



Queensland University of Technology
Brisbane Australia

This is the author's version of a work that was submitted/accepted for publication in the following source:

Hall, Joanne L., Rao, Asha, & Donovan, Diane (2012) Planar difference functions. In *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, IEEE Information Theory Society, Massachusetts Institute of Technology, Boston, MA, 1082 -1086.

This file was downloaded from: <http://eprints.qut.edu.au/58332/>

© Copyright 2012 IEEE

This work has been submitted to the IEEE for possible publication. Copyright may be transferred without notice, after which this version may no longer be accessible

Notice: *Changes introduced as a result of publishing processes such as copy-editing and formatting may not be reflected in this document. For a definitive version of this work, please refer to the published source:*

<http://dx.doi.org/10.1109/ISIT.2012.6283019>

Planar Difference Functions

Joanne L. Hall*, Asha Rao†, and Diane Donovan‡,

*Department of Algebra, Charles University in Prague
186 75 Praha 8, Sokolovska 83, Czech Republic

†* School of Mathematical and Geospatial Sciences, RMIT University
GPO Box 2476 Melbourne 3001, Australia

‡School of Mathematics and Physics, University of Queensland
St Lucia, Brisbane 4072, Australia

*Email: hall@karlin.mff.cuni.cz

†Email: asha@rmit.edu.au

‡Email: dmd@maths.uq.edu.au

Abstract—In 1980 Alltop produced a family of cubic phase sequences that nearly meet the Welch bound for maximum non-peak correlation magnitude. This family of sequences were shown by Wooters and Fields to be useful for quantum state tomography. Alltop’s construction used a function that is not planar, but whose difference function is planar. In this paper we show that Alltop type functions cannot exist in fields of characteristic 3 and that for a known class of planar functions, x^3 is the only Alltop type function.

I. INTRODUCTION

Planar functions belong to the larger class of highly nonlinear functions which are of use in classical cryptographic systems, coding theory as well as being of theoretical interest [4].

Let \mathbb{F}_{p^r} be a field of characteristic p . A function $f : \mathbb{F}_{p^r} \rightarrow \mathbb{F}_{p^r}$ is called a *planar function* if for every $a \in \mathbb{F}_{p^r}^*$ the function $\Delta_{f_a} : x \mapsto f(a+x) - f(x)$ is a bijection.

An equivalent definition of a planar function involves the ability to construct an affine plane [6, §5], which is where the name planar originates. It is known that planar functions do not exist on fields of characteristic 2 [6, §5].

Two orthonormal bases B_1 and B_2 of \mathbb{C}^d are *unbiased* if $|\langle \vec{x} | \vec{y} \rangle| = \frac{1}{\sqrt{d}}$ for all $\vec{x} \in B_1$ and $\vec{y} \in B_2$. A set of bases for \mathbb{C}^d which are pairwise unbiased is a set of *mutually unbiased bases* (MUBs). This idea is credited to Schwinger [14] who realised that a quantum system prepared in a basis state from B' reveals no information when measured with respect to the basis B . Mutually unbiased bases (MUBs) are an important tool in

quantum information theory and have applications in quantum cryptography [2], [13] and quantum state tomography [16].

We highlight two different constructions of mutually unbiased bases for odd prime power integers, one which uses a polynomial of degree 3 but only works for finite fields of characteristic $p \geq 5$ [9, Theorem 1]. This construction is a generalisation of low correlation complex sequences first constructed by Alltop [1] for spread spectrum radar and communication applications.

The other construction uses a polynomial of degree 2, which is a planar function, to construct the vectors in a complete set of MUBs (see Thm 1) [12], [9]. In contrast, the Alltop construction of complete sets of MUBs (Thm 2 [1], [9]) uses a function, $f(x) = x^3$ which is not planar, but for which the difference function $\Delta_{f_a}(x)$ is planar. We aim to discover if x^3 is the only polynomial function with this property.

Let $\omega_p := e^{\frac{2i\pi}{p}}$.

Theorem 1 (Planar function construction). [12, Thm 4.1] *Let \mathbb{F}_q be a field of odd characteristic p . Let $\Pi(x)$ be a planar function on \mathbb{F}_q . Let $V_a := \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors*

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left(\omega_p^{\text{tr}(a\Pi(x)+bx)} \right)_{x \in \mathbb{F}_q} \quad (1)$$

with $a, b \in \mathbb{F}_q$. The standard basis E along with the sets V_a , $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in \mathbb{C}^q .

The property that is being exploited in the planar function construction is that [4, Theorem

16]

$$\left| \sum_{x \in \mathbb{F}_q} \omega_p^{\text{tr}(\Pi(x))} \right| = \sqrt{q}. \quad (2)$$

Theorem 2 (Alltop Construction). [9, Thm 1] Let \mathbb{F}_q be a finite field of odd characteristic $p \geq 5$ and let $V_a := \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors

$$\vec{v}_{ab} := \frac{1}{\sqrt{q}} \left(\omega_p^{\text{tr}((x+a)^3 + b(x+a))} \right)_{x \in \mathbb{F}_q} \quad (3)$$

with $a, b \in \mathbb{F}_q$. The standard basis E along with the sets V_a , $a \in \mathbb{F}_q$, form a complete set of $q + 1$ MUBs in \mathbb{C}^q .

Although on the surface the Alltop construction does not use a planar function, when inspecting the inner product of the vectors,

$$\langle \vec{v}_{ab} | \vec{v}_{cd} \rangle = \frac{1}{q} \left| \sum_{x \in \mathbb{F}_q} \omega_p^{\text{tr}[3(a-c)x^2 + (3a^2 - 3c^2 + b-d)x + (a^3 - c^3 + ba - dc)]} \right| \quad (4)$$

we notice a polynomial of degree 2. Now $\Pi(x) = x^2$ is a planar function, and equation (2) ensures that a set of MUBs has been constructed. Thus if we take $f(x) = (x + b)^3$ then $\Delta_{fa}(x)$ is a planar function. The question that arises is whether $f(x) = (x + b)^3$ is the only function of this type:

Question 3. Is $f(x) = x^3$ the only polynomial function on a Galois field such that $\Delta_{fa}(x)$ is a planar function?

Two sets of MUBs, $\mathcal{B} = \{B_0, B_1, \dots, B_d\}$ and $\mathcal{C} = \{C_0, C_1, \dots, C_d\}$, written as matrices, are equivalent [3, App A] if either \mathcal{B} or \mathcal{B}^* is equal to $\{UC_0D_0P_0, UC_1D_1P_1, \dots, UC_dD_dP_d\}$ for some unitary matrix, U , unitary diagonal matrices, D_i , and permutation matrices, P_i .

Godsil and Roy [8] have shown that the Alltop construction produces MUBs that are equivalent to the set of MUBs constructed using $\Pi(x) = x^2$ in the Planar function construction, which naturally leads to the following question:

Question 4. If another function exists such that $\Delta_{fa}(x)$ is planar, will the sets of MUBs constructed be equivalent?

Any function which meets the criteria of Question 3 will hence forth be called an Alltop type function.

Definition 5. An Alltop type polynomial is a polynomial, f , such that for each $a \in \mathbb{F}_q^*$

$$\Delta_{fa}(x) = \Pi_a(x) \quad (5)$$

for some planar polynomial Π_a .

We investigate Question 3 establishing that Alltop type functions cannot exist on fields of characteristic 3, and show that for the class of planar functions of the form $\Pi(x) = x^{p^k+1}$ with p a prime, $f(x) = x^3$ is the only Alltop type function.

II. PRELIMINARIES

We begin with some preliminary results concerning polynomials. The following properties of binomial expansions will be used in calculating $\Delta_{fa}(x)$.

Lemma 6. [15, Prop. 8] Let $n = \sum a_i p^i$ and $k = \sum b_i p^i$ with $0 \leq a_i, b_i \leq p$. Then $p \nmid \binom{n}{k}$ if and only if $0 \leq b_i \leq a_i$ for all i .

Lemma 7. [15, Cor 19.1] If $p^s | n$ and $(k, p) = 1$, then $p^s | \binom{n}{k}$.

Lemma 8. [15, Cor 10.2]

$$\binom{p^s}{k} = \begin{cases} 1 \pmod{p} & \text{if } k \in \{0, p^s\} \\ 0 \pmod{p} & \text{if } 1 \leq k \leq p^s - 1 \end{cases} \quad (6)$$

Corollary 9.

$$\binom{p^s + 1}{k} \begin{cases} \neq 0 \pmod{p} & \text{if } k \in \{0, 1, p^s, p^s + 1\} \\ = 0 \pmod{p} & \text{if } 2 \leq k \leq p^s - 1 \end{cases} \quad (7)$$

$$\binom{p^s + 2}{k} \begin{cases} \neq 0 \pmod{p} & \text{if } k \in \{0, 1, 2, p^s, \\ & p^s + 1, p^s + 2\} \\ = 0 \pmod{p} & \text{if } 3 \leq k \leq p^s - 1 \end{cases} \quad (8)$$

Lemma 10. $k \binom{n}{k} = n \binom{n-1}{k-1}$.

Using these preliminary facts, we can calculate a few properties of $\Delta_{fa}(x)$ when f is a monomial.

Lemma 11. Let \mathbb{F}_q be a field of characteristic p and $f(x) = x^n$ with $n = p^s$, where $s \geq 0$. Then $\Delta_{fa}(x)$ is constant for all $a \in \mathbb{F}_q^*$.

Proof: By the Taylor's expansion $\Delta_{fa}(x) = \sum_{i=1}^n \binom{n}{i} a^i x^{n-i}$. By Lemma 8 $p | \binom{n}{k}$ for all $k \in \{1, \dots, p^s - 1\}$ hence $(x+a)^n - x^n$ is constant. ■

Theorem 12. Let \mathbb{F}_q be a field of characteristic p and $f(x) = x^n$ with $n = p^s m$ where

$s \geq 0, m > 1$ and $(m, p) = 1$. Then $\Delta_{fa}(x)$ has degree $p^s(m-1)$ for all $a \in \mathbb{F}_q^*$.

Proof: Let $f(x) = x^n$ then by the Taylor's expansion $\Delta_{fa}(x) = \sum_{i=1}^n \binom{n}{i} a^i x^{n-i}$. We need to show that the first non-zero coefficient in this binomial expansion is $\binom{n}{p^s}$.

We start with $s = 0$. Then n and p are co-prime and $\binom{n}{p^s} = \binom{n}{1} = n$ which is not divisible by p .

Next consider $s > 0$ and recall $m > 1$.

If $s = 1$, then $n = pm$ and, by Lemma 7, $p | \binom{n}{i}$ for $1 \leq i \leq p-1$ but $p \nmid \binom{n}{p}$ which is the coefficient of $x^{n-p} = x^{p(m-1)}$ and hence $\Delta_{fa}(x)$ has degree $p(m-1)$.

For $s > 1$, it is clear from Lemma 7 that $p | \binom{n}{i}$ for all i such that $(p, i) = 1$. The question that remains is whether $p | \binom{n}{i}$ for those $i < p^s$ with i, p not co-prime.

Let $i = p^k t$ for $1 \leq k < s$ and $(p, t) = 1, t \geq 1$.

By Lemmas 7 and 10,

$$\binom{n}{p^k t} = \frac{n}{p^k t} \binom{n-1}{p^k t - 1} \quad (9)$$

$$= \frac{p^{s-k} m}{t} \binom{n-1}{p^k t - 1} \quad (10)$$

$$= 0 \pmod{p}. \quad (11)$$

Since m and p^s are co-prime, $m = \sum_{i=0}^j a_i p^i$ where $a_0 \geq 1$. Hence $n = p^s m = \sum_{i=s}^{s+j} a_{i-s} p^i$, whereas $p^s = 1 \cdot p^s + \sum_{i \neq s} 0 \times p^i$. Using Lemma 6 we find that $p \nmid \binom{n}{p^s}$. Thus $\Delta_{fa}(x)$ has degree $p^s(m-1)$. ■

Corollary 13. Let $a \in \mathbb{F}_{p^r}^*$. If $\Delta_{fa}(x) \in \mathbb{F}_{p^r}[x]$ has degree $p^s l$, where $(l, p) = 1$ and $0 \leq s \leq r$, then

$$f(x) = g(x) + \sum_{t=0}^s b_t x^{p^t(p^{s-t}l+1)}$$

where at least one of $b_t \in \mathbb{F}_{p^r}^*$, and $g(x)$ is such that $\Delta_{ga}(x)$ is of degree less than $p^s l$.

Proof: From Theorem 12, if f has degree $p^t m$ then $\Delta_{fa}(x)$ has degree $p^t(m-1)$.

$$p^t(m-1) = p^s l \quad (12)$$

$$m = p^{s-t} l + 1. \quad (13)$$

Thus the possible monomials f for which $\Delta_{fa}(x)$ has degree $p^s l$ are of degree $p^t(p^{s-t}l+1)$ where $0 \leq t \leq s$. ■

Lemma 14. [5] Let $L(x)$ and $L'(x)$ be additive permutation polynomials, and $M(x)$ an additive polynomial on a field \mathbb{F} of characteristic p . Let $\Pi'(x) = L'(\Pi(L(x))) + M(x) + \delta$. If Π is a planar function on a field \mathbb{F} , then Π' is also a planar function on \mathbb{F} for all $\delta \in \mathbb{F}$.

The functions Π and Π' are considered equivalent [4]. For a field of characteristic p , an additive polynomial has the shape

$$M(x) = \sum_{i=0}^k a_i x^{p^i}. \quad (14)$$

The families of planar functions are specified by conditions on the degree of the monomials which make up Π . Hence we are only considering $L(x), L'(x)$ to have degree 1. Any polynomial on \mathbb{F}_q may be reduced modulo $x^q - x$ to yield a polynomial of degree less than q which induces the same function on \mathbb{F}_q [5]. Hence we only consider polynomials of degree less than q .

With the aid of the preceding facts about polynomial expansions, we show that no Alltop type functions exist in fields of characteristic 3, and that a specific class of planar functions has a unique Alltop type function.

A more recent and extensive list of planar functions can be found in [11]. New planar functions are continually being discovered. The results presented here are not an exhaustive investigation, but show some promising directions for future work.

III. SPECIFIC CLASSES OF PLANAR FUNCTIONS

It is known that planar functions do not exist in field of characteristic 2 [6]. We show that Alltop type functions cannot exist in a field of characteristic 3.

Theorem 15. There are no Alltop type polynomials over \mathbb{F}_{3^r} .

Proof:

$$\Delta_{fa}(x) = f(x+a) - f(x) \quad (15)$$

$$\Delta \Delta_{fab}(x) = f(x+a+b) - f(x+b) - f(x+a) + f(x). \quad (16)$$

In a field of characteristic 3, $-1 \equiv 2$, hence

$$\begin{aligned} \Delta\Delta_{fab}(x) &= f(x+a+b) + 2f(x+b) \\ &\quad + 2f(x+a) + f(x). \end{aligned} \quad (17)$$

Let $a = b = 1$ then

$$\begin{aligned} \Delta\Delta_{f11}(x) &= f(x+2) + 2f(x+1) + 2f(x+1) \\ &\quad + f(x) \end{aligned} \quad (18)$$

$$= f(x+2) + f(x+1) + f(x). \quad (19)$$

Now let $x = 1, 0$

$$\Delta\Delta_{f11}(0) = f(2) + f(1) + f(0), \quad (20)$$

$$\Delta\Delta_{f11}(1) = f(0) + f(2) + f(1), \quad (21)$$

$$= \Delta\Delta_{f11}(0). \quad (22)$$

Hence $\Delta\Delta_{f11}(x)$ is not a permutation polynomial, $\Delta_{f1}(x)$ is not a planar function, and f is not an Alltop type polynomial. ■

This is of particular importance since while new planar functions are continually being discovered, half of the known classes of planar functions exist only on fields of characteristic 3 [11]. On the other hand, the relative known abundance of planar functions on fields of characteristic 3, may be more a product of the ease of search, than the rarity of planar functions on fields of higher characteristic.

Theorem 16. [7] *Let $\Pi_1(x) = x^{p^k+1}$ on \mathbb{F}_{p^r} , where p is an odd prime, $k \geq 0$ is an integer and $\frac{r}{\gcd(r,k)}$ is an odd integer. Then $\Pi_1(x)$ is a planar function.*

This includes x^2 is a special case. We now show that a cubic is the only Alltop type polynomial for this class of planar functions, conditional that $p = 5$.

Theorem 17. *Let $\Pi_1(x) = x^{p^k+1}$ on \mathbb{F}_{p^r} , where $k \geq 0$ is an integer and $\frac{r}{\gcd(r,k)}$ is an odd integer. If for each $a \in \mathbb{F}_{p^r}^*$ there exist $\alpha_a, \beta_a, \delta_a \in \mathbb{F}_{p^r}$, an additive polynomial $M_a(x)$ and a polynomial $f_a(x)$ such that,*

$$\Delta_{fa}(x) = \alpha_a \Pi_1(x + \beta_a) + M_a(x) + \delta_a \quad (23)$$

then $p \geq 5$ and $f_a(x)$ is equivalent to a polynomial of degree 3.

Proof: Theorem 15 shows that $p \geq 5$. The proof proceeds by establishing a set of possible degrees for f , and eliminating all possibilities other

than 3. For ease of notation let $\alpha_a = \alpha$, $\beta_a = \beta$, $\delta_a = \delta$, $M_a(x) = M(x)$, and $f_a(x) = f(x)$.

It is assumed that $\Delta_{fa}(x) = \alpha \Pi_1(x + \beta) + M(x) + \delta$. Since $\alpha \Pi_1(x + \beta) + M(x) + \delta$ has a term of degree $p^k + 1$, and hence by Corollary 13 f has a term of degree $p^k + 2$.

Consider a general polynomial function $f(x)$ of degree n ; $f(x)$ takes the form $f(x) = \sum_{i=0}^n a_i x^i$, with $a_i \in \mathbb{F}_{p^r}$. That is, f can be written as the sum of monomials $f_i(x) = a_i x^i$ of degree i or equivalently $f(x) = \sum_{i=0}^n f_i(x)$. Hence

$$\begin{aligned} f(x+a) - f(x) &= \sum_{i=0}^n f_i(x+a) - f_i(x) \\ \Delta_{fa}(x) &= \sum_{i=1}^n \Delta_{f_i,a}(x). \end{aligned}$$

It follows that the degree of $\Delta_{f_i,a}(x)$ is less than or equal to $p^k + 1$ for all i . Each of these monomials can be treated separately, with an argument similar to that presented below.

Let $f_n = x^n$ where $n = p^s m$ and $\gcd(p, m) = 1$, and $\Delta_{f_n,a}(x)$ is of degree $p^k + 1$. By Theorem 12, the degree of $\Delta_{f_n,a}(x)$ is $p^s(m-1)$, and we know the degree of Π_1 is $p^k + 1$, so we require

$$p^s(m-1) = p^k + 1.$$

There are three cases to consider, $k, s \geq 1, k = 0$ or $s = 0$.

Case 1: If $k, s \geq 1, p | p^s(m-1)$ but $p \nmid (p^k + 1)$ leading to a contradiction.

Case 2: If $k = 0$, then $p^s(m-1) = 2$ and so $s = 0$ and $m = 3$, which implies $p \geq 5$ as already shown. This is the Alltop function.

Case 3: If $s = 0$, we assume $k \geq 1$ and search for solutions for n when for some i $f_i(x)$ has degree $p^k + 2$ thus

$$f(x) = x^{p^k+2} + g(x), \quad (24)$$

with $g(x)$ a polynomial function such that $\Delta_{ga}(x)$ is of degree p^k or less. By assumption

$$\Delta_{fa}(x) = \alpha(x + \beta)^{p^k+1} + M(x) + \delta.$$

Using Corollary 9, this can be simplified to

$$\begin{aligned} \Delta_{fa}(x) &= \alpha x^{p^k+1} + \alpha\beta x^{p^k} + \alpha\beta^{p^k} x \\ &\quad + \alpha\beta^{p^k+1} + \sum_{i=0}^k a_i x^{p^i} + \delta. \end{aligned} \quad (25)$$

On the other hand, using equation 24 and Corollary 9 we get

$$\begin{aligned} \Delta_{fa}(x) &= (x+a)^{p^k+2} - x^{p^k+2} + \Delta_{ga}(x) \\ &= 2ax^{p^k+1} + a^2x^{p^k} + a^{p^k}x^2 \\ &\quad + 2a^{p^k+1}x + a^{p^k+2} + \Delta_{ga}(x) \end{aligned} \quad (26)$$

By comparing the coefficient of the x^{p^k+1} terms in equations 25 and 26 we find that

$$\alpha = 2a. \quad (27)$$

If $\Delta_{ga}(x)$ has degree p^k , then by Corollary 13, $g(x) = \sum_{r=0}^k b_r x^{p^r(p^{k-r}+1)} + h(x)$ where $h(x)$ is a polynomial such that $\Delta_{ha}(x)$ is a polynomial of degree $p^k - 1$ or less. Let $b' = \sum_{r=0}^k \binom{p^k+p^r}{p^r} b_r a^{p^r}$.

$$\begin{aligned} \Delta_{fa}(x) &= (x+a)^{p^k+2} - x^{p^k+2} + \Delta_{ga}(x) \quad (28) \\ &= 2ax^{p^k+1} + (a^2 + b')x^{p^k} \\ &\quad + \sum_{r=0}^k \binom{p^k+p^r}{p^r} b_r a^{p^k} x^{p^r} \\ &\quad + a^{p^k}x^2 + 2a^{p^k+1}x + a^{p^k+2} \\ &\quad + \sum_{r=0}^k b_r a^{p^r(p^{k-r}+1)} + \Delta_{ha}(x) \end{aligned} \quad (29)$$

There exists an additive polynomial M in equation (23) that can equate the coefficients of any term of the x^{p^i} terms in equations (25) and (29).

Note that equation (25) has no x^2 term but equation (29) does. Hence the coefficient of the x^2 term in $\Delta_{ha}(x)$ must be nonzero, and must cancel with the x^2 term already present in equation (29).

However, we note that all the higher order terms are in agreement, hence all such terms in $\Delta_{ha}(x)$ must have zero coefficients implying $\Delta_{ha}(x)$ has degree 2, and consequently $h(x)$ is equivalent to a polynomial of degree 3. Thus let $h(x) = tx^3 + ux^2 + M(x) + w$ where $M'(x)$ is an additive polynomial. Equation (26) becomes

$$\begin{aligned} \Delta_{fa}(x) &= 2ax^{p^k+1} + (a^2 + b')x^{p^k} \\ &\quad + \sum_{r=0}^k \binom{p^k+p^r}{p^r} b_r a^{p^k} x^{p^r} \\ &\quad + (a^{p^k} + 3ta)x^2 \\ &\quad + (2a^{p^k+1} + 3ta^2 + 2ua)x + a^{p^k+2} \\ &\quad + \sum_{r=0}^k b_r a^{p^r(p^{k-r}+1)} + ta^3 + ua^2 \\ &\quad + \Delta_{M'a}(x) \end{aligned} \quad (30)$$

Note that $t, u, \in \mathbb{F}_{p^r}$ and are fixed for $f(x)$. The coefficient of the x^2 term in equation (30) is $\binom{p^k+2}{2}a^{p^k} + 3ta$ while in equation (25) the coefficient of x^2 is zero. Thus

$$\begin{aligned} 0 &= a^{p^k} + 3ta \\ &= a[a^{p^k-1} + 3t] \\ &= a^{p^k-1} + 3t \end{aligned} \quad (31)$$

In equation (31) p, k and t are fixed and a can take any value in the field. Under the given assumptions,

$$a^{p^k-1} = a^{t^{p^k-1}} \quad (32)$$

for all $a, a' \in \mathbb{F}_{p^r}^*$, hence

$$a^{p^k-1} = 1 \quad (33)$$

for all $a \in \mathbb{F}_{p^r}^*$. Consequently $x^{p^k+2} \equiv x^3$, and $x^{2p^k} \equiv x^2$. Note that equation 33 implies that $k = 0$ or r divides k . Hence f is equivalent to a polynomial of degree 3 which is already shown to be a valid solution in case 2. ■

IV. CONCLUSION

We have shown that for a specific family of Planar functions, a cubic is the only Alltop type polynomial. We have also shown that Alltop type functions cannot exist on fields of characteristic 3, which means that Alltop type functions cannot exist for many classes of planar functions.

New planar polynomials are continually being discovered. Thus investigating the existence of Alltop type polynomials for all classes of planar function cannot yet be completed. However many of the newly discovered planar functions are on fields of characteristic 3. So perhaps the possible solution space is not expanding so rapidly.

The question of the existence of another Alltop type polynomial is still open. As is the question of whether any Alltop type polynomial would produce a set of MUBs which are non-equivalent to the corresponding planar function MUBs.

ACKNOWLEDGMENT

Thanks are due to the referees who noted simplifications in the proof of Theorem 17.

This work was partially supported by an Australian Mathematical Society Lift-Off fellowship.

REFERENCES

- [1] W.O. Alltop. Complex sequences with low periodic correlations. *IEEE Transactions on Information Theory*, 26(3):350–354, 1980.
- [2] C.H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984.
- [3] S. Brierley and S. Weigert, and I. Bengtsson. All mutually unbiased bases in dimensions two to five. *Quantum Information and Computing*, 10(9):803–820 2010.
- [4] C. Carlet and C. Ding. Highly nonlinear mappings. *Journal of Complexity*, 20:205–244, 2004.
- [5] R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes and Cryptography*, 10(2):167–184, 1997.
- [6] P. Dembowski. *Finite Geometries*. Classics in Mathematics. Springer, reprint of the 1968 edition, 1997.
- [7] P. Dembowski and T.G. Ostrom. Planes of order n with collineation groups of order n^2 . *Mathematische Zeitschrift*, 103(3):239–258, 1968.
- [8] C. Godsil and A. Roy. Equiangular lines, mutually unbiased bases, and spin models. *European Journal of Combinatorics*, 30(1):246–262, 2009.
- [9] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. *Lecture Notes in Computer Science*, 2948:137–144, 2003.
- [10] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University press, 1997.
- [11] Alexander Pott and Yue Zhou. Switching construction of planar functions on finite fields. In M. Hasan and Tor Helleseth, editors, *Arithmetic of Finite Fields*, volume 6087 of *Lecture Notes in Computer Science*, pages 135–150. Springer Berlin / Heidelberg, 2010.
- [12] A. Roy and A.J. Scott. Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements. *Journal of Mathematical Physics*, 48(072110):1–24, 2007.
- [13] V. Scarani, A. Aćin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(057901):1–4, 2004.
- [14] J. Schwinger. Unitary Operator Bases. *Proceedings of the National Academy of Sciences of the United States of America*, 46(4):570–579, 1960.
- [15] David Singmaster. Divisibility of binomial and multinomial coefficients by primes and prime powers. In Verner E. Hoggatt Jr. and Marjorie Bicknell-Johnson, editors, *A Collection of Manuscripts Related to Fibonacci Sequences*, pages 98–113. The Fibonacci Association, Santa Clara, Calif, 1980.
- [16] W. Wootters and B. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.