Partial difference sets and amorphic group schemes from pseudo-quadratic bent functions

Yu Qing Chen · John Polhill

Received: 1 April 2011 / Accepted: 29 February 2012 / Published online: 22 March 2012
© Springer Science+Business Media, LLC 2012

Abstract We present new abelian partial difference sets and amorphic group schemes of both Latin square type and negative Latin square type in certain abelian p -groups. Our method is to construct what we call pseudo-quadratic bent functions and use them in place of quadratic forms. We also discuss a connection between strongly regular bent functions and amorphic group schemes.

Keywords Amorphic association scheme · Association scheme · Bent function · Partial difference set · Quadratic form · Negative Latin square

1 Introduction

A d -class association scheme $(X; R_0, R_1, \dots, R_d)$ is a finite set X together with a partition $R_0, R_1, \dots, R_d$ of $X \times X$ such that

- (i) $R_0 = \{(x, x) \mid x \in X\}$;
- (ii) $R_i^\top := \{(y, x) \mid (x, y) \in R_i\} \in \{R_1, R_2, \dots, R_d\}$ for all $i = 1, 2, \dots, d$;
- (iii) there are non-negative integers $p_{i,j}^k$, $i, j, k = 0, 1, \dots, d$, such that for any $(x, y) \in R_k$ the number of $z \in X$ with $(x, z) \in R_i$ and $(z, y) \in R_j$ is $p_{i,j}^k$.

An association scheme $(X; R_0, R_1, \dots, R_d)$ is *symmetric* if $R_i^\top = R_i$ for all $i = 1, 2, \dots, d$. It is *commutative* if $p_{i,j}^k = p_{j,i}^k$ for all $i, j, k = 0, 1, \dots, d$. Symmetric

Y.Q. Chen (✉)

Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA
e-mail: yuqing.chen@wright.edu

J. Polhill

Department of Mathematics, Computer Science, and Statistics, Bloomsburg University, Bloomsburg, PA 17815, USA
e-mail: jpolhill@bloomu.edu

schemes are necessarily commutative. We call a scheme $(X; R_0, R_1, \dots, R_d)$ a *group scheme* if X is a group and $(xg, yg) \in R_i$ whenever $(x, y) \in R_i$ for all $g \in X$ and all $i = 0, 1, 2, \dots, d$. Given a finite group G , if $(G; R_0, R_1, \dots, R_d)$ is a group scheme, we define $D_i = \{xy^{-1} \mid (x, y) \in R_i\}$ for all $i = 0, 1, 2, \dots, d$. Then $D_0 = \{0\}$ and $D_0, D_1, \dots, D_d$ form a partition of G and the $\mathbb{Z}$ -linear span of $D_0, D_1, \dots, D_d$ is a subring of the group ring $\mathbb{Z}[G]$. Such a subring is also known as a Schur ring of G [29] and it is the Bose–Mesner ring of the scheme. Conversely, every Schur ring of G gives rise to a group scheme of G and such a scheme will be simply denoted by $(G; D_0, D_1, \dots, D_d)$. For more general discussions of association schemes, we suggest the reader to consult [1, 2, 6, 19].

An association scheme $(X; R_0, R_1, \dots, R_d)$ is said to be *amorphic* if for any partition $S_0, S_1, \dots, S_e$ of $X \times X$ with $S_0 = R_0$ and each S_i being a union of some R_j 's for all $i = 1, 2, \dots, e$, $(X; S_0, S_1, \dots, S_e)$ is also an association scheme. When $d > 2$, such a scheme must be symmetric and, therefore, commutative.

Given a symmetric association scheme $(X; R_0, R_1, \dots, R_d)$, each subset R_i of $X \times X$ can be considered as the edge set of a graph Γ_i whose vertex set is X . Hence a symmetric association scheme can be regarded as an edge-decomposition $\{\Gamma_1, \Gamma_2, \dots, \Gamma_d\}$ of the complete graph on X . Amorphic schemes are closely related to strongly regular graphs and amorphic group schemes are closely related to partial difference sets.

A graph Γ is called a (v, k, λ, μ) -*strongly regular graph* if Γ is a k -regular graph on v vertices such that any two adjacent vertices of the graph share λ common neighbors and any two non-adjacent vertices share μ common neighbors. A subset D of a group G with $1 \notin D$ and $d^{-1} \in D$ for all $d \in D$ is called a regular (v, k, λ, μ) -*partial difference set* if the Cayley graph of G generated by D is a (v, k, λ, μ) -strongly regular graph. This is equivalent to saying that G is a finite group of order v , and D is a subset of size k in G having the property that the differences $d_1 d_2^{-1}$ of elements $d_1, d_2 \in D$ represent each element of D exactly λ times and the nonidentity element of $G \setminus D$ exactly μ times. Non-regular partial difference sets, i.e. partial difference sets containing the identity of G , can be similarly defined. The reader can find more details on strongly regular graphs in [6, 19] and on partial difference sets in [29].

A strongly regular graph with parameters

$$v = n^2, \quad k = r(n-1), \quad \lambda = n + r^2 - 3r, \quad \text{and} \quad \mu = r^2 - r \quad (1)$$

for some integers n and r is called a strongly regular graph with *Latin square type parameters*. When n and r are both positive, the strongly regular graph is known to be of *Latin square type*, and when n and r are both negative, *negative Latin square type*. We will take advantage of the fact that the parameters of these strongly regular graphs are determined by integers n and r and simply call a strongly regular graph having parameters (1) an (n, r) -Latin square type strongly regular graph or (n, r) -negative Latin square type strongly regular graph depending on whether n and r are positive or negative. We will do the same for partial difference sets having parameters (1). For example, given an positive integer r , a $(4r^2, 2r^2 - r, r^2 - r)$ -Hadamard difference set fixed by inversion in a finite group G of order $4r^2$ is a $(2r, r)$ -Latin square type partial difference set while its complement is a $(-2r, -r)$ -negative Latin square type partial difference set in G . On the other hand, given an odd positive integer n , an

$(n^2, (n^2 - 1)/2, (n^2 - 5)/4, (n^2 - 1)/4)$ -Paley type partial difference set in a finite group of order n^2 is both an $(n, (n + 1)/2)$ -Latin square type partial difference set and a $(-n, (-n + 1)/2)$ -negative Latin square type partial difference set. Paley type partial difference sets are the only partial difference sets which are simultaneously Latin square type and negative Latin square type. Constructions of these partial difference sets may be found in [4, 9, 12, 28, 33, 34]. For constructions of other Latin square type and negative Latin square type partial difference sets, see [11, 13, 18, 20–23, 27, 31, 32].

In [25] Ivanov proved that if a symmetric association scheme $\{\Gamma_1, \Gamma_2, \dots, \Gamma_d\}$ with $d > 2$ is amorphic, then the graphs $\Gamma_1, \Gamma_2, \dots, \Gamma_d$ are all strongly regular graphs of Latin square type or all strongly regular graphs of negative Latin square type. The converse of Ivanov's result was proved by Ito, Munemasa and Yamada [24]. More interestingly, van Dam proved the following two theorems in [39].

Theorem 1.1 ([39, Theorem 3]) *Let $\{\Gamma_1, \Gamma_2, \dots, \Gamma_d\}$ be a strongly regular decomposition of the complete graph on v vertices such that the graphs $\Gamma_1, \Gamma_2, \dots, \Gamma_d$ are all Latin square type or all negative Latin square type. Then the decomposition is an amorphic association scheme.*

Theorem 1.2 ([39, Corollary 1]) *Let Γ_1 and Γ_2 be two edge-disjoint strongly regular graphs on a vertex set X , both of Latin square type, or both of negative Latin square type. If the two graphs commute (i.e. their adjacency matrices commute), then their union $\Gamma_1 \cup \Gamma_2$ is also a strongly regular graph of Latin square type, or negative Latin square type, respectively.*

Note that Theorem 1.2 is equivalent to

Theorem 1.2' *Let Γ_1 and Γ_2 be two strongly regular graphs on a vertex set X , both of Latin square type, or both of negative Latin square type. If the edge set of Γ_1 is contained in that of Γ_2 and the two graphs commute, then their difference $\Gamma_2 \setminus \Gamma_1$ is also a strongly regular graph of Latin square type, or negative Latin square type, respectively.*

An interesting consequence of Theorem 1.1 and 1.2' is the following theorem.

Theorem 1.3 *Let G be an abelian group and $D_1 \subset D_2 \subset \dots \subset D_{d-1}$ be a chain of regular Latin square type partial difference sets, or a chain of regular negative Latin square type partial difference sets. Then $(G; \{0\}, D_1, D_2 \setminus D_1, D_3 \setminus D_2, \dots, D_{d-1} \setminus D_{d-2}, G \setminus D_{d-1})$ is a d -class abelian amorphic group scheme.*

The only known constructions of negative Latin square type abelian amorphic group schemes of 3 or more classes in non-elementary abelian groups are for some abelian 2-groups or 3-groups [14, 32]. In this paper we construct new negative Latin square type partial difference sets and abelian amorphic group schemes in non-elementary abelian p -groups for all primes p . Our method is to use what we call pseudo-quadratic bent functions as substitutes for quadratic forms, which is derived from a character theory-based idea.

Character sum is a powerful tool in the study of partial difference sets in abelian groups and was introduced into difference set community by Turyn [38]. A character on a finite abelian group G is a homomorphism from the group to the complex numbers of modulus 1. The principal character is the one whose values are 1 on all the elements of G , and any other character is called non-principal. One can naturally extend a character on G to a homomorphism of the group ring $\mathbb{Z}[G]$ as follows: if χ is a character on G , then for an element $A = \sum_{g \in G} a_g g$ in the group ring $\mathbb{Z}[G]$, let $\chi(A) = \sum_{g \in G} a_g \chi(g)$ so that if S is a subset of G , then $\chi(S) = \sum_{s \in S} \chi(s)$. By the Fourier inversion formula, one has

Theorem 1.4 *Let G be an abelian group of order n^2 and D a subset in $G \setminus \{0\}$ of size $r(n-1)$. Then D is a regular partial difference set having parameters (1) if and only if for every non-principal character χ on G , $\chi(D) = n-r$ or $-r$.*

2 Quadratic Latin subsets and quadratic amorphic partitions of finite fields

Given two additive abelian groups G and H with $|G|/|H|$ an integer, a function $f: G \rightarrow H$ will be called a *bent function* (or *perfect non-linear function*) if for each $a \neq 0$ in G , the number of elements x in G such that $f(x+a) - f(x) = b$ is $|G|/|H|$ for every b in H . The term bent function was introduced by Rothaus [35] for $|H| = 2$. Bent functions were studied in detail by Dillon in [15, 16] and generalized by Kumar, Scholtz and Welch in [26]. Our definition of bent functions is taken from [10] based upon their connection with splitting semi-regular relative difference sets (see [4] for details). By the Fourier inversion formula, one has

Lemma 2.1 *A function $f: G \rightarrow H$ from an abelian group G to an abelian group H with $|G|/|H|$ an integer is a bent function if and only if for each character χ of G and each non-principal character ϕ of H ,*

$$\left| \sum_{x \in G} \chi(x) \phi(f(x)) \right| = \sqrt{|G|}.$$

We will use certain kinds of bent functions to construct partial difference sets of both Latin square type and negative Latin square type and amorphic association schemes, particularly, those related to quadratic forms.

Quadratic forms have been used for constructing partial difference sets of both Latin square type and negative Latin square type (see [7, 29]) and amorphic association schemes [14, 18]. Let q be a power of a prime. We denote the field of q elements by $\mathbb{F}_q$. A quadratic form Q on a d -dimensional vector space $\mathbb{F}_q^d$ over $\mathbb{F}_q$ is a function $Q: \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ such that:

- (i) $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in \mathbb{F}_q$ and all $x \in \mathbb{F}_q^d$, and
- (ii) the function $B: \mathbb{F}_q^d \times \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ given by $B(x, y) = Q(x+y) - Q(x) - Q(y)$ is $\mathbb{F}_q$ -bilinear.

A quadratic form Q is said to be non-degenerate if $B(x, y) = 0$ for all $y \in \mathbb{F}_q^d$ implies $x = 0$. A simple fact about non-degenerate quadratic forms is that

Proposition 2.2 *A quadratic form $Q : \mathbb{F}_q^d \rightarrow \mathbb{F}_q$ is non-degenerate if and only if Q is a bent function.*

Proposition 2.2 is a direct consequence of Lemma 4.5 in [10]. We will call a non-degenerate quadratic form over $\mathbb{F}_q$ a quadratic bent function over $\mathbb{F}_q$.

In this paper, we are only interested in quadratic bent functions on an even dimensional vector space over $\mathbb{F}_q$. Every quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ is equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{2m-3}x_{2m-2} + Q'$ for a suitably chosen basis of $\mathbb{F}_q^{2m}$, where Q' is a quadratic bent function on a two dimensional subspace of $\mathbb{F}_q^{2m}$. If Q' is equivalent to $x_{2m-1}x_{2m}$, then Q is said to be *hyperbolic*. Otherwise, Q' is irreducible and Q is said to be *elliptic*. The following results concerning quadratic bent functions are well known, among which Proposition 2.3 can be proved (see [8]) using a method due to Minkowski [30], and the second part of both Propositions 2.4 and 2.5 can be easily derived from Proposition 2.3.

Proposition 2.3 *If $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ is a quadratic bent function over $\mathbb{F}_q$, then $|Q^{-1}(0)| - q^m = |Q^{-1}(\alpha)| = q^{2m-1} - q^{m-1}$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$ when Q is hyperbolic, or $|Q^{-1}(0)| + q^m = |Q^{-1}(\alpha)| = q^{2m-1} + q^{m-1}$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$ when Q is elliptic.*

Proposition 2.4 *If $Q_1 : \mathbb{F}_q^{2m_1} \rightarrow \mathbb{F}_q$ and $Q_2 : \mathbb{F}_q^{2m_2} \rightarrow \mathbb{F}_q$ are two quadratic bent functions over $\mathbb{F}_q$, then $Q_1 \oplus Q_2 : \mathbb{F}_q^{2(m_1+m_2)} \rightarrow \mathbb{F}_q$, with $Q_1 \oplus Q_2(x_1, x_2) = Q_1(x_1) + Q_2(x_2)$ for all $(x_1, x_2) \in \mathbb{F}_q^{2m_1} \times \mathbb{F}_q^{2m_2} = \mathbb{F}_q^{2(m_1+m_2)}$, is a quadratic bent function over $\mathbb{F}_q$. The direct sum $Q_1 \oplus Q_2$ is elliptic if and only if exactly one of Q_1 and Q_2 is elliptic.*

Proposition 2.5 *If $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ is a quadratic bent function over $\mathbb{F}_q$ and $\mathbb{F}_{q'}$ is a subfield of $\mathbb{F}_q$, then $\text{tr}_{q/q'} \circ Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_{q'}$ is a quadratic bent function over $\mathbb{F}_{q'}$, where $\text{tr}_{q/q'}$ is the relative trace map from $\mathbb{F}_q$ to $\mathbb{F}_{q'}$. The function $\text{tr}_{q/q'} \circ Q$ is elliptic if and only if Q is elliptic.*

Many partial difference sets of Latin square type, negative Latin square type and amorphic association schemes are constructed from quadratic bent functions. In all these constructions, the partial difference sets are always full pre-images under quadratic bent functions of subsets of $\mathbb{F}_q$. The type of difference set so obtained, Latin square type or negative Latin square type, depends only on the type of quadratic bent function, hyperbolic or elliptic, and does not depend on the subset in $\mathbb{F}_q$. Also, all these sets in $\mathbb{F}_q$ seem to be universal, meaning that their pre-images under all quadratic bent functions of even dimension are partial difference sets. This observation leads us to the following definition of quadratic Latin subsets and quadratic amorphic partitions of finite fields, as well as pseudo-quadratic bent functions given in next section.

Definition 2.6 Given a finite field $\mathbb{F}_q$, we denote by $\mathbb{F}_q^*$ the set of all non-zero elements of $\mathbb{F}_q$, which forms a cyclic group under multiplication. A subset A of $\mathbb{F}_q^*$ will be called a *quadratic Latin subset* if for every positive integer m and every quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$, the subset $Q^{-1}(A)$ is a $(q^m, |A|q^{m-1})$ -Latin square type partial difference set in $\mathbb{F}_q^{2m}$ when Q is hyperbolic, or a $(-q^m, -|A|q^{m-1})$ -negative Latin square type partial difference set in $\mathbb{F}_q^{2m}$ when Q is elliptic. A partition $\{A_1, A_2, \dots, A_k\}$ of $\mathbb{F}_q^*$ will be called a *quadratic amorphic partition* if all subsets $A_1, A_2, \dots, A_k$ are quadratic Latin subsets of $\mathbb{F}_q^*$.

By Theorem 1.1 and Propositions 2.3 and 2.5, we have

Proposition 2.7 Let $\mathbb{F}_{q'}$ be a subfield of $\mathbb{F}_q$ and A be a quadratic Latin subset of $\mathbb{F}_{q'}^*$. Then $\text{tr}_{q/q'}^{-1}(A)$ is a quadratic Latin subset of $\mathbb{F}_q^*$.

Proposition 2.8 A partition $\{A_1, A_2, \dots, A_k\}$ of $\mathbb{F}_q^*$ is a quadratic amorphic partition if and only if for every positive integer m and every quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$, $(\mathbb{F}_q^{2m}; \{0\}, Q^{-1}(0) \setminus \{0\}, Q^{-1}(A_1), Q^{-1}(A_2), \dots, Q^{-1}(A_k))$ is an amorphic group scheme.

The following are some examples of quadratic amorphic partitions of $\mathbb{F}_q$ which can be used with pseudo-quadratic bent functions in place of quadratic bent functions to obtain amorphic group schemes.

Example 2.9 ([7, 29]) For every prime power q , $\{\mathbb{F}_q^*\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$.

Example 2.10 ([7, 29]) If q is odd, we denote by S_q the set of all squares in $\mathbb{F}_q^*$ and N_q the set of all non-squares in $\mathbb{F}_q^*$. Then $\{S_q, N_q\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$ when q is odd.

Example 2.11 ([5]) Let $\mathbb{F}_{q'}$ be a subfield of $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q^*$. We define $H_1(\alpha) = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q'}(\alpha x) = 0 \text{ and } x \neq 0\}$ and $H_2(\alpha) = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q'}(\alpha x) \neq 0\}$. Then $\{H_1(\alpha), H_2(\alpha)\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$.

Example 2.12 ([14]) Let $\mathbb{F}_q = \mathbb{F}_{q_0} \supset \mathbb{F}_{q_1} \supset \dots \supset \mathbb{F}_{q_l}$ be a sequence of finite fields. Let $A_i = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_i}(x) \neq 0 \text{ and } \text{tr}_{q/q_{i+1}}(x) = 0\}$ for $i = 0, 1, 2, \dots, l-1$, and $A_l = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_l}(x) \neq 0\}$. Then $\{A_0, A_1, \dots, A_l\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$.

Example 2.13 ([14, 18]) The cyclotomic partition $\{C_0, C_1, \dots, C_q\}$ of $\mathbb{F}_{q^{2n}}^*$ is a quadratic amorphic partition, where $C_0, C_1, \dots, C_q$ are the $q+1$ distinct cosets of the subgroup $\{x \in \mathbb{F}_{q^{2n}}^* \mid N_{q^{2n}/q^2}(x) \in \mathbb{F}_q^*\}$ in $\mathbb{F}_{q^{2n}}^*$, where N_{q^{2n}/q^2} is the relative norm map from $\mathbb{F}_{q^{2n}}^*$ to $\mathbb{F}_{q^2}^*$, i.e. $N_{q^{2n}/q^2}(x) = xx^{q^2}x^{q^4} \dots x^{q^{2(n-1)}}$ for all $x \in \mathbb{F}_{q^{2n}}^*$.

Example 2.14 Let n be a positive integer such that $n = n_1 n_2 \cdots n_k$. Let $q_i = q^{n_i}$ for $i = 1, 2, \dots, k$. We assume that $(q_i + 1) \nmid (q_j + 1)$ when $i \neq j$. By Example 2.13, we get a quadratic amorphic partition from the cyclotomic partition $\{C_{i0}, C_{i1}, \dots, C_{iq_i}\}$ of $\mathbb{F}_{q^{2n}}^*$, where C_{i0} is a subgroup of index $q_i + 1$ in $\mathbb{F}_{q^{2n}}^*$, for each $i = 1, 2, \dots, k$. Let $C = \langle C_{10}, C_{20}, \dots, C_{k0} \rangle$ and $\{C_0, C_1, \dots, C_e\}$ be the set of all cosets of C in $\mathbb{F}_{q^{2n}}^*$. Then each coset C_s of C is a disjoint union of some cosets in $\{C_{i0}, C_{i1}, \dots, C_{iq_i}\}$ for each $i = 1, 2, \dots, k$. Hence we obtain a quadratic amorphic partition $\{D_1, D_2, \dots, D_t\}$ of $\mathbb{F}_{q^{2n}}^*$ which contains subsets from different cyclotomic partitions when $e > 0$. For instance, if q is odd and m and n are positive integers, then $\gcd(q + 1, q^{2^n} + 1) = 2$. Let C_{10} and C_{20} be the subgroups of index $q + 1$ and $q^{2^n} + 1$, respectively, in $\mathbb{F}_{q^{2^{m+n}}}^*$. Then $\langle C_{10}, C_{20} \rangle = S_{q^{2^{m+n}}}$ and $S_{q^{2^{m+n}}}$ is the union of $(q + 1)/2$ cosets of C_{10} and $N_{q^{2^{m+n}}}$ is the union of $(q^{2^n} + 1)/2$ cosets of C_{20} . Therefore there is a quadratic amorphic partition $\{D_1, D_2, \dots, D_{1+(q+q^{2^n})/2}\}$ of $\mathbb{F}_{q^{2^{m+n}}}^*$ that consists of $(q + 1)/2$ cosets of C_{10} and $(q^{2^n} + 1)/2$ cosets of C_{20} .

Example 2.15 Suppose q is odd. Let $\mathbb{F}_q = \mathbb{F}_{q_0} \supset \mathbb{F}_{q_1} \supset \cdots \supset \mathbb{F}_{q_l}$ be a sequence of finite fields. Let $A_i = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_i}(x) \neq 0 \text{ and } \text{tr}_{q/q_{i+1}}(x) = 0\}$ for $i = 0, 1, 2, \dots, l - 1$, $A_l = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_l}(x) \in S_{q_l}\}$ and $A_{l+1} = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_l}(x) \in N_{q_l}\}$. Then $\{A_0, A_1, \dots, A_l, A_{l+1}\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$.

Example 2.16 Let $\mathbb{F}_q = \mathbb{F}_{q_0} \supset \mathbb{F}_{q_1} \supset \cdots \supset \mathbb{F}_{q_l} \supset \mathbb{F}_{q_{l+1}}$ be a sequence of finite fields such that $q_l = q_{l+1}^{2^n}$. Let $\{D_1, D_2, \dots, D_t\}$ be the quadratic amorphic partition of $\mathbb{F}_{q_l}^*$ as described in Example 2.14. Define $A_i = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_i}(x) \neq 0 \text{ and } \text{tr}_{q/q_{i+1}}(x) = 0\}$ for $i = 0, 1, 2, \dots, l - 1$, $A_l = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_l}(x) \in D_1\}$ and $A_{l+1} = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_l}(x) \in D_2\}, \dots, A_{l+t-1} = \{x \in \mathbb{F}_q \mid \text{tr}_{q/q_l}(x) \in D_t\}$. Then $\{A_0, A_1, \dots, A_{l+t-1}\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$.

Remark 2.17 Among the examples of quadratic amorphic partitions given here, Examples 2.9, 2.10, and 2.13 are the basic ones and all others can be derived from these three using Theorems 1.1 and 1.2. Example 2.11 was first discovered by Brouwer in [5] and it can now be easily derived from Theorem 1.2', Proposition 2.5 and Examples 2.10. Example 2.12 is a direct consequence of Theorem 1.3, Proposition 2.5 and Example 2.9. Example 2.13 was first proved in [14] for $n = 1$ and generalized in [18] to all positive integers n . It is interesting to note that, as pointed out in [40], the cyclotomic partitions in Example 2.13 are precisely the ones that themselves are amorphic cyclotomic schemes, which was proved in [3]. If partial difference sets $D_1, D_2, \dots, D_t$ in Example 2.14 are of all Latin square type or all negative Latin square type, then by Theorem 1.1, it also gives rise to an amorphic group scheme in the additive group of the finite field which is comprised of different cyclotomic classes.

Remark 2.18 The union of any number of subsets in a quadratic amorphic partition of a finite field is a quadratic Latin subset of the field. Therefore one can obtain new Latin square type and negative Latin square type partial difference sets from

Example 2.15 and 2.16 by taking unions of those A_i 's and finding their full pre-images under quadratic bent functions of even dimension. Many of these new partial difference sets will have new parameters which are too tedious to list here.

3 Pseudo-quadratic bent functions

In this section we study what we call pseudo-quadratic bent functions.

Definition 3.1 Let G be an abelian group such that $|G|$ is a square and $\sqrt{|G|}/q$ is an integer. We call a function $P : G \rightarrow \mathbb{F}_q$ with $P(0) = 0$ a *pseudo-quadratic bent function* if there is a quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ for some positive integer m such that

- (i) for each non-principal character χ of G , there is a non-principal character χ' of $\mathbb{F}_q^{2m}$ such that $\chi(P^{-1}(\alpha))/\sqrt{|G|} = \chi'(Q^{-1}(\alpha))/q^m$ for all $\alpha \in \mathbb{F}_q$, and
- (ii) if Q is hyperbolic, then $|P^{-1}(0)| - \sqrt{|G|} = |P^{-1}(\alpha)| = (|G| - \sqrt{|G|})/q$ for every $\alpha \in \mathbb{F}_q \setminus \{0\}$; if Q is elliptic, then $|P^{-1}(0)| + \sqrt{|G|} = |P^{-1}(\alpha)| = (|G| + \sqrt{|G|})/q$ for every $\alpha \in \mathbb{F}_q \setminus \{0\}$.

If a function $P : G \rightarrow \mathbb{F}_q$ and a quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ satisfy Definition 3.1, by Lemma 2.1 and Proposition 2.2, P is a bent function and we say that the pseudo-quadratic bent function P is *modeled on* the quadratic bent function Q . Every quadratic bent function is a pseudo-quadratic bent function modeled on itself. We call P a *hyperbolic* pseudo-quadratic bent function if Q is hyperbolic, or an *elliptic* pseudo-quadratic bent function if Q is elliptic.

Propositions 2.4, 2.5 and 2.8 can be easily generalized from quadratic bent functions to pseudo-quadratic bent functions with some simple applications of characters of finite abelian groups.

Proposition 3.2 If $P_1 : G_1 \rightarrow \mathbb{F}_q$ and $P_2 : G_2 \rightarrow \mathbb{F}_q$ are two pseudo-quadratic bent functions modeled on quadratic bent functions $Q_1 : \mathbb{F}_q^{2m_1} \rightarrow \mathbb{F}_q$ and $Q_2 : \mathbb{F}_q^{2m_2} \rightarrow \mathbb{F}_q$, respectively, then $P_1 \oplus P_2 : G_1 \times G_2 \rightarrow \mathbb{F}_q$ is a pseudo-quadratic bent function modeled on $Q_1 \oplus Q_2 : \mathbb{F}_q^{2(m_1+m_2)} \rightarrow \mathbb{F}_q$. The direct sum $P_1 \oplus P_2$ is elliptic if and only if exactly one of P_1 and P_2 is elliptic.

Proposition 3.3 If $P : G \rightarrow \mathbb{F}_q$ is a pseudo-quadratic bent function modeled on quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ and $\mathbb{F}_{q'}$ is a subfield of $\mathbb{F}_q$, then $\text{tr}_{q/q'} \circ P : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_{q'}$ is a pseudo-quadratic bent function modeled on $\text{tr}_{q/q'} \circ Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_{q'}$. The function $\text{tr}_{q/q'} \circ P$ is elliptic if and only if P is elliptic.

Proposition 3.4 Let $P : G \rightarrow \mathbb{F}_q$ be a pseudo-quadratic bent function.

- (i) If a subset A in $\mathbb{F}_q^*$ is a quadratic Latin subset, then the subset $P^{-1}(A)$ in G is a $(\sqrt{|G|}, |A|\sqrt{|G|}/q)$ -Latin square type partial difference set when P is hyperbolic, or a $(-\sqrt{|G|}, -|A|\sqrt{|G|}/q)$ -negative Latin square type partial difference set when P is elliptic.

- (ii) If $\{A_1, A_2, \dots, A_k\}$ is a quadratic amorphic partition of $\mathbb{F}_q^*$, then $(G; \{0\}, P^{-1}(0) \setminus \{0\}, P^{-1}(A_1), P^{-1}(A_2), \dots, P^{-1}(A_k))$ is an amorphic group scheme.

Proposition 3.2 enables us to construct a large number of pseudo-quadratic bent functions from just a few examples and Proposition 3.4 allows us to produce new partial difference sets and amorphic association schemes in new abelian groups by applying pseudo-quadratic bent functions to Examples 2.9–2.16.

In order to facilitate a better understanding of pseudo-quadratic bent functions, let us take a closer look at such functions $P : G \rightarrow \mathbb{F}_q$ when q is small. Specifically, we want to determine when a bent function $P : G \rightarrow \mathbb{F}_q$ is a pseudo-quadratic bent functions for $q = 2, 3, 4$. This requires the following definition of regularity of a bent function, which is a simple modification of some existing definitions in the literature (see [22, 36] for instance and references therein).

Definition 3.5 A bent function $f : G \rightarrow H$ between two abelian groups G and H is said to be *strongly regular* if $f(0) = 0$ and there is a constant $\varepsilon = \pm 1$ and a function $\hat{f} : \hat{G} \rightarrow H$, where $\hat{G}$ is the group of characters of G , such that $\hat{f}(\hat{0}) = 0$, where $\hat{0}$ is the principal character of G , and for every character $\chi \in \hat{G}$ and every non-principal character ϕ of H ,

$$\sum_{x \in G} \chi(x) \phi(f(x)) = \varepsilon \sqrt{|G|} \phi(\hat{f}(\chi)).$$

We will call f *hyperbolic* if $\varepsilon = 1$ or *elliptic* if $\varepsilon = -1$.

The following proposition is an immediate consequence of the definition.

Proposition 3.6 If $f_1 : G_1 \rightarrow H$ and $f_2 : G_2 \rightarrow H$ are strongly regular bent functions, then $f_1 \oplus f_2 : G_1 \times G_2 \rightarrow H$ is also a strongly regular bent function.

Simple calculation shows that $\hat{f} : \hat{G} \rightarrow H$ is also a strongly regular bent function and $\hat{f}(x) = f(-x)$. When G is an elementary abelian p -group and $H = \mathbb{F}_p$, the regular p -ary bent functions $f : G \rightarrow H$ (see [22]) with $f(0) = 0$ are precisely hyperbolic strongly regular bent functions, and weakly regular p -ary bent functions $f : G \rightarrow H$ with $\mu = -1$ and $f(0) = 0$ are precisely elliptic strongly regular bent functions. These functions and their connection with strongly regular graphs are studied by Tan, Pott and Feng in [36]. The following theorem gives a generalization of Theorem 1 in [36] and puts most of constructions in [32] in the context of strongly regular bent functions.

Theorem 3.7 A function $f : G \rightarrow H$ between two abelian groups G and H with $f(0) = 0$ is a strongly regular bent function if and only if either $f^{-1}(y)$ is a $(\sqrt{|G|}, \sqrt{|G|}/|H|)$ -Latin square type partial difference set for every $y \in H \setminus \{0\}$ and $f^{-1}(0) \setminus \{0\}$ is a $(\sqrt{|G|}, 1 + \sqrt{|G|}/|H|)$ -Latin square type partial difference set, or $f^{-1}(y)$ is a $(-\sqrt{|G|}, -\sqrt{|G|}/|H|)$ -negative Latin square type partial difference set for every $y \in H \setminus \{0\}$ and $f^{-1}(0) \setminus \{0\}$ is a $(-\sqrt{|G|}, 1 - \sqrt{|G|}/|H|)$ -negative Latin square type partial difference set.

Proof From the definition of strongly regular bent functions, a function $f : G \rightarrow H$ is a strongly regular bent if and only if

$$\sum_{x \in G} \chi(x) \phi(f(x)) = \varepsilon \sqrt{|G|} \phi(\hat{f}(\chi))$$

for every character $\chi \in \widehat{G}$ and every non-principal character ϕ of H , which is equivalent to

$$\sum_{y \in H} \chi(f^{-1}(y)) \phi(y) = \varepsilon \sqrt{|G|} \phi(\hat{f}(\chi))$$

for every character $\chi \in \widehat{G}$ and every non-principal character ϕ of H . Therefore, for every fixed $\chi \in \widehat{G}$,

$$\sum_{y \in H} \chi(f^{-1}(y)) y = \varepsilon \sqrt{|G|} \hat{f}(\chi) + (\delta_{\chi, \hat{0}} |G| - \varepsilon \sqrt{|G|}) H / |H|,$$

where $\delta_{\chi, \hat{0}}$ is the Kronecker δ -symbol, in the group ring $\mathbb{Z}[H]$. We can then find all $\chi(f^{-1}(y))$ for all $\chi \in \widehat{G}$ and $y \in H$, which shows that $f^{-1}(y)$ is a $(\sqrt{|G|}, \sqrt{|G|}/|H|)$ -Latin square type partial difference set for every $y \in H \setminus \{0\}$ and $f^{-1}(0) \setminus \{0\}$ is a $(\sqrt{|G|}, 1 + \sqrt{|G|}/|H|)$ -Latin square type partial difference set when $\varepsilon = 1$, or $f^{-1}(y)$ is a $(-\sqrt{|G|}, -\sqrt{|G|}/|H|)$ -negative Latin square type partial difference set for every $x \in H \setminus \{0\}$ and $f^{-1}(0) \setminus \{0\}$ is a $(-\sqrt{|G|}, 1 - \sqrt{|G|}/|H|)$ -negative Latin square type partial difference set when $\varepsilon = -1$.

Conversely, if $f^{-1}(y)$ is a $(\sqrt{|G|}, \sqrt{|G|}/|H|)$ -Latin square type partial difference set for every $y \in H \setminus \{0\}$ and $f^{-1}(0) \setminus \{0\}$ is a $(\sqrt{|G|}, 1 + \sqrt{|G|}/|H|)$ -Latin square type partial difference set, or $f^{-1}(y)$ is a $(-\sqrt{|G|}, -\sqrt{|G|}/|H|)$ -negative Latin square type partial difference set for every $y \in H \setminus \{0\}$ and $f^{-1}(0) \setminus \{0\}$ is a $(-\sqrt{|G|}, 1 - \sqrt{|G|}/|H|)$ -negative Latin square type partial difference set, then for each $\chi \neq \hat{0}$ in $\widehat{G}$, by Lemma 2.1 of [32], the character sum $\chi(f^{-1}(y)) = -\varepsilon \sqrt{|G|}/|H|$ for all $y \in H$ with the exception of exactly one $y \in H$ with $\chi(f^{-1}(y)) = \varepsilon(\sqrt{|G|} - \sqrt{|G|}/|H|)$. Define $\hat{f}(\chi)$ to be the exceptional y for all $\chi \neq \hat{0}$ and $\hat{f}(0) = 0$. One can then easily check that f is a strongly regular bent function. $\square$

Theorem 3.7 clearly implies the following corollary.

Corollary 3.8 *Let $f : G \rightarrow H$ be a strongly regular bent function and H' be an abelian group such that $|H|/|H'|$ is an integer. Then for any function $g : H \rightarrow H'$ satisfying $g(0) = 0$ and $|g^{-1}(y)| = |H|/|H'|$ for all $y \in H'$, the function $g \circ f : G \rightarrow H'$ is a strongly regular bent function.*

Theorem 3.7 shows that strongly regular bent functions are equivalent to those amorphic group schemes studied in [32] and Proposition 3.6 is an equivalent form of Theorem 2.1–2.3 in [32]. Results in Chen, Ray-Chaudhuri and Xiang [11], Hou, Leung and Xiang [23] and Leung and Ma [27] can now also be rephrased in terms of strongly regular bent functions.

Proposition 3.9 *Let p be a prime and n be a positive integer.*

- (i) *For any abelian p -group G and any abelian group H of order p^n , there are hyperbolic strongly regular bent functions $f : G^{2n} \rightarrow H$.*
- (ii) *There are hyperbolic strongly regular bent functions $f : \mathbb{Z}_{p^2}^n \rightarrow H$ for any abelian groups H of order $p^{s(p,n)}$, where*

$$s(p, n) = \max_{d|n, d>0} d \left(\left\lfloor \frac{n-2d}{pd} \right\rfloor + 1 \right).$$

- (iii) *There are both hyperbolic and elliptic strongly regular bent functions $f : \mathbb{Z}_4^2 \rightarrow H$ for any abelian groups H of order 4.*

Remark 3.10 In Proposition 3.9, (i) is a consequence of results in [27] and [32] while (ii) is contained in [23] which improves a result in [11]. Elliptic strongly regular bent functions in (iii) are obtained in [13] and hyperbolic strongly regular bent functions in (iii) can be constructed from cyclic subgroups of order 4 in $\mathbb{Z}_4^2$, i.e. the partial congruence partition construction. It is very likely that the partial difference sets constructed by Hou [20, 21] can also be obtained from Proposition 3.6 and 3.9.

By Examples 2.9, 2.10 and 2.13, Theorem 3.7 shows that quadratic bent functions $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ are strongly regular bent functions when $q \leq 4$, i.e. every one element subset of $\mathbb{F}_q^*$ is a quadratic Latin set when $q \leq 4$. Proposition 3.4 implies the following characterization of pseudo-quadratic bent function $P : G \rightarrow \mathbb{F}_q$ for $q \leq 4$.

Theorem 3.11 *When $q \leq 4$, a function $P : G \rightarrow \mathbb{F}_q$ is a pseudo-quadratic bent function if and only if P is a strongly regular bent function.*

Proof The fact that pseudo-quadratic bent functions are strongly regular when $q \leq 4$ follows rather easily from Example 2.9, 2.10 and 2.13, Proposition 3.4 and Theorem 3.7. On the other hand, if $P : G \rightarrow \mathbb{F}_q$ is a strongly regular bent function for some $q \leq 4$, then it clearly satisfies all conditions in the definition of pseudo-quadratic bent functions except (i). In order to show that P also satisfies (i), one observes that for every non-principal character χ of G ,

$$\chi(P^{-1}(y))/\sqrt{|G|} = \varepsilon(-1/q) \text{ or } \varepsilon(1-1/q)$$

and it is independent of $|G|$. Therefore P is modeled on every quadratic bent function $Q : \mathbb{F}_q^{2m} \rightarrow \mathbb{F}_q$ of the same type, i.e. hyperbolic or elliptic, for any integer $m > 1$. Hence P is pseudo-quadratic. $\square$

Using constructions of Dillon [17], Chen [9] and a product construction of Turyn [37], we have the following proposition.

Proposition 3.12 *Let $G_1 = \mathbb{Z}_4^b \times H_1^2$ for some abelian 2-group H_1 and $G_2 = \mathbb{Z}_2^2 \times H_2^2 \times H_3^4$ for some elementary abelian 3-group H_2 and some product of elementary abelian groups H_3 . There are both hyperbolic and elliptic pseudo-quadratic bent functions $P : G \rightarrow \mathbb{F}_2$ for $G = G_1, G_2$ or $G_1 \times G_2$.*

Proposition 3.9 implies the following proposition.

Proposition 3.13 *Let $G_1 = \mathbb{Z}_9^b$ for some integer $b \geq 2$ and $G_2 = H^2$ for some abelian 3-group H . There are hyperbolic pseudo-quadratic bent functions $P : G \rightarrow \mathbb{F}_3$ and elliptic pseudo-quadratic bent functions $P : G \times \mathbb{Z}_3^2 \rightarrow \mathbb{F}_3$ for $G = G_1, G_2$ or $G_1 \times G_2$.*

By (i) in Proposition 3.9, there is a hyperbolic strongly regular bent function $P' : \mathbb{F}_8^2 \rightarrow \mathbb{F}_8$. By Corollary 3.8 and Theorem 3.11, there is a hyperbolic pseudo-quadratic bent function $P : \mathbb{Z}_2^6 \rightarrow \mathbb{F}_4$. Hence we get the following proposition.

Proposition 3.14 *Let $G_1 = H_1^4$, where H_1 is a product of cyclic 2-groups $\mathbb{Z}_{2^r}$ with $r \geq 1$, $G_2 = \mathbb{Z}_4^s$, where $s = 2$ or $s \geq 4$, $G_3 = \mathbb{Z}_2^{2t}$, where $t \geq 2$. There are hyperbolic pseudo-quadratic bent functions $P : G \rightarrow \mathbb{F}_4$ and elliptic pseudo-quadratic bent functions $P : G \times \mathbb{Z}_2^4 \rightarrow \mathbb{F}_4$ and $P : G \times \mathbb{Z}_4^2 \rightarrow \mathbb{F}_4$ when G is a product of some of G_1, G_2 , and G_3 .*

When $q > 4$, quadratic bent functions and pseudo-quadratic bent functions are no longer strongly regular. There are no known pseudo-quadratic bent functions $P : G \rightarrow \mathbb{F}_q$ other than quadratic bent functions for $q > 4$. In the remainder of this section, we present a hyperbolic pseudo-quadratic bent function $P : \mathbb{Z}_{p^2}^{2n} \rightarrow \mathbb{F}_q$, where $q = p^n$, for every prime p and every positive integer n .

Let $V = \mathbb{F}_q \times \mathbb{F}_q$ be a two dimensional vector space over $\mathbb{F}_q$. Let $Q : V \rightarrow \mathbb{F}_q$ be the hyperbolic quadratic bent function $Q(x, y) = xy$. For each $\alpha \in \mathbb{F}_q$, let $A_\alpha = Q^{-1}(\alpha) \subseteq V$. Let H_0 be an 1-dimensional $\mathbb{F}_q$ -subspace contained in A_0 . Our pseudo-quadratic bent function P will be modeled on Q .

Let $W = \mathbb{Z}_{p^2}^{2n}$ and $\pi : W \rightarrow V$ be a surjective homomorphism. Let $H_0, H_1, \dots, H_q$ be the $q + 1$ 1-dimensional subspaces of V with H_0 as specified above. Let $G_0 = \pi^{-1}(H_0), G_1 = \pi^{-1}(H_1), \dots, G_q = \pi^{-1}(H_q)$. Then $G_0, G_1, \dots, G_q$ satisfy $G_i \cong \mathbb{Z}_p^n \times \mathbb{Z}_{p^2}^n$ for all $i = 0, 1, \dots, q$ and

$$\bigcup_{i=0}^q G_i = W \quad \text{and} \quad G_i \cap G_j = E(W) \quad \text{for all } i \neq j,$$

where $E(W)$ denotes the maximum elementary abelian subgroup of W . Clearly $E(W) = E(G_i)$ for all $i = 0, 1, \dots, q$.

For each $i \in \{0, 1, \dots, q\}$, let $\pi_i : G_i \rightarrow V$ be a surjective homomorphism such that $\pi_i(E(G_i)) = H_0$. Since $H_0 \subseteq A_0$, $\pi_i^{-1}(A_\alpha) \cap E(W) = \pi_i^{-1}(A_\alpha) \cap E(G_i) = \emptyset$, and hence $\pi_i^{-1}(A_\alpha) \cap \pi_j^{-1}(A_\beta) = \emptyset$ for all $i \neq j$ and all $\alpha, \beta \in \mathbb{F}_q$ with $\alpha\beta \neq 0$. Now let

$$B_\alpha = \bigcup_{i=0}^q \pi_i^{-1}(A_\alpha)$$

for all $0 \neq \alpha \in \mathbb{F}_q$ and

$$B_0 = W \setminus \left(\bigcup_{\alpha \in \mathbb{F}_q \setminus \{0\}} B_\alpha \right).$$

We will also denote $E(W)$ by K_0 . Note that $H_0 \subseteq A_0$ while $K_0 \subseteq B_0$.

We now show that the character sums of B_α have striking resemblance to that of A_α for all $\alpha \in \mathbb{F}_q$.

Lemma 3.15 *The sizes $|A_\alpha| = q - 1$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$, and $|A_0| = 2q - 1$. If χ is a non-principal character of V which is principal on H_0 , then $\chi(A_\alpha) = -1$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$ and $\chi(A_0) = q - 1$.*

The sizes $|B_\alpha| = q^3 - q$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$, and $|B_0| = q^3 + q^2 - q$. If χ is a non-principal character of W , then there is a non-principal character χ' of V such that $\chi(B_\alpha) = q\chi'(A_\alpha)$ for all $\alpha \in \mathbb{F}_q$. In particular, if the non-principal character χ of W is principal on K_0 , then $\chi(B_\alpha) = -q$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$ and $\chi(B_0) = q(q - 1)$.

Proof Statements concerning A_α , $\alpha \in \mathbb{F}_q$, are easy to verify and we leave them to the reader. The sizes of B_α , $\alpha \in \mathbb{F}_q$, are also easy to check. We now examine the character values of B_α , $\alpha \in \mathbb{F}_q$, for non-principal characters of W .

Let χ be a non-principal character of W . When χ is non-principal on $K_0 = E(W)$, since the kernels $\text{Ker}(\pi_0), \text{Ker}(\pi_1), \dots, \text{Ker}(\pi_q)$ form a spread of K_0 , χ must be principal on exactly one, say $\text{Ker}(\pi_i)$ for some $0 \leq i \leq q$, of those kernels and non-principal on the rest. This implies that $\chi(\pi_j^{-1}(A_\alpha)) = 0$ for all $j = 0, 1, \dots, i - 1, i + 1, \dots, q$ and all $\alpha \in \mathbb{F}_q \setminus \{0\}$, and there is a non-principal character χ' on V such that $\chi|_{G_i} = \chi' \circ \pi_i$. Therefore $\chi(B_\alpha) = q\chi'(A_\alpha)$ for all $\alpha \in \mathbb{F}_q \setminus \{0\}$ and

$$\chi(B_0) = - \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \chi(B_\alpha) = - \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} q\chi'(A_\alpha) = -q \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \chi'(A_\alpha) = q\chi'(A_0).$$

When χ is principal on $K_0 = E(W)$, then χ is principal on exactly one, say G_i for some $0 \leq i \leq q$, of those pre-images and non-principal on the rest. Since χ is principal on $\text{Ker}(\pi_j)$ for all $j = 0, 1, \dots, q$, there are characters χ'_j on V such that $\chi|_{G_j} = \chi'_j \circ \pi_j$ for all $j = 0, 1, \dots, q$, and χ'_i is principal and χ'_j are non-principal for all $j = 0, 1, \dots, i - 1, i + 1, \dots, q$. The fact that $\pi_j(K_0) = H_0$ for all $j = 0, 1, \dots, q$ and χ is principal on K_0 implies that χ'_j is principal on H_0 for all $j = 0, 1, \dots, q$. From the character values of A_α , we get

$$\begin{aligned} \chi(B_\alpha) &= \sum_{j=0}^q q\chi'_j(A_\alpha) = q \left(\sum_{j=0}^{i-1} \chi'_j(A_\alpha) + \chi'_i(A_\alpha) + \sum_{j=i+1}^q \chi'_j(A_\alpha) \right) \\ &= q(-q + q - 1) = -q \end{aligned}$$

for all $\alpha \in \mathbb{F}_q \setminus \{0\}$ and

$$\chi(B_0) = - \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \chi(B_\alpha) = q(q - 1).$$

□

We define $P : \mathbb{Z}_{p^2}^{2n} \rightarrow \mathbb{F}_q$ with $P^{-1}(\alpha) = B_\alpha$ for all $\alpha \in \mathbb{F}_q$. Lemma 3.15 implies that

Theorem 3.16 *The function P is a hyperbolic pseudo-quadratic bent function modeled on Q .*

By Proposition 3.2 and Theorem 3.16, we get

Theorem 3.17 *Let p be a prime, H be an abelian p -group of exponent of at most p^2 and n be a positive integer. Let $q = p^n$ and $G = H^{2n}$. There exist hyperbolic pseudo-quadratic bent functions $P : G \rightarrow \mathbb{F}_q$ and elliptic pseudo-quadratic bent functions $P : G \times \mathbb{Z}_p^{2n} \rightarrow \mathbb{F}_q$.*

Remark 3.18 We need the factor $\mathbb{Z}_p^{2n}$ for elliptic pseudo-quadratic bent functions because we do not know the existence of such functions $P : \mathbb{Z}_{p^2}^{2n} \rightarrow \mathbb{F}_q$ except for $q = 2$ or 4 . We must rely on elliptic quadratic bent functions and Proposition 3.2 to obtain elliptic pseudo-quadratic bent functions.

Remark 3.18 raises an interesting question:

Question 3.19 Are there any elliptic pseudo-quadratic bent functions $P : \mathbb{Z}_{p^2}^{2n} \rightarrow \mathbb{F}_q$ for $q \neq 2$ or 4 ?

By Proposition 3.4 and Examples 2.9–2.16, we obtain many new partial difference sets and amorphic group schemes in G .

We can see from the discussion of pseudo-quadratic bent functions $P : G \rightarrow \mathbb{F}_q$ for $q \leq 4$, the constructions of this paper are a generalization of those in [32]. In that paper, partial difference sets were identified in certain p -groups with exponent p^r , $r \geq 1$, and used in much the same way that we use pseudo-quadratic bent function or strongly regular bent function pre-images in this paper. These results correspond to strongly regular bent functions in p -groups of arbitrary exponent. The similarities between the two constructions suggest another final question:

Question 3.20 Are there any pseudo-quadratic bent functions $P : \mathbb{Z}_{p^r}^{2n} \rightarrow \mathbb{F}_q$, with $r > 2$ and $q > 4$?

Acknowledgements The second author is supported by NSA grant H98230-10-1-0216.

References

1. Bailey, R.A.: Association Schemes—Designed Experiments, Algebra and Combinatorics. Cambridge Studies in Advanced Mathematics, vol. 84. Cambridge University Press, Cambridge (2004)
2. Bannai, E., Ito, T.: Algebraic Combinatorics I—Association Schemes. Benjamin/Cummings, Menlo Park (1984)
3. Baumert, L.D., Mills, W.H., Ward, R.L.: Uniform cyclotomy. J. Number Theory **14**, 67–82 (1982)

4. Beth, T., Jungnickel, D., Lenz, H.: Design Theory, vol. 1, 2nd edn. Cambridge University Press, Cambridge (1999)
5. Brouwer, A.E.: Some new two-weight codes and strongly regular graphs. *Discrete Appl. Math.* **10**, 111–114 (1985)
6. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs. Springer, New York (1989)
7. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. *Bull. Lond. Math. Soc.* **18**, 97–122 (1986)
8. Casselman, W.: <http://www.math.ubc.ca/~cass/siegel/FiniteFields.pdf>
9. Chen, Y.Q.: On the existence of abelian Hadamard difference sets and a new family of difference sets. *Finite Fields Appl.* **3**, 234–256 (1997)
10. Chen, Y.Q.: Divisible designs and semi-regular relative difference sets from additive Hadamard cocycles. *J. Comb. Theory, Ser. A* **118**, 2185–2206 (2011)
11. Chen, Y.Q., Ray-Chaudhuri, D.K., Xiang, Q.: Constructions of partial difference sets and relative difference sets using Galois rings II. *J. Comb. Theory, Ser. A* **76**, 179–196 (1996)
12. Davis, J.A.: Partial difference sets in p -groups. *Arch. Math.* **63**, 103–110 (1994)
13. Davis, J.A., Xiang, Q.: Negative Latin square type partial difference sets in non-elementary abelian 2-groups. *J. Lond. Math. Soc.* **70**, 125–141 (2004)
14. Davis, J.A., Xiang, Q.: Amorphic association schemes with negative Latin square-type graphs. *Finite Fields Appl.* **12**, 595–612 (2006)
15. Dillon, J.F.: Elementary Hadamard difference sets. PhD thesis, University of Maryland (1974)
16. Dillon, J.F.: Elementary Hadamard difference sets. In: Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Florida Atlantic Univ., Boca Raton, Fla., 1975. *Congressus Numerantium*, vol. XIV, pp. 237–249. Utilitas Math., Winnipeg (1975)
17. Dillon, J.F.: Difference sets in 2-groups. In: Finite Geometries and Combinatorial Designs, Lincoln, NE, 1987. *Contemp. Math.*, vol. 111, pp. 65–72. Amer. Math. Soc., Providence (1990)
18. Feng, T., Wen, B., Xiang, Q., Yin, J.: Partial difference sets from p -ary weakly regular bent functions and quadratic forms. [arXiv:1002.2797v1](https://arxiv.org/abs/1002.2797v1)
19. Godsil, C.D.: Algebraic Combinatorics. Chapman & Hall, New York (1993)
20. Hou, X.-D.: New partial difference sets in p -groups. *J. Comb. Des.* **10**, 394–402 (2002)
21. Hou, X.-D.: Rings and constructions of partial difference sets. *Discrete Math.* **270**, 149–176 (2003)
22. Hou, X.-D.: p -Ary and q -ary versions of certain results about bent functions and resilient functions. *Finite Fields Appl.* **10**, 566–582 (2004)
23. Hou, X.-D., Leung, K.H., Xiang, Q.: New partial difference sets in $\mathbb{Z}_{p^2}^t$ and a related problem about Galois ring. *Finite Fields Appl.* **7**, 165–188 (2001)
24. Ito, T., Munemasa, A., Yamada, M.: Amorphous association schemes over the Galois rings of characteristic 4. *Eur. J. Comb.* **12**, 513–526 (1991)
25. Ivanov, A.V.: Amorphous cell rings. II. In: Investigations in the Algebraic Theory of Combinatorial Objects, pp. 39–49. Vsesoyuz. Nauchno-Issled. Inst. Sistem. Issled., Moscow (1985) (Russian)
26. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. *J. Comb. Theory, Ser. A* **40**, 90–107 (1985)
27. Leung, K.H., Ma, S.L.: Constructions of partial difference sets and relative difference sets on p -groups. *Bull. Lond. Math. Soc.* **22**, 533–539 (1990)
28. Leung, K.H., Ma, S.L.: Partial difference sets with Paley parameters. *Bull. Lond. Math. Soc.* **27**, 553–564 (1995)
29. Ma, S.L.: A Survey of partial difference sets. *Des. Codes Cryptogr.* **4**, 221–261 (1994)
30. Minkowski, H.: Grundlagen für eine Theorie quadratischen Formen mit ganzzahligen Koeffizienten. In: *Gesammelte Abhandlungen*. Chelsea Book Series. American Mathematical Society, Providence (1967)
31. Polhill, J.: Generalizations of partial difference sets from cyclotomy to non-elementary abelian p -groups. *Electron. J. Comb.* **15**(1), 125 (2008)
32. Polhill, J.: New negative Latin square type partial difference sets in non-elementary abelian 2-groups and 3-groups. *Des. Codes Cryptogr.* **46**, 365–377 (2008)
33. Polhill, J.: Paley type partial difference sets in non p -groups. *Des. Codes Cryptogr.* **52**, 163–169 (2009)
34. Polhill, J.: Paley type partial difference sets in groups of order n^4 and $9n^4$ for any odd $n > 1$. *J. Comb. Theory, Ser. A* **117**, 1027–1036 (2010)
35. Rothaus, O.S.: On “bent” functions. *J. Comb. Theory, Ser. A* **2**, 300–305 (1976)

36. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary bent functions. *J. Comb. Theory, Ser. A* **117**, 668–682 (2010)
37. Turyn, R.J.: A special class of Williamson matrices and difference sets. *J. Comb. Theory, Ser. A* **12**, 111–115 (1984)
38. Turyn, R.J.: Character sums and difference sets. *Pac. J. Math.* **15**, 319–346 (1965)
39. van Dam, E.R.: Strongly regular decompositions of the complete graph. *J. Algebr. Comb.* **17**, 181–201 (2003)
40. van Dam, E.R., Muzychuk, M.: Some implications on amorphic association schemes. *J. Comb. Theory, Ser. A* **117**, 111–127 (2010)