. A k-element subset D of G is called an (m, n, k, λ) relative difference set in G relative to N if the list of "differences" $d_1 d_2^{-1}$, d_1, $d_2 \in D$, $d_1 \neq d_2$, represents each element in $G \backslash N$ exactly λ times, and represents no elements in N. Thus, D is an (m, n, k, λ) relative difference set in G relative to N if and only if it satisfies the following equation in the group ring $\mathbb{Z}[G]$:

$$\left(\sum_{d \in D} d\right)\left(\sum_{d \in D} d^{-1}\right) = k \cdot 1_G + \lambda\left(\sum_{g \in G} g - \sum_{h \in N} h\right), \tag{1}$$

where 1_G is the identity element of G. If the group G is cyclic, then D is called a cyclic relative difference set. When $n = 1$, D is an (m, k, λ) difference set in the usual sense.

We say that two (m, n, k, λ) relative difference sets D_1 and D_2 in an abelian group G relative to a subgroup N are equivalent if there exists an automorphism α of G and an element $g \in G$ such that $\alpha(D_1) = D_2 g$. In particular, if G is cyclic, then D_1 and D_2

are equivalent if there exists an integer t, $\gcd(t, mn) = 1$, such that $D_1^{(t)} = D_2 g$ for some $g \in G$, where $D_1^{(t)}$ stands for $\{d^t | d \in D_1\}$.

In the case where G is abelian, using the Fourier inversion formula, we obtain the following standard result in the theory of relative difference sets (see Beth et al. [3, p. 374]).

LEMMA 1.1. *Let G be an abelian group of order mn with a subgroup N of order n. Let k and λ be positive integers satisfying $k(k-1) = \lambda n(m-1)$. Then a k-subset D of G is an (m, n, k, λ) relative difference set in G relative to N if and only if for every nontrivial character χ of G,*

$$\chi(D)\overline{\chi(D)} = \begin{cases} k, & \text{if} \quad \chi \mid N \neq 1, \\ k - \lambda n, & \text{if} \quad \chi \mid N = 1. \end{cases} \tag{2}$$

Here, $\chi(D)$ stands for $\sum_{d \in D} \chi(d)$, and $\chi \mid_N$ is the restriction of χ to N.

The following well-known proposition (Beth et al. [3, p. 370], Elliot and Butson [6]) shows that relative difference sets can be thought of as "liftings" or "extensions" of difference sets.

PROPOSITION 1.2. *Let D be an (m, n, k, λ) relative difference set in G relative to N. Let U be a normal subgroup of G of order u contained in N, and let $\rho : G \to G/U$ be the natural epimorphism. Then $\rho(D)$ is an $(m, n/u, k, \lambda u)$ relative difference set in G/U relative to N/U. In particular, if $U = N$, then $\rho(D)$ is an $(m, k, \lambda n)$ difference set in G/N.*

The first examples of relative difference sets are due to Bose [4]. His construction admits the following well-known generalization (see Pott [17, p. 47]). Let $\mathbb{F}_{q^m}$ be the finite field with q^m elements, q being a power of a prime p, and let $\mathrm{Tr}_{q^m/q}$ be the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Define

$$R = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x) = 1\}.$$

Then R is a $((q^m - 1)/(q-1), q-1, q^{m-1}, q^{m-2})$ relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_q^*$. We will include a proof of this fact by using Lemma 1.1 and Gauss sums in Section 4 since we will need the character values of R in the p-rank computations. Let $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ denote the natural epimorphism. By Proposition 1.2, $\rho(R)$ is a cyclic $((q^m - 1)/(q-1), q^{m-1}, q^{m-2}(q-1))$ difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. Indeed, $\rho(R)$ is the complement of the Singer difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. So the relative difference set R is a lifting of the complement of the Singer set, and for this reason, R is called a classical relative difference set. (Some authors call it a classical affine difference set.) A relative difference set with the same parameters as those of R will be called a relative difference set with classical parameters.

Relative difference sets with classical parameters are important in many ways. First, their projections are difference sets with classical parameters by Proposition 1.2. Second, they are useful in recursive constructions of difference sets with classical

parameters such as the (general) GMW construction (see Pott [17, p. 75] and Jungnickel and Tonchev [11]). We emphasize that in the general GMW construction, the relative difference set used need not come from the classical relative difference set. The only requirement is that it come from the projection of a relative difference set with classical parameters (see the discussion in Pott [17, p. 88]). Third, relative difference sets with classical parameters are useful for constructions of difference families, which, in turn, are useful for constructions of Hadamard matrices (see Spence [20], Yamada [21]). For more details on these relative difference sets, we refer the reader to Pott [17].

In this paper, by modifying the constructions in Helleseth et al. [10] and No [15], we construct a family of $((q^{3k}-1)/(q-1), q-1, q^{3k-1}, q^{3k-2})$ cyclic relative difference sets, where $q = 3^e$. These relative difference sets are "liftings" of the difference sets constructed in Helleseth et al. [10] and No [15]. In order to demonstrate that these relative difference sets are in general new, we derive a general formula for the p-ranks of the classical relative difference sets (Theorem 4.1) and compute the 3-ranks of the newly constructed relative difference sets when $q = 3$ (Theorem 5.5). By rank comparison, we show that the newly constructed relative difference sets are never equivalent to the classical relative difference sets, and are in general inequivalent to the affine GMW difference sets. Along the way, we also show that when $k = 1$, the projection of the new relative difference set is equivalent to the Singer difference sets. The actual relation of these two difference sets was conjectured in No [15].

2. Preliminaries

We first introduce the definition of Gauss sums. Let $\mathbb{F}_q$ be the finite field with q elements, q being a power of a prime p. Let ξ_p be a fixed complex primitive p-th root of unity and let $\mathrm{Tr}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi(x) = \xi_p^{\mathrm{Tr}_{q/p}(x)},$$

which is easily seen to be a nontrivial character of the additive group of $\mathbb{F}_q$. Let

$$\chi : \mathbb{F}_q^* \to \mathbb{C}^*,$$

be a multiplicative character of $\mathbb{F}_q^*$.

Define the Gauss sum by

$$g(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi(a).$$

Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of

$\psi \mid_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q$. That is, for every $c \in \mathbb{F}_q^*$,

$$\psi(c) = \frac{1}{q-1} \sum_{\chi \in X} g(\chi)\chi^{-1}(c), \tag{3}$$

where X denotes the character group of $\mathbb{F}_q^*$.

One of the elementary properties of Gauss sums is Berndt et al. [2, Theorem 1.1.4]

$$g(\chi)\overline{g(\chi)} = q, \quad \text{if} \quad \chi \neq 1. \tag{4}$$

A deeper result on Gauss sums is Stickelberger's theorem (Theorem 2.1 below) on the prime ideal factorization of Gauss sums. We first introduce some notation.

Let p be a prime, $q = p^e$, and let ξ_{q-1} be a complex primitive $(q-1)$-th root of unity. Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{p}$ is a finite field of order q, which we identify with $\mathbb{F}_q$. Let $\omega_\mathfrak{p}$ be the Teichmüller character on $\mathbb{F}_q$, i.e., an isomorphism

$$\omega_\mathfrak{p} : \mathbb{F}_q^* \to \{1, \xi_{q-1}, \xi_{q-1}^2, \ldots, \xi_{q-1}^{q-2}\},$$

satisfying

$$\omega_\mathfrak{p}(\alpha) (\mathrm{mod}\ \mathfrak{p}) = \alpha, \tag{5}$$

for all α in $\mathbb{F}_q^*$.The Teichmüller character $\omega_\mathfrak{p}$ has order $q-1$; hence it generates all multiplicative characters of $\mathbb{F}_q$.

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{p}$. For an integer a, let

$$s(a) = v_\mathfrak{P}(g(\omega_\mathfrak{p}^{-a})),$$

where $v_\mathfrak{P}$ is the $\mathfrak{P}$-adic valuation. Thus $\mathfrak{P}^{s(a)} \,||\, g(\omega_\mathfrak{p}^{-a})$. The following evaluation of $s(a)$ is due to Stickelberger (see Lang [13, p. 7], Berndt et al. [2, p. 344]).

THEOREM 2.1. *Let p be a prime, and $q = p^e$. For an integer a not divisible by $q-1$, let $a_0 + a_1 p + a_2 p^2 + \cdots + a_{e-1}p^{e-1}$, $0 \leq a_i \leq p-1$, be the p-adic expansion of the reduction of a modulo $q-1$. Then*

$$s(a) = a_0 + a_1 + \cdots + a_{e-1},$$

that is, $s(a)$ is the sum of the p-adic digits of the reduction of a modulo $q-1$. Furthermore, define

$$\gamma(a) = a_0! a_1! \cdots a_{m-1}!.$$

Then with $s(a)$ and ω as above we have the congruence

$$\frac{g(\omega^{-a})}{(\xi_p - 1)^{s(a)}} \equiv \frac{-1}{\gamma(a)} (\mathrm{mod}\ \mathfrak{P}).$$

We now define the p-rank of a relative difference set, analogously to the p-rank of a difference set. Let G be a (multiplicative) abelian group of order mn with a subgroup N of order n, and let D be an (m, n, k, λ) relative difference set in G relative to N. Then we can construct a square (m, n, k, λ) divisible design $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ as follows. The points in $\mathscr{P}$ are the group elements of G, which are naturally partitioned into m classes Ng, where g runs through a complete set of coset representatives of N in G. The blocks of $\mathscr{D}$ are the translates Dg, $g \in G$, of D. Two points in distinct point classes are contained in exactly λ blocks, and two points in the same point class are not contained in any block. Moreover the group G is a sharply transitive automorphism group of $\mathscr{D}$. We may define the usual point-block incidence matrix of $\mathscr{D}$ in the standard manner. The vector space over $\mathbb{F}_p$ spanned by the column vectors (characteristic vectors of blocks) of a point-block incidence matrix of $\mathscr{D}$ is called the p-ary code of $\mathscr{D}$, denoted by $\mathscr{C}_p(\mathscr{D})$. The $\mathbb{F}_p$-dimension of $\mathscr{C}_p(\mathscr{D})$ is called the p-rank of the relative difference set D. It is known that $\mathscr{C}_p(\mathscr{D})$ is of interest only if $p \mid (k - \lambda n)$ or $p \mid k$ (see Pott [17]). So from now on, we always assume that $p \mid (k - \lambda n)$ or $p \mid k$. As in the case of difference sets, the p-ranks of relative difference sets can help us distinguish nonisomorphic divisible designs, in particular, inequivalent relative difference sets.

In our computation of p-ranks of relative difference sets, we will take the well known approach described by the following lemma.

LEMMA 2.2. *Let G be an Abelian group of order $v = mn$ and exponent v^*, let p be a prime not dividing v^*, and let $\mathfrak{p}$ be a prime ideal above p in $\mathbb{Z}[\xi_{v^*}]$. Let D be an (m, n, k, λ) relative difference set in G relative to a subgroup N of G. Then the p-rank of D is equal to the number of complex characters χ of G with $\chi(D) \not\equiv 0 \pmod{\mathfrak{p}}$.*

For the proof of this lemma, we refer the reader to Pott [17, p. 25], and Beth et al. [3, p. 465].

3. Some New Cyclic Relative Difference Sets

In this section, we modify the constructions in Helleseth et al. [10] and No [15] to get some cyclic $((q^{3k} - 1)/(q - 1), q - 1, q^{3k-1}, q^{3k-2})$ relative difference sets in $\mathbb{F}_{q^{3k}}^*$ relative to $\mathbb{F}_q^*$, where $q = 3^e$, $e \geq 1$. We need the following lemma on certain binomial additive character sums.

LEMMA 3.1. *Let $q = 3^e$, $e \geq 1$, $d = q^{2k} - q^k + 1$, and let $\xi_3 = e^{2\pi i/3}$. Then*

$$\sum_{x \in \mathbb{F}_{q^{3k}}} \xi_3^{\mathrm{Tr}_{q^{3k}/3}(x + ux^d)} = 0,$$

for all $u \in \{(z+1)^d - z^d \mid z \in \mathbb{F}_{q^{3k}}\}$.

The proof of this lemma uses the theory of quadratic forms over finite fields, and is completely analogous to that of Theorem 1 in Helleseth [10] (simply change 3 in the proof of that theorem to $3^e = q$). So we omit it.

THEOREM 3.2. *Let $q = 3^e$, $e \geq 1$, let $d = q^{2k} - q^k + 1$, and set*

$$D = \{x \in \mathbb{F}_{q^{3k}} \mid \mathrm{Tr}_{q^{3k}/q}(x + x^d) = 1\}. \tag{6}$$

Then D is a cyclic $((q^{3k}-1)/(q-1), q-1, q^{3k-1}, q^{3k-2})$ relative difference set in $\mathbb{F}^*_{q^{3k}}$ relative to $\mathbb{F}^*_q$.

Proof. Let L be a system of coset representatives of $\mathbb{F}^*_q$ in $\mathbb{F}^*_{q^{3k}}$, and let $L_0 = \{x \in L \mid \mathrm{Tr}_{q^{3k}/q}(x + x^d) = 0\}$. If $x \in L$ and $\mathrm{Tr}_{q^{3k}/q}(x + x^d) = a \neq 0$, then we may replace x by x/a, and

$$\mathrm{Tr}_{q^{3k}/q}\left(\frac{x}{a} + \left(\frac{x}{a}\right)^d\right) = \mathrm{Tr}_{q^{3k}/q}(x + x^d)/a = 1.$$

Therefore we may choose L such that $L = L_0 \cup L_1$, where $L_1 = \{x \in L \mid \mathrm{Tr}_{q^{3k}/q}(x + x^d) = 1\}$. It is then easy to see that $L_1 = D$.

For any multiplicative character χ of $\mathbb{F}_{q^{3k}}$, we define the sum

$$S_d(\chi) = \sum_{x \in \mathbb{F}^*_{q^{3k}}} \chi(x) \xi_3^{\mathrm{Tr}_{q^{3k}/3}(x+x^d)}. \tag{7}$$

Writing $x = ay$, with $a \in \mathbb{F}^*_q$ and $y \in L$, we have

$$\begin{aligned} S_d(\chi) &= \sum_{a \in \mathbb{F}^*_q} \chi(a) \sum_{y \in L} \chi(y) \xi_3^{\mathrm{Tr}_{q/3}\left(a\mathrm{Tr}_{q^{3k}/q}(y+y^d)\right)} \\ &= \sum_{y \in L_0} \chi(y) \sum_{a \in \mathbb{F}^*_q} \chi(a) + \sum_{y \in L_1} \chi(y) \sum_{a \in \mathbb{F}^*_q} \chi(a) \xi_3^{\mathrm{Tr}_{q/3}(a)}. \end{aligned}$$

If $\chi = 1$, then $S_d(1) = (q-1)|L_0| - |L_1| = q^{3k} - 1 - q|L_1|$.

If $\chi \neq 1$, but $\chi|_{\mathbb{F}^*_q} = 1$, then $S_d(\chi) = -q\chi(L_1)$.

If $\chi \neq 1$, and $\chi|_{\mathbb{F}^*_q} \neq 1$, then $S_d(\chi) = \chi(L_1) \cdot g_1(\chi_1)$, where χ_1 is the restriction of χ to $\mathbb{F}^*_q$, and $g_1(\chi_1)$ is the Gauss sum over the finite field $\mathbb{F}_q$ with respect to χ_1.

In summary, if χ is a nontrivial multiplicative character of $\mathbb{F}_{q^{3k}}$, then

$$\chi(L_1) = \begin{cases} -\frac{1}{q} S_d(\chi), & \text{if} \quad \chi \mid_{\mathbb{F}^*_q} = 1, \\ \frac{S_d(\chi)}{g_1(\chi_1)}, & \text{if} \quad \chi \mid_{\mathbb{F}^*_q} \neq 1. \end{cases} \tag{8}$$

By Lemma 3.1, we see that $S_d(1) = -1$, hence $|L_1| = q^{3k-1}$. Next we compute

$S_d(\chi)\overline{S_d(\chi)}$ for every nontrivial χ.

$$\begin{aligned} S_d(\chi)\overline{S_d(\chi)} &= \sum_{x,y\in\mathbb{F}_{q^{3k}}^*} \chi(x/y)\xi_3^{\mathrm{Tr}_{q^{3k}/3}(x-y+x^d-y^d)} \\ &= \sum_{z\in\mathbb{F}_{q^{3k}}^*} \chi(z) \sum_{y\in\mathbb{F}_{q^{3k}}^*} \xi_3^{\mathrm{Tr}_{q^{3k}/3}(y(z-1)+y^d(z^d-1))} \\ &= (q^{3k}-1) + \sum_{z\in\mathbb{F}_{q^{3k}}^*\setminus\{-1\}} \chi((z+1)/z) \sum_{y\in\mathbb{F}_{q^{3k}}^*} \xi_3^{\mathrm{Tr}_{q^{3k}/3}(y+y^d((z+1)^d-z^d))}. \end{aligned}$$

By Lemma 3.1, we have $S_d(\chi)\overline{S_d(\chi)} = q^{3k}$ for every $\chi \neq 1$. Using this together with (4), we have that, for every $\chi \neq 1$,

$$\chi(L_1)\overline{\chi(L_1)} = \begin{cases} q^{3k-2}, & \text{if} \quad \chi\,|_{\mathbb{F}_q^*} = 1, \\ q^{3k-1}, & \text{if} \quad \chi\,|_{\mathbb{F}_q^*} \neq 1. \end{cases} \tag{9}$$

By Lemma 1.1, L_1 is a cyclic $((q^{3k}-1)/(q-1), q-1, q^{3k-1}, q^{3k-2})$ relative difference set in $\mathbb{F}_{q^{3k}}^*$ relative to $\mathbb{F}_q^*$. This completes the proof. ■

COROLLARY 3.3. *Let D be defined as in* (6), *and let $\rho : \mathbb{F}_{q^{3k}}^* \to \mathbb{F}_{q^{3k}}^*/\mathbb{F}_q^*$ be the natural epimorphism. Then $\rho(D)$ is a $((q^{3k}-1)/(q-1), q^{3k-1}, q^{3k-2}(q-1))$ difference set in $\mathbb{F}_{q^{3k}}^*/\mathbb{F}_q^*$.*

Proof. This follows from Theorem 3.2 and Proposition 1.2. ■

The difference set in Corollary 3.3 was constructed in No [15]. When $k = 1, \rho(D)$ is a $(q^2+q+1, q^2, q(q-1))$ difference set in $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$. The complement of $\rho(D)$ in $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ has parameters $(q^2+q+1, q+1, 1)$, which are the parameters of a projective plane of order q. Since it is generally believed that there is only one equivalent class of planar difference sets of prime power order, there is a question of verifying that when $k = 1, \rho(D)$ is equivalent to the complement of the planar Singer difference set. We answer this question in the following proposition.

PROPOSITION 3.4. *Let $q = 3^e$, $e \geq 1$, $d = q^2 - q + 1$, $\rho : \mathbb{F}_{q^3}^* \to \mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ be the natural epimorphism, and let D be defined as in* (6) *with $k = 1$. Then the complement of $\rho(D)$ is equivalent to the planar Singer difference set by the following relation*:

$$\{\rho(x) \mid x\in\mathbb{F}_{q^3}^*, \mathrm{Tr}_{q^3/q}(x+x^d) = 0\} = \{\rho(x) \mid x\in\mathbb{F}_{q^3}^*, \mathrm{Tr}_{q^3/q}(x^{(q+1)/2}) = 0\}. \tag{10}$$

Proof. Let $x\in\mathbb{F}_{q^3}^*$ satisfy

$$\mathrm{Tr}_{q^3/q}(x^{(q+1)/2}) = x^{(q+1)/2} + x^{(q^2+q)/2} + x^{(q^3+q^2)/2} = 0.$$

Solving for each term and squaring we get

$$x^{q+1} = x^{q+q^2} - x^{q^2}x^{(q+q^3)/2} + x^{1+q^2},$$
$$x^{q^2+q} = x^{q+1} - x^{(q^3+q^2+q+1)/2} + x^{1+q^2},$$
$$x^{q^2+1} = x^{q+1} - x^{q}x^{(q^2+1)/2} + x^{q+q^2}.$$

Substituting these expressions into

$$\mathrm{Tr}_{q^3/q}(x + x^d) = x + x^q + x^{q^2} + x^{q^2-q+1} + x^{1-q^2+q} + x^{q-1+q^2},$$

we get

$$\begin{aligned}\mathrm{Tr}_{q^3/q}(x + x^d) &= x + x^q + x^{q^2} \\ &\quad + (x - x^{(q^2+1)/2} + x^{q^2}) + (x^q - x^{(q+q^3)/2} + x) \\ &\quad + (x^q - x^{(q^3+q^2+q-1)/2} + x^{q^2}) \\ &= -x^{(q^3-1)/2}\mathrm{Tr}_{q^3/q}(x^{(q+1)/2}) = 0.\end{aligned}$$

Since the two sets in (10) have the same cardinality $q + 1$, and now we have shown that the set on the right hand side of (10) is contained in the one on the left hand side, these two sets must be identical. The proof is complete. ■

Remark. The above proposition was conjectured by No [15].

In order to show that the relative difference sets constructed in this section are new, we compute the p-ranks of the classical relative difference sets in Section 4 and the 3-rank of D when $q = 3$ in Section 5.

4. The p-ranks of the Classical Relative Difference Sets

Even though the p-ranks of the Singer difference sets were computed by many people (see MacWilliams and Mann [14], Smith [19], Goethals and Delsarte [8], and Evans et al. [7]), a general p-rank formula for the classical relative difference sets seems not to have appeared anywhere in the literature. In this section, we compute the p-ranks of the classical relative difference sets.

Let $m \geq 2$ be an integer. We define

$$R = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x) = 1\}, \tag{11}$$

where $\mathrm{Tr}_{q^m/q}$ is the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Let χ be a nontrivial multiplicative character of $\mathbb{F}_{q^m}$. The character value $\chi(R) = \sum_{x \in R} \chi(x)$ has been calculated in Berndt et al. [2, p. 389, 400], Yamamoto [22],

Yamada [21] (see also Arasu et al. [1]). So we simply record the result here.

$$\chi(R) = \begin{cases} -\frac{1}{q}g(\chi), & \text{if} \quad \chi|_{\mathbb{F}_q^*} = 1, \\ \frac{g(\chi)}{g_1(\chi_1)}, & \text{if} \quad \chi|_{\mathbb{F}_q^*} \neq 1, \end{cases} \tag{12}$$

where $\chi_1 = \chi|_{\mathbb{F}_q^*}$ (the restriction of χ to $\mathbb{F}_q$), and $g_1(\chi_1)$ is the Gauss sum over $\mathbb{F}_q$ with respect to the character χ_1. By (4), we see that for every nontrivial χ,

$$\chi(R)\overline{\chi(R)} = \begin{cases} q^{m-2}, & \text{if} \quad \chi|_{\mathbb{F}_q^*} = 1, \\ q^{m-1}, & \text{if} \quad \chi|_{\mathbb{F}_q^*} \neq 1. \end{cases} \tag{13}$$

By Lemma 1.1, R is a $((q^m-1)/(q-1), q-1, q^{m-1}, q^{m-2})$ relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_q^*$. This proof appeared in Yamada [21].

Now we are ready to compute the p-rank of R.

THEOREM 4.1. *Let R be the relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_q^*$ defined in* (11). *Let $q = p^e$, where p is a prime. Then the p-rank of R is equal to*

$$\binom{p+m-2}{m-1}^e + \sum_{0<x<(q-1)} \prod_{j=0}^{e-1} \binom{x_j+m-1}{m-1},$$

where $x = \sum_{j=0}^{e-1} x_j p^j, 0 \le x_j \le (p-1)$.

Proof. For $\mathfrak{P}$ a prime ideal in $\mathbb{Z}[\xi_{q^m-1}]$ lying over p, let $\omega_{\mathfrak{P}}$ be the Teichmüller character on $\mathbb{F}_{q^m}^*$. Then any nontrivial character of $\mathbb{F}_{q^m}^*$ takes the form $\omega_{\mathfrak{P}}^{-a}, 0 < a < (q^m-1)$.

By (12), for each a, $0 < a < q^m - 1$, we have

$$\omega_{\mathfrak{P}}^{-a}(R) = \begin{cases} -\frac{1}{q}g(\omega_{\mathfrak{P}}^{-a}), & \text{if} \quad (q-1) \mid a, \\ \frac{g(\omega_{\mathfrak{P}}^{-a})}{g_1(\omega_{\mathfrak{p}}^{-a})}, & \text{if} \quad (q-1) \nmid a, \end{cases} \tag{14}$$

where $g_1(\phi)$ is the Gauss sum over $\mathbb{F}_q$ with respect to the multiplicative character ϕ of $\mathbb{F}_q^*$. Note that here we have used the fact that $\omega_{\mathfrak{P}}|_{\mathbb{F}_q^*} = \omega_{\mathfrak{p}}$, where $\mathfrak{p}$ is the prime ideal in $\mathbb{Z}[\xi_{q-1}]$ lying above p, and lying below $\mathfrak{P}$. To simplify notation, we will supress the index $\mathfrak{P}$ in the character $\omega_{\mathfrak{P}}$ if there is no confusion.

By Lemma 2.2, the p-rank of R is equal to the number of χ, where $\chi = \omega^{-a}, 0 < a < (q^m-1)$, such that $\chi(R) (\mathrm{mod}\ \mathfrak{P}) \neq 0$. Let $\tilde{\mathfrak{P}}$ be the prime ideal of $\mathbb{Z}[\xi_{q^m-1}, \xi_p]$ lying above $\mathfrak{P}$. Since $\tilde{\mathfrak{P}} \mid \chi(R)$ if and only if $\mathfrak{P} \mid \chi(R)$, the p-rank of R is equal to the number of χ such that $\tilde{\mathfrak{P}} \nmid \chi(R)$.

Corresponding to the two cases in (14), we have the following two cases.

Case 1. $\omega^{-a}|_{\mathbb{F}_q^*} = 1$ (i.e., $(q-1) \mid a$). By (14), we have $\omega^{-a}(R) = -(1/p^e)g(\omega^{-a})$. By Theorem 2.1, we have

$$v_{\tilde{\mathfrak{P}}}(g(\omega^{-a})) = s(a),$$

where $s(a)$ is the p-ary weight of $a \pmod{q^m - 1}$. Also it is clear that $v_{\tilde{\mathfrak{P}}}(p^e) = (p-1)e$. Therefore in this case, the number of a, $0 < a < (q^m - 1)$, such that $\omega^{-a}(R) \not\equiv 0 \pmod{\tilde{\mathfrak{P}}}$, is equal to

$$\#\{a \mid 0 < a < (q^m - 1), (q-1) \mid a, s(a) = (p-1)e\}.$$

Let us denote this cardinality by A. It was shown in Evans et al. [7, p. 85] that

$$A = \binom{p+m-2}{m-1}^e.$$

Case 2. $\omega^{-a}|_{\mathbb{F}_q^*} \neq 1$ (i.e., $(q-1) \nmid a$). By (14), we have

$$\omega^{-a}(R) = \frac{g(\omega_{\mathfrak{P}}^{-a})}{g_1(\omega_{\mathfrak{p}}^{-a})}.$$

So in this case the number of a, $0 < a < (q^m - 1)$, such that $\omega^{-a}(R) \not\equiv 0 \pmod{\tilde{\mathfrak{P}}}$, is equal to

$$\#\{a \mid 0 < a < (q^m - 1), (q-1) \nmid a, s(a) = s_1(a)\},$$

where $s_1(a)$ is the p-ary weight of $a \pmod{q-1}$. Let us denote this cardinality by B.

We can compute B as follows. For an integer X, $0 < X < q^m - 1$, we write $X = \sum_{i=0}^{m-1} X_i q^i$, $X_i = \sum_{j=0}^{e-1} X_{ij} p^j$, with $0 \le X_{ij} \le p-1$. Given an $x = \sum_{j=0}^{e-1} x_j p^j$, $0 \le x_j \le p-1$, $0 < x < (q-1)$, since we want to count those X, $0 < X < (q^m - 1)$ such that $X \equiv x \bmod q-1$, and $s(X) = s_1(x)$, we require that

$$\sum_{i=0}^{m-1} X_{ij} = x_j.$$

That is, the addition $X_0 + X_1 + \cdots + X_{m-1} \pmod{q-1}$ has no carry. Given an x_j, there are precisely

$$\binom{x_j + m - 1}{m-1},$$

ways to distribute the quantity x_j over the X_{ij}'s. So for each x, $0 < x < q-1$, the number of "liftings" X, $0 < X < (q^m - 1)$, of x is $\prod_{j=0}^{e-1} \binom{x_j+m-1}{m-1}$. Summing over x,

$0 < x < (q-1)$, we get

$$B = \sum_{0<x<(q-1)} \prod_{j=0}^{e-1} \binom{x_j + m - 1}{m-1},$$

where $x = \sum_{j=0}^{e-1} x_j p^j$, $0 \le x_j \le (p-1)$.

Adding up the expressions for A and B, we obtain the p-rank formula of R stated in the theorem. ■

In some special cases, we can make the p-rank formula in Theorem 4.1 more explicit.

COROLLARY 4.2. *Let R be the relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_q^*$ defined in* (11), *and let $q = 2^e$. Then the 2-rank of R is $(m+1)^e - 1$.*

Proof. By Theorem 4.1, the 2-rank of R is equal to

$$m^e + \sum_{0<x<(q-1)} \prod_{j=0}^{e-1} \binom{x_j + m - 1}{m-1},$$

where $x = \sum_{j=0}^{e-1} x_j 2^j$, $x_j = 0$ or 1. Since $x_j = 0$ or 1, we see that the product $\prod_{j=0}^{e-1} \binom{x_j+m-1}{m-1}$ in the above formula is simply $m^{s(x)}$, where $s(x)$ is the binary weight of $x \pmod{q-1}$. Hence the 2-rank of R is

$$m^e + \sum_{i=1}^{e-1} \binom{e}{i} m^i = (m+1)^e - 1.$$

This completes the proof. ■

For future use, we also consider the case $p = 3$.

COROLLARY 4.3. *Let R be the relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_q^*$ defined in* (11), *and let $q = 3^e$. Then the 3-rank of R is*

$$\binom{m+1}{2}^e + \sum_{0<x<(q-1)} m^{n_1(x)} \binom{m+1}{2}^{n_2(x)},$$

where $n_1(x)$ and $n_2(x)$ are the number of 1's and the number of 2's respectively in the ternary expansion of x. Furthermore, if $e = 1$ (i.e., $q = 3$), then the 3-rank of R is $m(m+3)/2$.

Proof. This follows from Theorem 4.1. The proof is similar to that of Corollary 4.2. ■

5. The 3-ranks of some Non-Classical Relative Difference Sets

In this section, we compute the 3-rank of the relative difference set D constructed in Section 3. In order to state our results, we introduce some notation first.

Let $q = 3^e$, $e \geq 1$, $m = 3k$, let $d = q^{2k} - q^k + 1$, and let $D = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}$ be the relative difference set constructed in Theorem 3.2.

For $\mathfrak{P}$ a prime ideal in $\mathbb{Z}[\xi_{q^m-1}]$ lying over 3, let $\omega_{\mathfrak{P}}$ be the Teichmüller character on $\mathbb{F}_{q^m}$. Then any nontrivial character of $\mathbb{F}_{q^m}^*$ takes the form $\omega_{\mathfrak{P}}^{-a}$, $0 < a < (q^m - 1)$.

As in the proof of Theorem 3.2, we define for each a, $0 < a < q^m - 1$, the sum

$$S_d(\omega_{\mathfrak{P}}^{-a}) = \sum_{x \in \mathbb{F}_{q^m}^*} \omega_{\mathfrak{P}}^{-a}(x) \xi_3^{\mathrm{Tr}_{q^m/3}(x+x^d)}. \tag{15}$$

Let $\tilde{\mathfrak{P}}$ be the prime ideal of $\mathbb{Z}[\xi_{q^m-1}, \xi_3]$ lying above $\mathfrak{P}$, and let

$$t(a) = v_{\tilde{\mathfrak{P}}}(S_d(\omega_{\mathfrak{P}}^{-a})) \tag{16}$$

be the $\tilde{\mathfrak{P}}$-adic valuation of $S_d(\omega_{\mathfrak{P}}^{-a})$.

LEMMA 5.1. *With the above notation, the 3-rank of D is $A + B$, where*

$$A = |\{a \mid 0 < a < (q^m - 1), (q - 1) \mid a, t(a) = 2e\}|,$$

and

$$B = |\{a \mid 0 < a < (q^m - 1), (q - 1) \nmid a, t(a) = s_1(a)\}|.$$

Proof. By Lemma 2.2, the 3-rank of D is equal to the number of χ, where $\chi = \omega_{\mathfrak{P}}^{-a}$, $0 < a < (q^m - 1)$, such that $\chi(D) \pmod{\mathfrak{P}} \neq 0$. Since $\tilde{\mathfrak{P}} \mid \chi(D)$ if and only if $\mathfrak{P} \mid \chi(D)$, the 3-rank of D is equal to the number of χ such that $\tilde{\mathfrak{P}} \nmid \chi(D)$. To simplify notation, we will usually drop the index in $\omega_{\mathfrak{P}}$ if there is no confusion.

Corresponding to the two cases in (8), we have the following two cases.

Case 1. $\omega^{-a} \mid_{\mathbb{F}_q^*} = 1$ (i.e., $(q - 1) \mid a$). By (8), we have $\omega^{-a}(D) = -(1/3^e) S_d(\omega^{-a})$. By definition, we have

$$v_{\tilde{\mathfrak{P}}}(S_d(\omega^{-a})) = t(a).$$

Also it is clear that $v_{\tilde{\mathfrak{P}}}(3^e) = 2e$. Therefore in this case, the number of a, $0 < a < (q^m - 1)$, such that $\omega^{-a}(D) \not\equiv 0 \pmod{\tilde{\mathfrak{P}}}$, is equal to the cardinality of the set

$$\mathscr{A} = \{a \mid 0 < a < (q^m - 1), (q - 1) \mid a, t(a) = 2e\}. \tag{17}$$

We will denote this cardinality by A.

Case 2. $\omega^{-a}|_{\mathbb{F}_q^*} \neq 1$ (i.e., $(q-1)\nmid a$). By (8),

$$\omega^{-a}(D) = \frac{S_d(\omega_{\mathfrak{P}}^{-a})}{g_1(\omega_{\mathfrak{p}}^{-a})}.$$

So in this case the number of a, $0 < a < (q^m-1)$, such that $\omega^{-a}(D) \not\equiv 0 \pmod{\tilde{\mathfrak{P}}}$, is equal to the cardinality of the set

$$\mathscr{B} = \{a \mid 0 < a < (q^m-1), (q-1)\nmid a, t(a) = s_1(a)\}, \tag{18}$$

where $s_1(a)$ is the p-ary weight of $a \pmod{q-1}$. We will denote this cardinality by B.

In summary, the 3-rank of D is $A+B$, where A, B are defined as above. This completes the proof of the lemma. ■

In order to compute explicitly the 3-rank of D, we have to compute $t(a)$ first. By (3), we have

$$\xi_3^{\mathrm{Tr}_{q^m/3}(x^d)} = \frac{1}{q^m-1}\sum_{b=0}^{q^m-2} g(\omega^{-b})\omega^b(x^d).$$

Hence

$$\begin{aligned} S_d(\omega^{-a}) &= \frac{1}{q^m-1}\sum_{x\in\mathbb{F}_{q^m}^*} \omega^{-a}(x)\xi_3^{\mathrm{Tr}_{q^m/3}(x)} \sum_{b=0}^{q^m-2} g(\omega^{-b})\omega^{bd}(x) \\ &= \frac{1}{q^m-1}\sum_{b=0}^{q^m-2} g(\omega^{-b})g(\omega^{bd-a}). \end{aligned}$$

For any integer x not divisible by q^m-1, we as usual use $s(x)$ to denote the 3-adic weight of $x \pmod{q^m-1}$. In addition, if $x \equiv 0 \pmod{q^m-1}$, we set $s(x)=0$. With this convention, using Theorem 2.1, we see that

$$t(a) \geq \min_{0\leq b\leq q^m-2}\{s(b)+s(a-bd)\}. \tag{19}$$

Moreover, if the above minimum is attained at exactly one value of b in $[0, q^m-2]$, then

$$t(a) = \min_{0\leq b\leq q^m-2}\{s(b)+s(a-bd)\}.$$

In general, the function $t(a)$ is hard to control, hence it is difficult to compute explicitly the cardinalities of $\mathscr{A}$ and $\mathscr{B}$ (defined (17) and (18)). However in the case $q=3$ (i.e., $e=1$), the counting problem can be solved easily.

LEMMA 5.2. *Let* $q = 3^e$, $e = 1$, $m = 3k$, $k > 1$ *and* $d = 3^{2k} - 3^k + 1$. *With the definition of* $\mathscr{A}$ *given in* (17), *we have*

$$\begin{aligned}\mathscr{A} = &\{3^i + 3^j \mid 0 \le i \ne j \le m-1\} \cup \{(d + 3^i)3^j \mid 0 \le i,j \le m-1, i \ne k\} \\ &\cup \{2d3^i \mid 0 \le i \le m-1\} \\ &\cup \{d(3^i + 3^j) \mid 0 \le i < j \le m-1, j \ne k+i, j \ne 2k+i\}.\end{aligned}$$

The cardinality of $\mathscr{A}$ *is* $2m^2 - 2m$.

Proof. Let a be an integer such that $0 < a < 3^m - 1$. Then $a \in \mathscr{A}$ if and only if a is even and $t(a) = 2$. By (19), we need to consider $\min_{0 \le b \le 3^m - 2} \{s(b) + s(a - bd)\}$.

The only way for $s(b) + s(a - bd) = 0$ to occur is $a = b = 0$. This does not occur since we require that $a \not\equiv 0 \pmod{3^m - 1}$. Now a is even: $s(b)$ and $s(a - bd)$ are either both even or both odd; so $s(b) + s(a - bd) = 1$ does not occur. Therefore

$$\min_{0 \le b \le 3^m - 2} \{s(b) + s(a - bd)\} \ge 2.$$

We now find all values of a and b for which $s(b) + s(a - bd) = 2$. There are three possibilities:

i. $s(b) = 0$ and $s(a - bd) = 2$,

ii. $s(b) = s(a - bd) = 1$,

iii. $s(b) = 2$ and $s(a - bd) = 0$.

In the first case, $b = 0$ and a has 3-adic weight 2, that is, either $a = 2 \cdot 3^i$, $0 \le i \le m - 1$ or $a = 3^i + 3^j$, $0 \le i \ne j \le m - 1$. But for $a = 2 \cdot 3^i$, there are two b's such that $s(b) + s(a - bd) = 2$, namely $b = 0$ and $b = (1 + 3^k)3^i$. We will show in Lemma 5.3 that $t(2 \cdot 3^i) > 2$; so these a are not contained in $\mathscr{A}$. For $a = (1 + 3^{2k})3^i$, even though there are two b's ($b = 0$ and $b = 3^i$) satisfying $s(b) + s(a - bd) = 2$, we will show in Lemma 5.3 that $t((1 + 3^{2k})3^i) = 2$. For other a's, one can show that there is a *unique* b in the range satisfying $s(b) + s(a - bd) = 2$, hence $t(a) = 2$. Therefore in this case, the total contribution to $\mathscr{A}$ is $\binom{m}{2}$.

In the second case, b has 3-adic weight 1 and a is the sum of bd and another number with 3-adic weight 1. We write $a = (3^i + d)3^j$, $0 \le i,j \le m - 1$. Note that when $i = k$, we have $(3^i + d)3^j = 3^j + 3^{j+2k}$. These are already counted in Case (i); they should be excluded from consideration in this case. For other values of a, one can see that there is a *unique* b such that $s(b) + s(a - bd) = 2$. So we get $m^2 - m$ values of a in this case.

In the third case, b has 3-adic weight 2 and $a = bd$. Write $a = d(1 + 3^i)3^j$. We get another $m + \binom{m}{2}$ values of a, but m of these (i.e., $i = k$, so $a = 2 \cdot 3^j$) should be excluded since they are already considered in Case (i). So the contribution to $\mathscr{A}$ is $\binom{m}{2}$.

To see that each admissible a above is associated with a unique value of b, with the exceptions noted above, it is enough to show that the above three cases produce

distinct a's. Let us consider the ternary expansion of each a. From Case (i), each a is of the form $3^i + 3^j, i \neq j$. As for Case (ii), we have $a = (3^i + d)3^j$, $i \neq k$. Note that d is represented by k 0's, followed by k 2's, and then followed by $(k-1)$ 0's and a 1. If a 1 is added to any place in the first or last group, a unique run of k 2's remains (see (20)). If a 1 is added to any of the 2's but the lowest, the result is a shorter run of 2's and 1's in the low-order places of the first and third groups (see (21)). So the a's from Case (ii) are different from those a's in Case (i) except the ones already noted. For Case (iii), $a = d(1 + 3^i)3^j$, $i \neq k$, we note three possibilities: $i = 0$ and $a = 2d3^j$; $0 < i < k$; and $k < i \leq 3k/2$. If d is doubled, we get $(k-1)$ 2's bordered by 1's (see (22)). If $0 < i < k$, we get a run of $(k-1)$ 2's with a 1 inserted somewhere (see (23)). If $k < i \leq 3k/2$, we get two separated runs of 2's (see (24)). These are all different from the a's from Case (i) or (ii). Finally note also that a never has a period less than $3k$.

$$\begin{aligned} d &= 000022220001 \\ &\underline{+\,001000000000} \\ a &= 001022220001 \end{aligned} \tag{20}$$

$$\begin{aligned} d &= 000022220001 \\ &\underline{+\,000001000000} \\ a &= 000100220001 \end{aligned} \tag{21}$$

$$\begin{aligned} d &= 000022220001 \\ d &= \underline{000022220001} \\ a &= 000122210002 \end{aligned} \tag{22}$$

$$\begin{aligned} d &= 000022220001 \\ &\underline{+\,002222000100} \\ a &= 010021220101 \end{aligned} \tag{23}$$

$$\begin{aligned} d &= 000022220001 \\ &\underline{+\,222000100002} \\ a &= 222100020010 \end{aligned} \tag{24}$$

In summary, we can write down the elements of $\mathscr{A}$ explicitly, and the cardinality of $\mathscr{A}$ is $2\binom{m}{2} + m^2 - m = 2m^2 - 2m$. ■

The following lemma shows that $t(2) > 2$, and $t(1 + 3^{2k}) = 2$. From these, it follows that $t(2 \cdot 3^i) > 2$, and $t((1 + 3^{2k})3^i) = 2$ for all i. These are needed to complete the proof of Lemma 5.2.

LEMMA 5.3. *Using the notation above, we have*

$$v_{\tilde{\mathfrak{B}}}(g(\omega^{-0})g(\omega^{-1-3^k}) + g(\omega^{-0})g(\omega^{-2})) > 2$$

and

$$v_{\tilde{\mathfrak{P}}}(g(\omega^{-0})g(\omega^{-1-3^{2k}}) + (g(\omega^{-1}))^2) = 2.$$

Proof. We use the Stickelberger congruence as stated in Theorem 2.1. Given an integer a in the interval $(0, 3^m - 1)$, we write $a = a_0 + a_1 3 + a_2 3^2 + \cdots + a_{m-1}3^{m-1}$, where $a_i = 0, 1$ or 2 for all i, $0 \le i \le (m-1)$. We remind the reader that $\gamma(a)$ is defined to be $a_0!a_1! \cdots a_{m-1}!$. Since $2 \equiv -1 \pmod{\tilde{\mathfrak{P}}}$, we have $\gamma(a) \equiv 1 \pmod{\tilde{\mathfrak{P}}}$ if the 3-adic expansion of a has an even number of 2's, and $\gamma(a) \equiv -1 \pmod{\tilde{\mathfrak{P}}}$ if the number of 2's is odd. Thus by Stickelberger's congruence,

$$\begin{aligned}\frac{g(\omega^{-0})g(\omega^{-1-3^k}) + g(\omega^{-0})g(\omega^{-2})}{(\xi_3 - 1)^2} &\equiv (-1)\frac{-1}{\gamma(1+3^k)} + (-1)\frac{-1}{\gamma(2)} \\ &\equiv (-1)(-1) + (-1)(1) \\ &\equiv 0 \pmod{\tilde{\mathfrak{P}}},\end{aligned}$$

and

$$\frac{g(\omega^{-0})g(\omega^{-1-3^{2k}}) + (g(\omega^{-1}))^2}{(\xi_3 - 1)^2} \equiv (-1)(-1) + (-1)(-1) \equiv -1 \pmod{\tilde{\mathfrak{P}}}.$$

The conclusion of the lemma now follows. ∎

LEMMA 5.4. *Let* $q = 3^e$, $e = 1$, $m = 3k$, $k > 1$ *and* $d = 3^{2k} - 3^k + 1$. *With the definition of* $\mathscr{B}$ *give in* (18), *we have*

$$\mathscr{B} = \{3^i, d3^i \mid 0 \le i \le m-1\}.$$

Proof. We need to solve for odd a, $0 < a < 3^m - 1$, such that $t(a) = s_1(a)$ where $s_1(a)$ is the 3-adic weight of $a \pmod 2$. That is, $t(a) = 1$. Here we have two cases. Either $s(b) = 0$ and $s(a) = 1$, or $s(b) = 1$ and $a = bd$. So either $a = 3^i$ or $a = d3^i$. For these a's, there is a unique b in the range $[0, 3^m - 2]$ satisfying $s(b) + s(a - bd) = 1$. So $t(a) = \min_{0 \le b \le 3^m - 2}\{s(b) + s(a - bd)\} = 1$. Therefore the lemma follows. ∎

THEOREM 5.5. *Let* $q = 3^e$, $e = 1$, $m = 3k$, $k > 1$ *and* $d = 3^{2k} - 3^k + 1$. *Let* $D = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}$ *be the relative difference set constructed in Theorem 3.2. Then the 3-rank of* D *is* $2m^2$.

Proof. By Lemma 5.1, the 3-rank of D is equal to $|\mathscr{A}| + |\mathscr{B}|$. In Lemma 5.2 and 5.4, we find that when $e = 1, |\mathscr{A}| = 2m^2 - 2m$, and $|\mathscr{B}| = 2m$. So the 3-rank of D is $2m^2$. ∎

Remarks. The 3-rank formula in Theorem 5.5 is not valid in the case $k = 1$ (i.e., $m = 3$). The reason is that when $m = 3$, the elements $2d3^i$, $0 \le i \le m-1$, of the set $\mathscr{A}$ coincide with some of the elements in $\{(d + 3^i)3^j \mid 0 \le i, j \le m-1, i \ne k\} \subset \mathscr{A}$.

In the case $k = 1$, the relative difference set D has parameters $(13, 2, 9, 3)$, and it has 3-rank 12. This relative difference set D is equivalent to the first $(13, 2, 9, 3)$ relative difference set listed on page 90 of Pott [17] (see also Lam [12]). The second $(13, 2, 9, 3)$ relative difference set listed on the same page is the classical relative difference set, which has 3-rank 9.

COROLLARY 5.6. *Let D be defined as in* (6), *and let $\rho : \mathbb{F}_{q^{3k}}^* \to \mathbb{F}_{q^{3k}}^*/\mathbb{F}_q^*$ be the natural epimorphism. Let $e = 1$, $m = 3k$, $k > 1$. Then the 3-rank of $\rho(D)$ is $2m^2 - 2m$.*

Proof. The 3-rank of $\rho(D)$ is equal to the size of $\mathscr{A}$, which is $2m^2 - 2m$ in the case $e = 1$. ■

Remarks. The 3-rank of $\rho(D)$ was computed recently in No et al. [16]. Our method here is different from that of No et al. [16].

6. Inequivalence of Relative Difference Sets

In this section, we use rank comparison to obtain inequivalence results of relative difference sets with classical parameters.

THEOREM 6.1. *Let $q = 3^e$, $e = 1$, $m = 3k$, $k > 1$ and $d = 3^{2k} - 3^k + 1$. Let $D = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}$ be the relative difference set constructed in Theorem 3.2. Then D is inequivalent to the classical relative difference set R with the same parameters.*

Proof. By Theorem 5.5, the 3-rank of D is $2m^2$. On the other hand, by Corollary 4.3, the 3-rank of R is $m(m+3)/2$. These ranks are not equal: the theorem follows. ■

Besides the classical relative difference sets, there is another large family of relative difference sets with classical parameters known previously. These are the so-called affine GMW difference sets. The idea is the same as in the classical GMW construction. We describe the construction of affine GMW difference sets as follows. For more details, see Pott [17, p. 77].

Let $m = st$, where $s > 1$, $t > 1$ are integers, let q be a power of a prime p. Define

$$T = \{x \in \mathbb{F}_{q^t} \mid \mathrm{Tr}_{q^t/q}(x) = 1\},$$

and

$$S = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q^t}(x) = 1\}.$$

Let r be an integer coprime to $q^t - 1$. Then the set $T^{(r)}S$ is a $((q^m - 1)/(q - 1), q - 1, q^{m-1}, q^{m-2})$ relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_q^*$. This is an affine GMW

difference set. If $r = 1$ or r is a power of p, then $T^{(r)}S$ is nothing but the classical relative difference set R. So we will not consider the case where r is a power of p.

In principle, we can also derive a formula for the p-ranks of affine GMW difference sets as we did for GMW difference sets in Arasu et al. [1]. But the formula will be very complicated. So we will use MAGMA (Cannon and Playoust [5]) to do some numerical computations of the 3-ranks of affine GMW difference sets.

EXAMPLE 6.2. *Let $q = 3, m = 6, t = 2$. The possible choices of r are 5, 7. We choose $r = 5$ since $7 \equiv 3 \cdot 5$ (mod 8). Using MAGMA, we find that the 3-rank of the affine GMW difference set $T^{(5)}S$ is 57 (this was also computed by Pott* [17, p. 86]*). On the other hand, the 3-rank of D (defined in Theorem 3.2) in this case is $2m^2 = 72$. Hence D is not equivalent to this affine GMW difference set.*

EXAMPLE 6.3. *Let $q = 3, m = 6, t = 3$. The possible choices of r are 5, 7, 17 and their multiples by powers of 3. Using MAGMA, we find that the 3-rank of $T^{(5)}S$ is 57, the 3-rank of $T^{(7)}S$ is 63, and the 3-rank of $T^{(17)}S$ is 117. (These 3-ranks were also computed by Pott* [17, p. 86].*) On the other hand, the 3-rank of D (defined in Theorem 3.2) in this case is $2m^2 = 72$. Hence D is not equivalent to any of these affine GMW difference sets.*

EXAMPLE 6.4. *Let $q = 3, m = 9, t = 3$. The possible choices of r are 5, 7, 17 and their multiples by powers of 3. Using MAGMA, we find that the 3-rank of $T^{(5)}S$ is 189, the 3-rank of $T^{(7)}S$ is 234, and the 3-rank of $T^{(17)}S$ is 594. On the other hand, the 3-rank of D (defined in Theorem 3.2) in this case is $2m^2 = 162$. Hence D is not equivalent to any affine GMW difference sets.*

These examples show that the relative difference set D is in general not equivalent to affine GMW difference sets. Since there are only two types of relative difference sets with these parameters known (i.e., the classical and affine GMW relative difference sets), the relative difference set D is new.

References

1. K. T. Arasu, H. D. L. Hollmann, K. Player and Q. Xiang, *Codes and Designs* (Columbus, OH, 2000), 9–35, Ohio State Univ. Math. Res. Inst. Publ. 10, de Gruyter, Berlin (2002).
2. B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Wiley Interscience (1998).
3. T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Vol. 1, Second edition, Cambridge University Press, Cambridge (1999).
4. R. C. Bose, An affine analog of Singer's theorem, *J. Indian Math. Soc.*, Vol. 6 (1942) pp. 1–15.
5. J. Cannon and C. Playoust, *An Introduction to MAGMA*, University of Sydney, Australia (1993).
6. J. E. H. Elliott and A. T. Butson, Relative difference sets, *Illinois J. Math.*, Vol. 10 (1966) pp. 517–531.
7. R. Evans, H. D. L. Hollmann, C. Krattenthaler and Q. Xiang, Gauss sums, Jacobi sums and p-ranks of difference sets, *J. Combin. Theory Ser. A*, Vol. 87 (1999) pp. 74–119.
8. J. M. Goethals and P. Delsarte, On a class of majority logic decodable cyclic codes, *IEEE Trans. Inform. Theory*, Vol. 14 (1968) pp. 182–188.

9. B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, *Canad. J. Math.*, Vol. 14 (1962) pp. 614–625.
10. T. Helleseth, P. V. Kumar and H. M. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation, *Designs, Codes and Cryptography*, Vol. 23, No. 2 (2001) pp. 157–166.
11. D. Jungnickel and V. D. Tonchev, Decompositions of difference sets, *J. Algebra*, Vol. 217 (1999) pp. 21–39.
12. C. W. H. Lam, *On relative difference sets*, In *Proc. 7th Manitoba Conference on Numerical Mathematics and Computing* (1977) pp. 445–474.
13. S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York (1978).
14. J. MacWilliams and H. B. Mann, On the p-rank of the design matrix of a difference set, *Inform. Control*, Vol. 12 (1968) pp. 474–488.
15. J.-S. No, *New cyclic difference sets with Singer parameters constructed from d-homogeneous functions*, preprint.
16. J.-S. No, D.-J. Shin and T. Helleseth, *On the p-ranks and characteristic polynomials of cyclic difference sets*, preprint.
17. A. Pott, *Finite geometry and character theory*, Springer LNM 1601 (1995).
18. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. AMS*, Vol. 43 (1938) pp. 377–385.
19. K. J. C. Smith, On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry, *J. Combin. Theory*, Vol. 7 (1969) pp. 122–129.
20. E. Spence, Hadamard matrices from relative difference sets, *J. Combin. Theory*, Vol. 19 (1975) pp. 287–300.
21. M. Yamada, On a relation between a cyclic relative difference sets associated with the quadratic extensions of a finite field and the Szekeres difference set, *Combinatorica*, Vol. 8 (1988) pp. 207–216.
22. K. Yamamoto, On congruences arising from relative Gauss sums, In *Number Theory and Combinatorics*, Japan 1984, World Scientific Publ. (1985) pp. 423–446.