Finite Fields and Their Applications **7,** 165–188 (2001)
doi.10.1006/ffta.2000.0307, available online at http://www.idealibrary.com on IDEAL®

New Partial Difference Sets in $\mathbb{Z}_{p^2}^t$ and a Related Problem about Galois Rings

Xiang-Dong Hou

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435
E-mail: xhou@euler-math.wright.edu

Ka Hin Leung

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260
E-mail: matlkh@nus.edu.sg

and

Qing Xiang

Department of Mathematical Sciences, University of Delaware, Newark, Delaware 19716
E-mail: xiang@math.udel.edu

Communicated by Dieter Jungnickel

Received November 3, 1999; accepted September 2, 2000; published online November 29, 2000

We generalize a construction of partial difference sets (PDS) by Chen, Ray-Chaudhuri, and Xiang through a study of the Teichmüller sets of the Galois rings. Let $R = GR(p^2, t)$ be the Galois ring of characteristic p^2 and rank t with Teichmüller set T and let $\pi: R \to R/pR$ be the natural homomorphism. We give a construction of PDS in R with the parameters $v = p^{2t}$, $k = r(p^t - 1)$, $\lambda = p^t + r^2 - 3r$, $\mu = r^2 - r$, where $r = lp^{t-s(p,t)}$, $1 \le l \le p^{s(p,t)}$, and $s(p, t)$ is the largest dimension of a $GF(p)$-subspace $W \subset R/pR$ such that $\pi^{-1}(W) \cap T$ generates a subgroup of R of rank $< t$. We prove that $s(p, t)$ is the largest dimension of a $GF(p)$-subspace W of $GF(p^t)$ such that $\dim W^p < t$, where W^p is the $GF(p)$-space generated by $\{\prod_{i=1}^{p} w_i \mid w_i \in W, 1 \le i \le p\}$. We determine the values of $s(p, t)$ completely and solve a general problem about $\dim_E W^r$ for an E-vector space W in a finite extension of a finite field E. The PDS constructed here contain the family constructed by Chen, Ray-Chaudhuri, and Xiang and have a wider range of parameters.

Key Words: finite field; Galois ring; partial difference set; Teichmüller set; the Cauchy–Davenport theorem; the Dyson *e*-transform.

1071-5797/00 $35.00

1. INTRODUCTION

Let G be a finite abelian group of order v. A subset $D \subset G$ is called a (v, k, λ, μ)-*partial difference set* (*PDS*) in G if the differences $d_1 d_2^{-1}$ $(d_1, d_2 \in D, d_1 \neq d_2)$ represent each nonidentity element in D exactly λ times and represent each nonidentity element in $G \backslash D$ exactly μ times. A PDS is called *regular* if $e \notin D$ and D is closed under inversion. (The requirement that $e \notin D$ is not essential since D is a PDS if and only if $G \backslash D$ is.) As usual, we identify a subset $D \subset G$ with the element $\sum_{g \in D} g$ in the group algebra $\mathbb{Z}[G]$. Then a subset $D \subset G \backslash \{e\}$ is a regular PDS in G if and only if, for every character χ of G,

$$\chi(D) = \begin{cases} k, & \text{if } \chi \text{ is principal,} \\ a \text{ or } b, & \text{if } \chi \text{ is nonprincipal,} \end{cases} \tag{1.1}$$

where a and b are real numbers. In this case, the parameters of D are (v, k, λ, μ), where

$$\begin{cases} \lambda = k + ab + a + b, \\ \mu = k + ab. \end{cases} \tag{1.2}$$

The reader is referred to Ma [7] for a thorough survey on the subject of partial difference sets. As described in [7], partial difference sets are closely related to partial geometries, Schur rings, strongly regular graphs, and two-weight codes. Here we point out a new connection between partial difference sets and bent functions on abelian groups. Let G be a finite abelian group and let G^* be the character group of G. A function $f: G \to T = \{z \in \mathbb{C} : |z| = 1\}$ is called a *bent function* if its Fourier transform

$$\begin{aligned} \hat{f}: G^* &\to \mathbb{C} \\ \chi &\mapsto \sum_{g \in G} f(g)\chi(g) \end{aligned} \tag{1.3}$$

has the property that $|\hat{f}(\chi)| = \sqrt{|G|}$ for all $\chi \in G^*$ ([2]). This is a natural generalization of the binary bent functions defined by Rothaus [11] and the q-ary bent functions defined by Kumar *et al.* [3]. Let $D \subset G \backslash \{e\}$ be a partial difference set whose character values are given by (1.1). Define

$$\begin{aligned} f: G &\to T \\ g &\mapsto \begin{cases} 1, & \text{if } g = e, \\ e^{i\alpha}, & \text{if } g \in D, \\ e^{i\beta}, & \text{if } g \in G \backslash (D \cup \{e\}), \end{cases} \end{aligned} \tag{1.4}$$

where α, β are real numbers to be chosen. For each nonprincipal $\chi \in G^*$,

$$\begin{aligned}\hat{f}(\chi) &= \sum_{g \in G} f(g)\chi(g) \\ &= 1 + \chi(D)e^{i\alpha} + \chi(G\backslash(D \cup \{e\}))e^{i\beta} \qquad (1.5) \\ &= \begin{cases} 1 + ae^{i\alpha} + (-a-1)e^{i\beta}, & \text{if } \chi(D) = a, \\ 1 + be^{i\alpha} + (-b-1)e^{i\beta}, & \text{if } \chi(D) = b. \end{cases}\end{aligned}$$

Thus f is a bent function on G if we can choose α and β such that

$$\begin{cases} |1 + ae^{i\alpha} + (-a-1)e^{i\beta}|^2 = |G|, \\ |1 + be^{i\alpha} + (-b-1)e^{i\beta}|^2 = |G|. \end{cases} \qquad (1.6)$$

The general condition for (1.6) to have a solution is rather complicated to describe. However, if D is a Paley PDS in G, i.e., if D is a regular PDS with parameters $(v, (v-1)/2, (v-5)/4, (v-1)/4)$, then system (1.6) always has a solution. Note that in this case the two nonprincipal values a, b of D satisfy $a + b = -1$ and $(a-b)^2 = v$. Let $g(\alpha) = |1 + ae^{i\alpha} + be^{-i\alpha}|^2 - v$. We have $g(0) = -v < 0$, $g(\pi/2) = 1 > 0$ and $g(\pi) = 4 - v$. Thus g has at least one zero in $(0, \pi/2)$. When $v \geq 4$, g also has at least one zero in $(\pi/2, \pi]$. For each zero α_0 of g, $(\alpha, \beta) = (\alpha_0, -\alpha_0)$ is a solution of (1.6).

Most of the known families of PDSs in an abelian group G are obtained using a ring structure on G. When G is an elementary abelian p-group, it has a finite field structure. When G is a non-elementary abelian p-group, what one needs is usually a local ring structure on G. Leung and Ma [4, 5] gave two constructions of partial difference sets in the additive group of $R \times R$ where R is a chain ring; their first construction has been generalized by Hou [2] to the case where R is a quasi-Frobenius local ring. Chen *et al.* [1] constructed a family of PDS in $\mathbb{Z}_{p^2}^t$ by using the Galois ring structure $GR(p^2, t)$ on $\mathbb{Z}_{p^2}^t$. (Also see Ray-Chaudhuri and Xiang [10] and Leung and Ma [6].) It is the construction of [1] that this paper seeks to generalize.

The PDS's constructed in [1] have the following parameters:

$$\begin{aligned} v &= p^{2t}, \\ k &= r(p^t - 1), \\ \lambda &= p^t + r^2 - 3r, \\ \mu &= r^2 - r. \end{aligned} \qquad (1.7)$$

In (1.7), p is a prime, $t > 1$, and

$$r = lp^{t-s} + \varepsilon, \tag{1.8}$$

where s is the largest proper divisor of t and $1 \le l \le p^s$, $\varepsilon = 0$ or 1. One notes that a larger value of s in (1.8) implies a larger range of the parameters of the PDS. However, when t is a prime, its largest proper divisor is 1. The first goal of this paper is to give a family of partial difference sets in $\mathbb{Z}_{p^2}^t$ which contains the family in [1]. The parameters of our PDSs are also given by (1.7) and (1.8). However, in (1.8), s will be replaced by some function $s(p, t)$. The function $s(p, t)$ is the largest integer s such that there is an s-dimensional subspace $W \subset GF(p^t)$ such that the preimage of W in the Teichmüller set of $GR(p^2, t)$ is contained in a subgroup of $GR(p^2, t)$ of rank $< t$. The second goal of this paper is to determine the function $s(p, t)$. To achieve this, we first establish an equivalent definition for $s(p, t)$, which rather surprisingly, is independent of the Galois ring. It turns out that $s(p, t)$ is the largest dimension of a $GF(p)$-subspace W of $GF(p^t)$ such that $\dim W^p < t$, where W^p is the $GF(p)$-vector space generated by $\{\prod_{i=1}^p w_i \mid w_i \in W, 1 \le i \le p\}$. At this point, a more general question arises naturally: Let $E \subset K$ be finite fields with $[K:E] = t$ and let r be a positive integer. What is the largest dimension of an E-subspace W of K such that $W^r \ne K$? We answer this question completely by showing that the largest dimension of such a W is

$$\max_{k|t} k\left(\left\lfloor \frac{t/k - 2}{r} \right\rfloor + 1\right). \tag{1.9}$$

In particular, $s(p, t) = \max_{k|t} k(\lfloor \frac{(t/k)-2}{p} \rfloor + 1)$. It is worth noting that in answering the above question, we proved a vector space analog of the Cauchy–Davenport Theorem ([8, p. 44]) in additive number theory. Returning to PDS, we see that the PDS in this paper have a larger range of parameters than those in [1] since

$$s(p, t) \ge \text{the largest proper divisor of } t \tag{1.10}$$

in general and inequality (1.10) is strict in many cases, especially when t is prime.

The paper is organized as follows. Section 2 provides some algebraic background. It includes a brief review of the Galois rings and a description of the finite abelian p-groups in which every subgroup can be extended to a direct component of the same rank. In Section 3, we give the construction of the partial difference sets. The function $s(p, t)$ arises naturally in the construction. Section 4 establishes the equivalent definition of the function $s(p, t)$. In

Section 5, the above question about $\dim W^r$ is answered and $s(p, t)$ is thus determined.

2. ALGEBRAIC BACKGROUND

We begin with a brief review of the Galois rings. The reader is referred to McDonald [9] for a detailed account of such rings. Let p be a prime and n a positive integer. Let $f \in \mathbb{Z}_{p^n}[x]$ be a monic polynomial of degree t whose image in $\mathbb{Z}_p[x]$ is irreducible. Then the ring structure of $\mathbb{Z}_p[x]/(f)$ depends only on p, n and t but not on the choice of f. The ring $\mathbb{Z}_p[x]/(f)$ is called *the Galois ring of characteristic p^n and rank t* and is denoted by $GR(p^n, t)$. It is known that $GR(p^n, t)$ is a local ring with maximal ideal $pGR(p^n, t)$ and $GR(p^n, t)/pGR(p^n, t) \cong GF(p^t)$. As an $\mathbb{Z}_{p^n}$-module, $GR(p^n, t)$ is free of rank t. The group of units $GR(p^n, t)^*$ of $GR(p^n, t)$ contains an unique cyclic subgroup T^* of order $p^t - 1$. The set $T = T^* \cup \{0\}$ is called *the Teichmüller set of* $GR(p^n, t)$ and it forms a complete system of coset representatives of $GR(p^n, t)/pGR(p^n, t)$. Each element $a \in GR(p^n, t)$ has an unique p-adic expansion

$$a = \xi_0 + p\xi_1 + \cdots + p^{n-1}\xi_{n-1}, \quad \xi_i \in T. \tag{2.1}$$

The Frobenius map

$$\begin{array}{ccc} \sigma: & GR(p^n, t) & \to & GR(p^n, t) \\ & \xi_0 + p\xi_1 + \cdots + p^{n-1}\xi_{n-1} & \mapsto & \xi_0^p + p\xi_1^p + \cdots + p^{n-1}\xi_{n-1}^p \end{array} \tag{2.2}$$

is an automorphism of $GR(p^n, t)$ of order t and $\mathrm{Aut}(GR(p^n, t)) = \langle \sigma \rangle$. The trace map $\mathrm{Tr}: GR(p^n, t) \to \mathbb{Z}_{p^n}$ is defined by

$$\mathrm{Tr}(a) = \sum_{i=0}^{t-1} \sigma^i(a) \quad \text{for all } a \in GR(p^n, t). \tag{2.3}$$

The remainder of this section is devoted to a different question: What kind of finite abelian p-groups G has the property that every subgroup $H < G$ can be extended to a direct component K of G such that $\mathrm{rank}\, K = \mathrm{rank}\, H$? The fact that $\mathbb{Z}_{p^2}^t$ has this property, which can be proved directly, will be used in the next section. Here we give a complete answer to the question because of its general interest.

PROPOSITION 2.1. *Let G be a finite abelian p-group. Then the following are equivalent.*

(i) $G = \mathbb{Z}_{p^n}^a \times \mathbb{Z}_{p^{n-1}}^b$.

(ii) *For each* $H < G$, *there exist* $K, L < G$ *such that* $H \subset K$, $\operatorname{rank} H = \operatorname{rank} K$ *and* $G = K \times L$.

Proof. (i) $\Rightarrow$ (ii). Let $\operatorname{rank} H = r$ and let H be generated by the rows of an $r \times (a+b)$ matrix A. Factor all the powers of p out of the first row of A and let the resulting matrix be

$$\begin{bmatrix} x_1 \cdots x_a \; y_1 \cdots y_b \\ * \end{bmatrix}. \tag{2.4}$$

Then the rows of (2.4) generate a subgroup H_1 of G such that $H_1 \supset H$ and $\operatorname{rank} H_1 = r$.

Case 1. Some x_i is $\not\equiv 0 \pmod p$. Without loss of generality, assume $x_1 = 1$. Let

$$\psi : G \to G$$

$$\alpha \mapsto \alpha \begin{bmatrix} 1 & & & & & & \\ -x_2 & 1 & & & & & \\ \vdots & & \ddots & & & & \\ -x_a & & & 1 & & & \\ -y_1 & & & & 1 & & \\ \vdots & & & & & \ddots & \\ -y_b & & & & & & 1 \end{bmatrix}. \tag{2.5}$$

Then $\psi \in \operatorname{Aut}(G)$ and $\psi(H_1)$ is generated by the rows of

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{bmatrix}. \tag{2.6}$$

Case 2. All $x_i \equiv 0 \pmod p$. Then at least one of y_j is $\not\equiv 0 \pmod p$. We may assume $y_b = 1$. Let

$$\psi : G \to G$$

$$\alpha \mapsto \alpha \begin{bmatrix} 1 & & & & & & -x_1 \\ & \ddots & & & & & \vdots \\ & & 1 & & & & -x_a \\ & & & 1 & & & -y_1 \\ & & & & \ddots & & \vdots \\ & & & & & 1 & -y_{b-1} \\ & & & & & & 1 \end{bmatrix}. \tag{2.7}$$

Then again, $\psi \in \mathrm{Aut}(G)$ and $\psi(H_1)$ is generated by the rows of

$$\begin{bmatrix} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & * & & \vdots \\ & & & 0 \end{bmatrix}. \tag{2.8}$$

Using induction, we see that there are a $\psi \in \mathrm{Aut}(G)$ and a subgroup $K < G$ such that $\psi(H) \subset K$ and K is generated by the rows of an $r \times (a+b)$ matrix which has exactly one 1 in each row and at most one 1 in each column and 0 elsewhere. Thus rank $K = r$ and $G = K \times L$ for some $L < G$. We have $H \subset \psi^{-1}(K)$, rank $\psi^{-1}(K) = r$ and $G = \psi^{-1}(K) \times \psi^{-1}(L)$.

(ii) $\Rightarrow$ (i). Assume $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m} \times \cdots$, where $m \geq n+2$, and consider $H = \langle (1, p, 0, \ldots, 0) \rangle < \mathrm{G}$. Every cyclic subgroup of G containing H has to be H itself. However, H is not a direct component of G. Suppose $G = H \times L$ for some $L < G$. Then

$$\begin{aligned} \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m} \times \{0\} &= G \cap \{(*, *, 0, \ldots, 0)\} \\ &= \langle (1, p, 0, \ldots, 0) \rangle \times (L \cap \{(*, *, 0, \ldots, 0)\}) \\ &\simeq \mathbb{Z}_{p^{m-1}} \times \cdots, \end{aligned} \tag{2.9}$$

which is a contradiction. ■

3. NEW PARTIAL DIFFERENCE SETS IN $\mathbb{Z}_{p^2}^t$

Let $R = GR(p^2, t)$. Let $\ell : R \to \mathbb{Z}_{p^2}$ be a nondegenerate linear map; i.e., $\ker \ell$ does not contain any nonzero ideal of R. (For example, the trace map Tr: $R \to \mathbb{Z}_{p^2}$ is nondegenerate.) Define $\chi : R \to \mathbb{C}$, via $\chi(x) = \zeta^{\ell(x)}$, for all $x \in R$,

where $\zeta = e^{2\pi\sqrt{-1}/p^2}$. Then $\chi_a(\ ) = \chi(a\cdot)$ gives all the additive characters of R as a runs over R. As abelian groups, $R/pR \simeq pR \cong \mathbb{Z}_p^t$. Define

$$\langle \cdot, \cdot \rangle : R/pR \times pR \to p\mathbb{Z}_{p^2} \simeq \mathbb{Z}_p$$

$$\langle \bar{a}, pb \rangle \mapsto \ell(apb), \quad \text{for all } a, b \in R. \tag{3.1}$$

Then $\langle \cdot, \cdot \rangle$ is a well-defined nondegenerate $\mathbb{Z}_p$-bilinear form. Thus for any $\mathbb{Z}_p$-subspaces $A \subset R/pR$, $B \subset pR$, $A^\perp \subset pR$, $B^\perp \subset R/pR$ are defined, and $((\ )^\perp)^\perp = (\ )$, $\dim(\ ) + \dim(\ )^\perp = t$.

LEMMA 3.1. *Let R denote the Galois ring $GR(p^2, t)$ with Teichmüller set T and the group of principal units $T^* = T\backslash\{0\}$. With the above notation, let $W \subset R/pR$ be a $\mathbb{Z}_p$-subspace such that $\pi^{-1}(W) \cap T \subset \ker \ell$, where $\pi : R \to R/pR$ is the projection. Let $\alpha \in pR$ and*

$$D = T^*(1 + \alpha + W^\perp) \subset R. \tag{3.2}$$

Then for each $a \in R$,

$$\chi_a(D) = \begin{cases} |T^*|\,|W^\perp|, & \text{if } a = 0, \\ -|W^\perp|, & \text{if } a \in pR\backslash\{0\}, \\ -|W^\perp|, & \text{if } a = \xi(1 + p\eta), \xi \in T^*, \eta \in T, p\eta + \alpha \notin W^\perp, \\ |pR| - |W^\perp|, & \text{if } a = \xi(1 + p\eta), \xi \in T^*, \eta \in T, p\eta + \alpha \in W^\perp. \end{cases} \tag{3.3}$$

Proof. *Case* 1. $a = 0$. Obvious.

Case 2. $a \in pR\backslash\{0\}$. Let $a = p\xi$ for some $\xi \in T^*$. Then

$$\chi(aD) = \chi(pT^*(1 + \alpha + W^\perp)) = |W^\perp|\chi(pT^*) = |W^\perp|(\chi(pT) - 1) = -|W^\perp|, \tag{3.4}$$

since pT is a subgroup of R and χ is nonprincipal on pT.

Case 3. $a = \xi(1 + p\eta)$, $\xi \in T^*$, $\eta \in T$. Then

$$\begin{aligned} \chi(aD) &= \chi(T^*(1 + \alpha + W^\perp)(1 + p\eta)) \\ &= \chi(T^*(1 + p\eta + \alpha + W^\perp)) \\ &= \sum_{\varepsilon \in T^*} \chi(\varepsilon(1 + p\eta + \alpha))\chi(\varepsilon W^\perp). \end{aligned} \tag{3.5}$$

Note that χ is principal on $\varepsilon W^\perp \Leftrightarrow \varepsilon W^\perp \subset \ker \ell \Leftrightarrow \bar{\varepsilon} \in W$. Thus (3.5) continues as

$$\chi(aD) = |W^\perp| \sum_{\substack{\varepsilon \in T^* \\ \bar{\varepsilon} \in W}} \chi(\varepsilon(1 + p\eta + \alpha))$$

$$= |W^\perp| \left(\sum_{\varepsilon \in \pi^{-1}(W) \cap T} \chi(\varepsilon)\chi(\varepsilon(p\eta + \alpha)) - 1 \right)$$

$$= |W^\perp| \left(\sum_{\varepsilon \in \pi^{-1}(W) \cap T} \chi(\varepsilon(p\eta + \alpha)) - 1 \right), \quad \text{since } \pi^{-1}(W) \cap T \subset \ker \chi. \tag{3.6}$$

Since $p\eta + \alpha \in pR$, $\{\varepsilon(p\eta + \alpha) : \varepsilon \in \pi^{-1}(W) \cap T\}$ is a subgroup of R. Note that χ is principal on this subgroup iff $p\eta + \alpha \in W^\perp$ since $\ell(\varepsilon(p\eta + \alpha)) = \langle \pi(\varepsilon), p\eta + \alpha \rangle$ and $\pi(\pi^{-1}(W) \cap T) = W$. Hence

$$\chi(aD) = \begin{cases} -|W^\perp|, & \text{if } p\eta + \alpha \notin W^\perp, \\ |W^\perp|(|W| - 1) = |pR| - |W^\perp|, & \text{if } p\eta + \alpha \in W^\perp. \end{cases} \tag{3.7}$$

■

THEOREM 3.2. *In the notation of Lemma* 3.1, *let* $\alpha_1, \ldots, \alpha_l \in pR$ *represent distinct cosets in* $pR/W^\perp$, *and let*

$$D = \bigcup_{i=1}^{l} T^*(1 + \alpha_i + W^\perp). \tag{3.8}$$

Then for each $a \in R$,

$$\chi_a(D) = \begin{cases} l|T^*||W^\perp|, & \text{if } a = 0, \\ -l|W^\perp|, & \text{if } a \in pR \backslash \{0\}, \\ -l|W^\perp|, & \text{if } a = \xi(1 + p\eta),\ \xi \in T^*,\ \eta \in T, \\ & p\eta \not\equiv -\alpha_i \pmod{W^\perp} \text{ for all } i, \\ |pR| - l|W^\perp|, & \text{if } a = \xi(1 + p\eta),\ \xi \in T^*,\ \eta \in T, \\ & p\eta \equiv -\alpha_i \pmod{W^\perp} \text{ for some } i. \end{cases} \tag{3.9}$$

The subset D *is a regular PDS in* R *with parameters*

$$v = p^{2t},\ k = l|W^\perp|(p^t - 1),\ \lambda = p^t + l^2|W^\perp|^2 - 3l|W^\perp|,$$

$$\mu = l^2|W^\perp|^2 - l|W^\perp|, \tag{3.10}$$

and $D \cup (pR \setminus \{0\})$ *is a regular PDS in* R *with parameters*

$$v = p^{2t},$$

$$k = (l\,|W^{\perp}| + 1)(p^t - 1),$$

$$\lambda = p^t + (l|W^{\perp}| + 1)^2 - 3(l|W^{\perp}| + 1),$$

$$\mu = (l|W^{\perp}| + 1)^2 - (l|W^{\perp}| + 1). \tag{3.11}$$

Proof. Equation (3.9), which follows directly from (3.3), states that D has only two nonprincipal character values: $-l|W^{\perp}|$ and $p^t - l|W^{\perp}|$. Thus D is a regular PDS in R and (3.10) follows from (1.2). To see the claims about $D \cup (pR \setminus \{0\})$, note that

$$\chi_a(pR \setminus \{0\}) = \begin{cases} |pR| - 1, & \text{if } a \in pR, \\ -1, & \text{if } a \in R \setminus pR. \end{cases} \tag{3.12}$$

Hence $D \cup (pR \setminus \{0\})$ has only two nonprincipal character values: $-(l|W^{\perp}| + 1)$ and $p^t - (l|W^{\perp}| + 1)$. ■

The restriction $\pi|_T : T \to R/pR$ of π is a bijection. Use $\tau : R/pR \to T$ to denote $(\pi|_T)^{-1}$. Note that $\tau : (R/pR)^* \to T^*$ is a group isomorphism. In order for the construction in Theorem 3.2 to work, all we need is a $\mathbb{Z}_p$-subspace W of R/pR such that $\tau(W) \subset \ker \ell$ for some nondegenerate linear map $\ell \in \mathrm{Hom}_{\mathbb{Z}_{p^2}}(R, \mathbb{Z}_{p^2})$. The kernels of nondegenerate linear maps in $\mathrm{Hom}_{\mathbb{Z}_{p^2}}(R, \mathbb{Z}_{p^2})$ are precisely the subgroups of R of the type $\mathbb{Z}_{p^2}^{t-1}$. If $\tau(W)$ generates a subgroup of R of rank $< t$, then by Proposition 2.1, $\tau(W)$ is contained in a subgroup of R of the type $\mathbb{Z}_{p^2}^{t-1}$.

In Theorem 3.2, the range for l is $1 \le l \le p^{\dim W}$. To achieve the maximum range of the parameters in (3.10) and (3.11), we want to maximize $\dim W$. This prompts the following definition.

DEFINITION 3.3. *Let* $R = GR(p^2, t)$ *with Teichmüller set* T *and let* $\tau : R/pR \to T$ *be the inverse of the restriction of* $\pi : R \to R/pR$ *on* T. *Define*

$$s(p, t) = \max\{\dim W : W \text{ is a } \mathbb{Z}_p\text{-subspace of } R/pR \text{ such that } \tau(W) \text{ generates}$$
$$\text{a subgroup of } R \text{ of rank} < t\}. \tag{3.13}$$

COROLLARY 3.4. *Let $R = GR(p^2, t)$. Then there are regular PDS in R with the parameters*

$$\begin{aligned} v &= p^{2t}, \\ k &= r(p^t - 1), \\ \lambda &= p^t + r^2 - 3r, \\ \mu &= r^2 - r, \end{aligned} \tag{3.14}$$

where

$$r = lp^{t-s(p,t)} + \varepsilon, \quad 1 \le l \le p^{s(p,t)}, \quad \varepsilon = 0, 1. \tag{3.15}$$

If s is a proper divisor of t, we have the commutative diagram

$$\begin{array}{ccccc} GR(p^2, s) & \hookrightarrow & GR(p^2, t) & = & R \\ \downarrow \pi & & \downarrow \pi & & \\ GR(p^2, s)/pGR(p^2, s) & \hookrightarrow & GR(p^2, t)/pGR(p^2, t) & & \\ \| & & \| & & \\ GF(p^s) & & GF(p^t) & & \end{array} \tag{3.16}$$

Let W be any one-dimensional $GF(p^s)$-subspace of $GF(p^t)$. Then $\tau(W)$ generates a free $GR(p^2, s)$-submodule of R of rank 1 since $\tau : (R/pR)^* \to T^*$ is a group isomorphism and $\tau(GF(p^s)^*) \subset GR(p^2, s)$. Thus $\tau(W)$ generates a subgroup of R of rank $s < t$. Choosing such a W in Theorem 3.2, one obtains the PDS of [1]. The above arguments also show that $s(p, t)$ is at least as big as the largest proper divisor of t.

For the remainder of this paper, our goal is to determine the function $s(p, t)$ completely.

4. AN EQUIVALENT DEFINITION OF $s(p, t)$

In this section, we give an equivalent definition of $s(p, t)$ (see (4.16) below), which will be used to determine the values of $s(p, t)$ completely in Section 5. We indeed have two different approaches to proving the equivalence of the two definitions of $s(p, t)$ given in (3.13) and in (4.16) respectively. The first approach uses the idea that an additive subgroup of $GR(p^2, t)$ has rank $< t$ if and only if it is contained in the kernel of some order p^2 additive character of

$GR(p^2, t)$. Therefore this approach involves Galois ring traces. The starting point of the second approach is the observation that an additive subgroup H of $GR(p^2, t)$ has rank $< t$ if and only if $\dim_{GF(p)}(H \cap pGR(p^2, t)) < t$. This also leads to a direct proof of the equivalence of the two definitions. Here we present the first approach in its full detail because we feel that some of the ingredients such as the p-adic expansion of the Galois ring traces in the proof might have other uses later on, and the connection with the generalized Reed–Muller codes, in particular the use of derivatives in the proof, might be interesting to people in related areas. We will also briefly sketch the main ideas of the second approach at the end of this section.

Let $R = GR(p^2, t)$. The Teichmüller sets of R and $\mathbb{Z}_{p^2}$ are denoted by $T(R)$ and $T(\mathbb{Z}_{p^2})$ respectively. We will use the same π to denote both homomorphisms from R to R/pR and from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_{p^2}/p\mathbb{Z}_{p^2}$. The inverse maps of $\pi|_{T(R)}: T(R) \to R/pR = GF(p^t)$ and $\pi|_{T(\mathbb{Z}_{p^2})}: T(\mathbb{Z}_{p^2}) \to \mathbb{Z}_{p^2}/p\mathbb{Z}_{p^2} = \mathbb{Z}_p$ are both denoted by τ. Let $\mathrm{Tr}: R \to \mathbb{Z}_{p^2}$ and $\mathrm{tr}: GF(p^t) \to \mathbb{Z}_p$ be the trace maps of R and $GF(p^t)$ respectively. Every $x \in \mathbb{Z}_{p^2}$ can be uniquely written as

$$x = \alpha(x) + p\beta(x), \quad \alpha(x), \beta(x) \in T(\mathbb{Z}_{p^2}). \tag{4.1}$$

Thus we have maps $\alpha, \beta: \mathbb{Z}_{p^2} \to T(\mathbb{Z}_{p^2})$. Obviously,

$$p\beta(x) = x - x^p, \quad \text{for all } x \in \mathbb{Z}_{p^2}. \tag{4.2}$$

Let $\xi \in T(R)$ and $x \in R/pR$. We first need to compute $\mathrm{Tr}((1 + p\xi)\tau(x))$. Using the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\mathrm{Tr}} & \mathbb{Z}_{p^2} \\ \downarrow\pi & & \downarrow\pi \\ R/pR & & \mathbb{Z}_{p^2}/p\mathbb{Z}_{p^2} \\ \| & & \| \\ GF(p^t) & \xrightarrow{\mathrm{tr}} & \mathbb{Z}_p \end{array} \tag{4.3}$$

we have

$$\begin{aligned} \mathrm{Tr}((1 + p\xi)\tau(x)) &= \mathrm{Tr}(\tau(x)) + p\mathrm{Tr}(\xi\tau(x)) \\ &= \alpha(\mathrm{Tr}(\tau(x))) + p\beta(\mathrm{Tr}(\tau(x))) + p\tau(\mathrm{tr}(\pi(\xi)x)) \\ &= \tau(\mathrm{tr}(x)) + p\beta(\mathrm{Tr}(\tau(x))) + p\tau(\mathrm{tr}(\pi(\xi)x)). \end{aligned} \tag{4.4}$$

By (4.2) and straightforward computations, we have

$$p\beta(\mathrm{Tr}(\tau(x))) = \mathrm{Tr}(\tau(x)) - (\mathrm{Tr}(\tau(x)))^p$$
$$= -p\tau(Q(x)), \tag{4.5}$$

where $Q: GF(p^t) \to \mathbb{Z}_p$ is the function defined by

$$Q(x) = \sum_{\substack{j_0 + \cdots + j_{t-1} = p \\ 0 \le j_0, \ldots, j_{t-1} < p}} \frac{(p-1)!}{j_0! \cdots j_{t-1}!} [\sigma^0(x)]^{j_0} \cdots [\sigma^{t-1}(x)]^{j_{t-1}} \tag{4.6}$$

and σ is the Frobenius map of $GF(p^t)$. Therefore

$$\mathrm{Tr}((1 + p\xi)\tau(x)) = \tau(\mathrm{tr}(x)) + p\tau(\mathrm{tr}(\pi(\xi)x) - Q(x)). \tag{4.7}$$

LEMMA 4.1. *Let $s(p, t)$ be defined as in* (3.13). *Then*

$$s(p, t) = \max\{\dim W: W \text{ is a subspace of } R/pR = GF(p^t) \text{ such that } \mathrm{tr}(W) = 0$$
$$\text{and } Q|_W \text{ is linear}\}. \tag{4.8}$$

Proof. Let R^* be the group of units of R. Clearly,

$$s(p, t) = \max\{\dim W: \mathrm{Tr}(a\tau(W)) = 0 \text{ for some } a \in R^*\}$$
$$= \max\{\dim W: \mathrm{Tr}((1 + p\xi)\tau(W)) = 0 \text{ for some } \xi \in T(R)\}. \tag{4.9}$$

However, by (4.7), $\mathrm{Tr}((1 + p\xi)\tau(W)) = 0 \Leftrightarrow \mathrm{tr}(W) = 0$ and $Q|_W(\cdot) = \mathrm{tr}(\pi(\xi)\cdot)$ for some $\xi \in T(R)$; i.e., $Q|_W$ is linear. ■

LEMMA 4.2. *Let R be a commutative ring with identity, p a prime, and*

$$F(X_1, \ldots, X_t) = \sum_{\substack{j_1 + \cdots + j_t = p \\ 0 \le j_1, \ldots, j_t < p}} \frac{(p-1)!}{j_1! \cdots j_t!} X_1^{j_1} \cdots X_t^{j_t} \in R[X_1, \ldots, X_t]. \tag{4.10}$$

Then for any $(a_1, \ldots, a_t) \in R^t$,

$$F(X_1 + a_1, \ldots, X_t + a_t) - F(X_1, \ldots, X_t)$$
$$\equiv (a_1 + \cdots + a_t)(X_1 + \cdots + X_t)^{p-1} - a_1 X_1^{p-1} - \cdots - a_t X_t^{p-1}$$
$$(\mathrm{mod}\ R_{p-2}[X_1, \ldots, X_t]), \tag{4.11}$$

where $R_{p-2}[X_1, \ldots, X_t] = \{f \in R[X_1, \ldots, X_t]: \deg f \le p-2\}$.

Proof. First assume that $\operatorname{char} R = 0$. Since

$$pF = (X_1 + \cdots + X_t)^p - X_1^p - \cdots - X_t^p, \tag{4.12}$$

we have

$$\begin{aligned} &p[F(X_1 + a_1, \ldots, X_t + a_t) - F(X_1, \ldots, X_t)] \\ &\quad \equiv p(a_1 + \cdots + a_t)(X_1 + \cdots + X_t)^{p-1} - pa_1 X_1^{p-1} - \cdots - pa_t X_t^{p-1} \\ &\qquad (\operatorname{mod} R_{p-2}[X_1, \ldots, X_t]) \end{aligned} \tag{4.13}$$

and (4.11) follows. If $\operatorname{char} R \neq 0$, let R' be the polynomial ring over $\mathbb{Z}$ in $|R|$ indeterminants. Then there is an onto homomorphism $\phi: R' \to R$ which induces an onto homomorphism $\phi: R'[X_1, \ldots, X_t] \to R[X_1, \ldots, X_t]$. We obtain formula (4.11) by applying ϕ to the same formula in $R'[X_1, \ldots, X_t]$. ■

Every function $f: GF(p)^t \to GF(p)$ can be uniquely represented as an element in $GF(p)[X_1, \ldots, X_t]/(X_1^p - X_1, \ldots, X_t^p - X_t)$. The degree of such an f is the degree of its polynomial representation. The set of all functions from $GF(p)^t$ to $GF(p)$ of degree $\leq r$, which is a generalized Reed–Muller code, is denoted by $GRM_p(r, t)$. For $f: GF(p)^t \to GF(p)$ and $a \in GF(p)^t$, *the derivative of f in the direction of a* is defined to be

$$\begin{aligned} D_a f: GF(p)^t &\to GF(p) \\ x &\mapsto f(x + a) - f(x). \end{aligned} \tag{4.14}$$

COROLLARY 4.3. *Let Q be the function defined in* (4.6). *For any $a \in GF(p^t)$, we have*

$$(D_a Q)(x) \equiv \operatorname{tr}(a)(\operatorname{tr}(x))^{p-1} - \operatorname{tr}(ax^{p-1}) \quad (\operatorname{mod} GRM_p(p-2, t)). \tag{4.15}$$

Proof. This follows from Lemma 4.2 immediately. ■

THEOREM 4.4. *Let $s(p, t)$ be defined as in* (3.13). *Then*

$$s(p, t) = \max\{\dim W: W \text{ is a subspace of } GF(p^t) \text{ and } \dim W^p < t\}, \tag{4.16}$$

where W^p is the linear span of $\{\prod_{i=1}^p a_i: a_i \in W\}$ over $GF(p)$.

Proof. Let $s = s(p, t)$. By Lemma 4.1, there is an s-dimensional subspace $W \subset GF(p^t)$ such that $\mathrm{tr}|_W = 0$ and $Q|_W$ is linear. Thus for any $a_1, \ldots, a_p \in W$, $(D_{a_1} \cdots D_{a_p} Q)|_W = 0$. But by (4.15),

$$D_{a_1} \cdots D_{a_p} Q = (p-1)!(\mathrm{tr}(a_1) \cdots \mathrm{tr}(a_p) - \mathrm{tr}(a_1 \cdots a_p))$$

$$= -(p-1)!\,\mathrm{tr}(a_1 \cdots a_p). \tag{4.17}$$

Thus $\mathrm{tr}(a_1 \cdots a_p) = 0$. Hence $\dim W^p < t$ and $s \leq$ the RHS of (4.16).

On the other hand, assume that there is a subspace $W \subset GF(p^t)$ such that $\dim W^p < t$. Then there exists $0 \neq a \in GF(p^t)$ such that $\mathrm{tr}(aW^p) = 0$. Let $a = \varepsilon^p$ for some $\varepsilon \in GF(p^t)$, and $V = \varepsilon W$. Then $\mathrm{tr}(V^p) = 0$, hence $\mathrm{tr}|_V = 0$. We claim that $Q|_V$ is linear. Since $Q(rx) = rQ(x)$ for all $x \in GF(p^t)$ and $r \in GF(p)$, it is clear that

$$Q = Q_p + Q_1, \tag{4.18}$$

where Q_p and Q_1 are homogeneous of degrees p and 1. For each $a \in V$, by (4.15), we have

$$(D_a Q)|_V \equiv (\mathrm{tr}(a)(\mathrm{tr}(x))^{p-1} - \mathrm{tr}(ax^{p-1}))|_V \pmod{GRM_p(p-2, t')}$$

$$= 0, \tag{4.19}$$

where $t' = \dim V$. Hence, $Q_p|_V = 0$. Therefore $Q|_V = Q_1|_V$, which is linear. Hence $\dim W = \dim V \leq s(p, t)$; namely, the RHS of (4.16) is $\leq s(p, t)$. This completes the proof. ■

As we mentioned at the beginning of this section, there is a second approach to proving the equivalence of the two definitions of $s(p, t)$. This approach uses the fact that an additive subgroup H of $GR(p^2, t)$ has rank $< t$ if and only if $\dim_{GF(p)}(H \cap pGR(p^2, t)) < t$. We briefly explain the idea of this approach.

Let R and τ be defined as before. Let W be a $GF(p)$-subspace of $GF(p^t)$ and let $\langle \tau(W) \rangle$ be the subgroup of R generated by $\tau(W)$. In order to find the maximum dimension of W such that $\mathrm{rank}(\langle \tau(W) \rangle) < t$, we therefore consider $W' = \langle \tau(W) \rangle \cap pR$. It turns out that by finding a special generating set of W', one can construct a $GF(p)$-subspace V in $GF(p^t)$ such that $\dim_{GF(p)} W = \dim_{GF(p)} V$ and $\dim_{GF(p)} W' = \dim_{GF(p)} V^p$, where V^p is the $GF(p)$-subspace spanned by $\{\prod_{i=1}^p v_i | v_i \in V, 1 \leq i \leq p\}$. It then follows that $s(p, t) = \max\{\dim W : W$ is a subspace of $GF(p^t)$ and $\dim W^p < t\}$. This provides another proof of Theorem 4.4.

5. THE DETERMINATION OF $s(p, t)$

Let t and r be positive integers. We define

$$M(r, t) = \max_{k \mid t} k\left(\left\lfloor \frac{t/k - 2}{r} \right\rfloor + 1\right). \tag{5.1}$$

The main result in this section is the following theorem:

THEOREM 5.1. *Let $E \subset K$ be finite fields with $[K : E] = t$ and let r be a positive integer. Then*

$$M(r, t) = \max\{\dim_E W : W \text{ is an } E\text{-subspace of } K \text{ such that } W^r \neq K\}, \tag{5.2}$$

where W^r is the E-vector space generated by $\{\prod_{i=1}^{r} w_i : w_i \in W,\ 1 \leq i \leq r\}$.

It follows immediately from Theorem 5.1 that $s(p, t) = M(p, t)$. We begin with some preliminary properties of the function $M(r, t)$. Obviously,

$$M(r, t) \geq kM\left(r, \frac{t}{k}\right) \quad \text{for any divisor } k \text{ of } t \tag{5.3}$$

and

$$M(r, t) \geq \frac{t - 1}{r}. \tag{5.4}$$

(To see (5.4), let $k = 1$ in (5.1).) Assume that $r > 1$. Let k be a divisor of t and write $t/k = ar + j$, $0 \leq j \leq r - 1$. Then

$$k\left(\left\lfloor \frac{t/k - 2}{r} \right\rfloor + 1\right) = \begin{cases} ka = \dfrac{t - kj}{r} \leq \dfrac{t}{r}, & \text{if } j = 0, 1, \\ k(a + 1) = \dfrac{t + k(r - j)}{r} > \dfrac{t}{r}, & \text{if } j \geq 2. \end{cases} \tag{5.5}$$

LEMMA 5.2. *Assume that $r > 1$. Let*

$$\mathscr{A} = \{q : q \text{ is a prime divisor of } t \text{ and } q \equiv 0 \text{ or } 1 \pmod{r}\} \tag{5.6}$$

$$\mathscr{B} = \{q : q \text{ is a prime divisor of } t \text{ and } q \not\equiv 0 \text{ or } 1 \pmod{r}\}. \tag{5.7}$$

Then

(i) $M(r, t) = \lfloor t/r \rfloor$ *if* $\mathscr{B} = \emptyset$.

(ii) *If the smallest prime divisor q of t satisfies $q \leq r/2$, then $M(r, t) = t/q$.*

(iii) $M(r, t) = \frac{t}{q}(\lfloor \frac{q-2}{r} \rfloor + 1)$ *for some $q \in \mathscr{B}$ if $\mathscr{B} \neq \emptyset$.*

Proof. (i) Let $M(r,t) = k(\lfloor \frac{(t/k)-2}{r} \rfloor + 1)$, where $k \mid t$, and write $t/k = ar + j$, where $j = 0$ or 1. Then

$$M(r,t) = ka = \frac{t - kj}{r} \leq \left\lfloor \frac{t}{r} \right\rfloor. \tag{5.8}$$

On the other hand,

$$M(r,t) \geq \left\lfloor \frac{t-2}{r} \right\rfloor + 1 = \left\lfloor \frac{t}{r} \right\rfloor. \tag{5.9}$$

This proves (i).

(ii) Let $M(r,t) = k(\lfloor \frac{(t/k)-2}{r} \rfloor + 1)$, where $k \mid t$. Then

$$k\left(\frac{t/k - 2}{r} + 1\right) \geq M(r,t) \geq \frac{t}{q} \geq \frac{2t}{r}, \tag{5.10}$$

which implies that $t/k \leq r - 2$. Thus $M(r,t) = k$. Hence k is the largest proper divisor of t, so $k = t/q$.

(iii) Use induction on t. Again, let $M(r,t) = k(\lfloor \frac{(t/k)-2}{r} \rfloor + 1)$, where $k \mid t$. By (5.5), $t/k \not\equiv 0, 1 \pmod r$. If $k = 1$, choose any $q \in \mathscr{B}$. By (5.5), $\frac{t}{q}(\lfloor \frac{q-2}{r} \rfloor + 1) \geq \lfloor \frac{t-2}{r} \rfloor + 1 = M(r,t)$. Hence $M(r,t) = \frac{t}{q}(\lfloor \frac{q-2}{r} \rfloor + 1)$. If $k > 1$, by the induction hypothesis, $M(r, t/k) = \frac{t}{kq}(\lfloor \frac{q-2}{r} \rfloor + 1)$ for some prime divisor q of t/k with $q \not\equiv 0, 1 \pmod r$. Since

$$M(r,t) = k\left(\left\lfloor \frac{t/k - 2}{r} \right\rfloor + 1\right) \leq kM\left(r, \frac{t}{k}\right) = \frac{t}{q}\left(\left\lfloor \frac{q-2}{r} \right\rfloor + 1\right), \tag{5.11}$$

the conclusion follows. ∎

To prove Theorem 5.1, we need a series of lemmas. Let $E \subset K$ be fields. For any two E-vector spaces A, B of K, define

$$AB = \text{the } E\text{-vector space generated by } \{ab : a \in A, b \in B\}. \tag{5.12}$$

LEMMA 5.3. *Let $E \subset K$ be fields and let A, B be E-subspaces of K such that $0 < \dim_E A < \infty$, $0 < \dim_E B < \infty$, and $AB \neq K$. Then for each $a \in A$, $b \in B$, there exist a proper subfield H_{ab} of K containing E and an H_{ab}-vector space V_{ab} in AB such that $ab \in V_{ab}$ and*

$$\dim_E V_{ab} + \dim_E H_{ab} \geq \dim_E A + \dim_E B. \tag{5.13}$$

Proof. It suffices to prove (5.13) for $ab \neq 0$. Replacing A by $a^{-1}A$ and B by $b^{-1}B$, we may further assume $a = b = 1$, and $1 \in A \cap B$. Use induction on $\dim_E B$. If $\dim_E B = 1$, take $V_{ab} = A$ and $H_{ab} = E$, the result follows. Now assume $\dim_E B > 1$. For any $0 \neq e \in A$, put

$$\begin{aligned} A(e) &= A + Be, \\ B(e) &= B \cap Ae^{-1}. \end{aligned} \tag{5.14}$$

(We mention that $(A(e), B(e))$ is called the Dyson e-transform of (A, B); see [8, p. 42].) Note that $A(e)B(e) \subset AB$ and $\dim_E A(e) + \dim_E B(e) = \dim_E A + \dim_E B$.

Case 1. $B(e) = B$ for all $0 \neq e \in A$. Then $B \subset Ae^{-1}$ for all $0 \neq e \in A$, i.e., $AB \subset A$. Let H be the subfield of K generated by B and let $V = A$. Since $1 \in B$, we have $H \supset E$ and $AB = AH = A$. Therefore A is an H-space, $H \neq K$ as $AB \neq K$, $1 \in V \subset AB$, and

$$\dim_E V + \dim_E H \geq \dim_E B + \dim_E A. \tag{5.15}$$

Case 2. $B(e) \neq B$ for some $0 \neq e \in A$. Then $0 < \dim_E B(e) < \dim_E B$ and $1 \in A(e)$, $1 \in B(e)$. By the induction hypothesis, there exist a proper subfield H of K containing E and an H-vector space $V \subset A(e)B(e) \subset AB$ such that $1 \in V$ and

$$\begin{aligned} \dim_E V + \dim_E H &\geq \dim_E A(e) + \dim_E B(e) \\ &= \dim_E A + \dim_E B. \end{aligned} \tag{5.16}$$

■

In Lemma 5.3, if we do not insist on the subfield H_{ab} being proper, we can drop the condition that $AB \neq K$.

LEMMA 5.4. *Let $E \subset K$ be fields and let A, B be E-subspaces of K such that $0 < \dim_E A < \infty$ and $0 < \dim_E B < \infty$. Then for each $a \in A$, $b \in B$, there exist a subfield H_{ab} of K containing E and an H_{ab}-vector space V_{ab} in AB such that $ab \in V_{ab}$ and*

$$\dim_E V_{ab} + \dim_E H_{ab} \geq \dim_E A + \dim_E B. \tag{5.17}$$

Proof. In the case $AB = K$, simply take $H_{ab} = K$ and $V_{ab} = K$. ■

COROLLARY 5.5. *Let $E \subset K$ be fields such that $[K : E] = t < \infty$. If two E-subspaces A, B of K satisfy $\dim_E A + \dim_E B > t$, then $AB = K$.*

Proof. By Lemma 5.4, there exist a subfield H of K containing E and an H-vector space V in AB such that $\dim_E V > t - \dim_E H$. Since $\dim_E H$ divides both $\dim_E V$ and t, we have $\dim_E V \geq t$. Hence $AB \supset V = K$. ■

COROLLARY 5.6. *Let $E \subset K$ be fields such that $[E:K] = t$ is a prime. Then for any two nonzero E-subspaces of A, B of K,*

$$\dim_E AB \geq \min\{t, \dim_E A + \dim_E B - 1\}. \tag{5.18}$$

Remarks. (i) Corollary 5.6 can be viewed as a vector space analog of the following well-known theorem in additive number theory.

THE CAUCHY–DAVENPORT THEOREM [8, p. 44]. *Let p be a prime and let A, B be nonempty subsets of $\mathbb{Z}_p$. Then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}, \tag{5.19}$$

where $A + B = \{a + b : a \in A, b \in B\}$.

(ii) For finite fields, Corollary 5.6 can be generalized as follows: Let $E \subset K$ be finite fields and let A, B be two nonzero E-subspaces of K. Then

$$\dim_E AB \geq \dim_E A + \dim_E B - \dim_E H(AB), \tag{5.20}$$

where $H(AB) = \{x \in K : xAB \subseteq AB\}$ is the stabilizer of AB in K. This generalization will be proved in a forthcoming paper.

LEMMA 5.7. *Let $E \subset K$ be fields such that $[K:E] = t < \infty$ and let $1 \leq s \leq r$ be integers. Let W be an E-vector space in K with $\dim_E W > M(r, t)$. Then for any $a_1, \ldots, a_s \in W$, there exist a subfield F of K containing E with $\dim_E F = f$, and an F-vector space V in W^s such that $a_1, \ldots, a_s \in V$ and*

$$\dim_E V \geq \begin{cases} sM(r, t) + 1, & \text{if } f = 1, \\ sfM\left(r, \dfrac{t}{f}\right), & \text{if } f > 1. \end{cases} \tag{5.21}$$

Proof. If $s = 1$, choose $V = W$ and $F = E$. So, assume $s \geq 2$. Put $F_1 = E$ and $V_1 = W$. By Lemma 5.4, there exist a subfield F_2 of K containing E and an F_2-vector space V_2 in W^2 such that $a_1 a_2 \in V_2$ and

$$\dim_E V_2 \geq \dim_E W + \dim_E W - \dim_E F_2. \tag{5.22}$$

Apply Lemma 5.4 to the F_2-space V_2 and $F_2 W$, we see that there exist a subfield F_3 of K containing F_2 and an F_3-vector space V_3 in

$V_2F_2W = V_2W \subset W^2$ such that $a_1a_2a_3 \in V_3$ and

$$\dim_E V_3 \geq \dim_E V_2 + \dim_E F_2W - \dim_E F_3. \tag{5.23}$$

Continuing this way, we see that for each $2 \leq i \leq s$, there exist a subfield F_i of K and an F_i-vector space V_i in W^i such that $E = F_1 \subset F_2 \subset \cdots \subset F_s$, $a_1 \ldots a_i \in V_i$ and

$$\dim_E V_i \geq \dim_E V_{i-1} + \dim_E F_{i-1}W - \dim_E F_i. \tag{5.24}$$

Adding up (5.24) for $i = 2, \ldots, s$, we have

$$\dim_E V_s \geq 2\dim_E W - \dim_E F_s + \sum_{i=2}^{s-1} (\dim_E F_iW - \dim_E F_i). \tag{5.25}$$

Put $V = V_s$, $F = F_s$ and $f = \dim_E F_s$. If $f = 1$, then $F_i = E$ for all $2 \leq i \leq s$. Thus by (5.25)

$$\dim_E V \geq s\dim_E W - (s-1) \geq s(M(r,t)+1) - (s-1) = sM(r,t) + 1. \tag{5.26}$$

Without assuming $f = 1$, we have

$$\begin{aligned} \dim_E F_iW - \dim_E F_i &\geq \dim_E W - \dim_E F_i \\ &> M(r,t) - \dim_E F_i \\ &\geq fM\left(r, \frac{t}{f}\right) - \dim_E F_i, \quad 2 \leq i \leq s. \end{aligned} \tag{5.27}$$

Since $\dim_E F_i$ divides both $\dim_E F_iW$ and f, we have $\dim_E F_iW - \dim_E F_i \geq fM(r, \frac{t}{f})$ for all $2 \leq i \leq s$. Thus by (5.25),

$$\begin{aligned} \dim_E V &> 2M(r,t) - f + (s-2)fM(r, \tfrac{t}{f}) \\ &\geq sfM\left(r, \frac{t}{f}\right) - f. \end{aligned} \tag{5.28}$$

Hence $\dim_E V \geq sfM(r, \frac{t}{f})$ since $f | \dim_E V$. ■

LEMMA 5.8. *Let $E \subset K$ be finite fields with $[K:E] = t$ and let r be a positive integer. If W is an E-subspace of K with $\dim_E W > M(r,t)$, then $W^r = K$.*

Proof. The conclusion is obvious when $r = 1$ since $M(1, t) = t - 1$. So assume that $r \geq 2$. Put $W_{r-1} = \{a_1 \cdots a_{r-1} : a_i \in W,\ 1 \leq i \leq r-1\}$. For each $x \in W_{r-1}$, by Lemma 5.7, there exist a subfield F_x of K containing E with $[F_x : E] = f_x$ and an F_x-vector space V_x such that $x \in V_x \subset W^{r-1}$ and

$$\dim_E V_x \geq \begin{cases} (r-1)M(r,t) + 1, & \text{if } f_x = 1, \\ (r-1) f_x M\left(r, \dfrac{t}{f_x}\right), & \text{if } f_x > 1. \end{cases} \tag{5.29}$$

Since $\dim_E F_x W > M(r,t) \geq f_x M(r, \frac{t}{f_x})$ and $f_x | \dim_E F_x W$, we have $\dim_E F_x W \geq f_x(M(r, \frac{t}{f_x}) + 1)$. Thus by (5.29) and (5.4),

$$\dim_E V_x + \dim_E F_x W \geq \begin{cases} rM(r,t) + 2 > t, & \text{if } f_x = 1, \\ r f_x M\left(r, \dfrac{t}{f_x}\right) + f_x \geq t, & \text{if } f_x > 1. \end{cases} \tag{5.30}$$

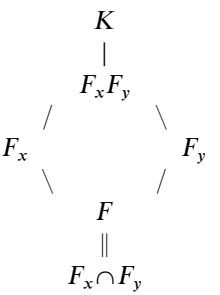
If $\dim_E V_x + \dim_E F_x W > t$, then $K = V_x F_x W \subset W^r$ by Corollary 5.5 and we are done. Thus we assume that $\dim_E V_x + \dim_E F_x W \leq t$ for all $x \in W_{r-1}$. By (5.30), the assumption implies that for all $x \in W_{r-1}$,

(i) $f_x > 1$, and

(ii) $\dim_E F_x W = f_x(M(r, \frac{t}{f_x}) + 1) = \frac{t + (r-1) f_x}{r}$.

We may assume that there exist $x,\ y \in W_{r-1}$ such that $F_x \not\subset F_y$ and $F_y \not\subset F_x$. Otherwise, the subfields F_x, $x \in W_{r-1}$, are linearly ordered, hence $\bigcap_{x \in W_{r-1}} F_x = F_z$ for some $z \in W_{r-1}$. Since $W^{r-1} = \sum_{x \in W_{r-1}} V_x$, we have $F_z W^{r-1} = W^{r-1}$. Then $W^r = (F_z W)^r$, $[K : F_z] < t$, and $\dim_{F_z} F_z W > \frac{1}{f_z} M(r,t) \geq M(r, \frac{t}{f_z})$. Using induction on t, we have $W^r = (F_z W)^r = K$, and we are done in this case.

Now put $F = F_x \cap F_y$, $f = [F : E]$, $g_x = [F_x : F]$, $g_y = [F_y : F]$, $s = [K : F]$, and $U = FW$. Then $g_x > 1$ and $g_y > 1$. We have the following diagram of fields:



(5.31)

Note that $fg_xg_y | t$. Since

$$\dim_E F_xF_yU \geq \dim_E W > M(r,t) \geq fg_xg_yM\left(r, \frac{t}{fg_xg_y}\right) \tag{5.32}$$

and $fg_xg_y | \dim_E F_xF_yU$, we have

$$\begin{aligned}\dim_E F_xF_yU &\geq fg_xg_y\left(M\left(r, \frac{t}{fg_xg_y}\right)+1\right)\\ &\geq fg_xg_y\left(\frac{t/fg_xg_y-1}{r}+1\right) \quad \text{(by (5.4))}\\ &= \frac{t+(r-1)fg_xg_y}{r}. \end{aligned}\tag{5.33}$$

In the same way,

$$\dim_E U \geq \frac{t+(r-1)f}{r}. \tag{5.34}$$

Putting together (5.33), (5.34) and the above condition (ii) on F_x and F_y, we have

$$\begin{aligned}\dim_F U &\geq \frac{s+(r-1)}{r}\\ \dim_F F_xU &= \frac{s+(r-1)g_x}{r}\\ \dim_F F_yU &= \frac{s+(r-1)g_y}{r}\\ \dim_F F_xF_yU &\geq \frac{s+(r-1)g_xg_y}{r}. \end{aligned}\tag{5.35}$$

We now show that (5.35) is impossible. Since $g_x > 1$, we have $\dim_F F_xF_yU > \dim_F F_yU$, hence $F_xU \neq U$. Choose $u \in F_xU \setminus U$ and consider

the homomorphism

$$\phi\colon F_y/F \to F_yU/(F_xU \cap F_yU)$$

$$a \mapsto au. \tag{5.36}$$

Since

$$\begin{aligned}\dim_F(F_y/F) &= g_y - 1\\ &> \frac{r-1}{r}(g_y - 1)\\ &\geq \dim_F F_yU - \dim_F U\\ &\geq \dim_F(F_yU/(F_xU \cap F_yU)),\end{aligned} \tag{5.37}$$

we have $\ker \phi \neq \{0\}$. Thus there exists an $\alpha \in F_y \backslash F$ such that $\alpha u \in F_xU$. Clearly, there is an onto homomorphism

$$\psi\colon (F_xU/U) \otimes_F F_y \to F_xF_yU/F_yU$$

$$v \otimes a \mapsto av. \tag{5.38}$$

But by (5.35), $\dim_F[(F_xU/U) \otimes_F F_y] \leq \frac{r-1}{r}(g_x - 1)g_y \leq \dim_F(F_xF_yU/F_yU)$. Hence $\ker \psi = \{0\}$. However, it is clear that $\psi(\alpha u \otimes 1 - u \otimes \alpha) = 0$, and $0 \neq \alpha u \otimes 1 - u \otimes \alpha \in (F_xU/U) \otimes_F F_y$ since $\alpha \notin F$. We have a contradiction. ■

Now we are ready to prove Theorem 5.1.

Proof of Theorem 5.1. Because of Lemma 5.8, it suffices to find an E-subspace W of K such that $\dim_E W = M(r, t)$ and $W^r \neq K$. We may assume $t > 1$. Let $M(r, t) = k(\lfloor \frac{(t/k)-2}{r} \rfloor + 1)$, where $k \mid t$, $k < t$. Let F be the field such that $E \subset F \subset K$ and $[F:E] = k$. Write $K = F[x]$ $(x \in K)$. Put $n = \lfloor \frac{(t/k)-2}{r} \rfloor$ and let W be the F-subspace of K generated by $\{1, x, \ldots, x^n\}$. Then W^r is the F-subspace generated by $\{1, x, \ldots, x^{nr}\}$. Thus $\dim_E W = k(n+1) = M(r, t)$ and

$$\dim_E W^r = k(nr+1) = k\left(r\left\lfloor \frac{t/k-2}{r} \right\rfloor + 1\right) < t. \tag{5.39}$$

■

COROLLARY 5.9. *Let p be a prime and t a positive integer. Then*

$$s(p, t) = M(p, t) = \max_{k \mid t} k \left(\left\lfloor \frac{t/k - 2}{r} \right\rfloor + 1 \right). \tag{5.40}$$

Remarks. (i) When $p = 2$, by Corollary 5.9 and Lemma 5.2, we have $s(2, t) = \lfloor \frac{t}{2} \rfloor$. This was previously proved in [12] by using some theory of quadratic forms in characteristic two.

(ii) Corollary 5.9 determines the values of $s(p, t)$ completely. Consequently, the range of the parameters of the PDS in Corollary 3.4 is completely determined.

ACKNOWLEDGMENTS

Part of this work was done during the first author's sabbatical visit to INRIA in France. Support from Wright State University and INRIA is gratefully acknowledged. The second author is partially supported by an NUS research grant, Project RP 3982723. The research of the third author was supported in part by NSA Grant MDA 904-99-1-0012.

REFERENCES

1. Y. Chen, D. K. Ray-Chaudhuri, and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings, II, *J. Combin. Theory Ser. A* **76** (1996), 179–196.
2. X. Hou, Bent functions, partial difference sets and quasi-Frobenius local rings, *Des. Codes Cryptogr.* **20** (2000), 251–268.
3. P. V. Kumar, R. A. Scholtz, and L. R. Welch, Generalized bent functions and their properties. *J. Combin. Theory Ser. A* **40** (1985), 90–107.
4. K. H. Leung and S. L. Ma, Construction of partial difference sets and relative difference sets on p-groups, *Bull. London Math. Soc.* **22** (1990), 533–539.
5. K. H. Leung and S. L. Ma, Partial difference sets with Paley parameters. *Bull. London Math. Soc.* **27** (1995), 553–564.
6. K. H. Leung and S. L. Ma, A construction of partial difference sets in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^2}$, *Des. Codes Cryptogr.* **8** (1996), 167–172.
7. S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.
8. M. B. Nathanson, "Additive Number Theory, Inverse Problems and the Geometry of Sumsets", Springer-Verlag, New York, 1996.
9. B. R. McDonald, "Finite Rings with Identity," Dekker, New York, 1974.
10. D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings, *Des. Codes Cryptogr.* **8** (1996), 215–227.
11. O. S. Rothaus, On "bent" functions, *J. Combin. Theory Ser. A* **20** (1976), 300–305.
12. Q. Xiang and J. A. Davis, Constructions of low rank relative difference sets in 2-groups using Galois rings, *Finite Fields Appl.* **6** (2000), 130–145.