Bull. Austral. Math. Soc. 11T06
Vol. 56 (1997) [429-437]

BENT POLYNOMIALS OVER FINITE FIELDS

Robert S. Coulter and Rex W. Matthews

The definition of bent is redefined for any finite field. Our main result is a complete description of the relationship between bent polynomials and perfect non-linear functions over finite fields: we show they are equivalent. This result shows that bent polynomials can also be viewed as the generalisation to several variables of the class of polynomials known as planar polynomials. An explicit method for obtaining large sets of not necessarily distinct maximal orthogonal systems using bent polynomials is given and we end with a short discussion on the existence of bent polynomials over finite fields.

1. Origins and definitions

Bent functions were introduced by Rothaus in 1976 and have since been shown to have a wide range of applications. Defined originally over $\mathbb{Z}_2$ and then generalised to $\mathbb{Z}_q$ for general q they have indirectly been studied over prime fields. In this article we formally define the notion of bent polynomial for any finite field. The definition relies on the concept of the Discrete Fourier Transform which we define in terms of additive characters following the notation used in [**6**, Chapter 5]. Throughout we use the following conventions: p is a prime, $q = p^e$ for some positive integer e, $\mathbb{F}_q$ denotes the finite field with q elements and $\mathbb{F}_q^*$ the non-zero elements of $\mathbb{F}_q$. For a positive integer n, $\mathbb{F}_q^n$ denotes the set of all n-tuples of elements from $\mathbb{F}_q$ while $\mathbb{Z}_m^n$ is similarly defined from the ring of integers modulo m. Finally, we use $\mathbb{F}_q[X_1, \ldots, X_n]$ to denote the set of all n-variable polynomials over $\mathbb{F}_q$ and $\mathbb{V}_q^m[X_1, \ldots, X_n]$ for the set of all m-tuples of polynomials in the variables $X_1, \ldots, X_n$ in $\mathbb{F}_q$.

The function χ_1 defined by

$$\chi_1(x) = e^{2\pi i Tr(x)/p}$$

for all $x \in \mathbb{F}_q$ is called the canonical additive character of $\mathbb{F}_q$. Here $Tr : \mathbb{F}_q \to \mathbb{F}_p$ denotes the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. For $y \in \mathbb{F}_q$, the function $\chi_y(x) = \chi_1(yx)$ for

Received 13th January, 1997

The majority of this work was completed in [**2**] and presented at the 3rd International Conference of Finite Fields and Applications at Glasgow, Scotland in July, 1995. We note that parts of this work have appeared recently in [**1**].

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

all $x \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$ and every character of $\mathbb{F}_q$ can be obtained in this way. Finally, we note that χ_0 is the trivial additive character which satisfies $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$.

Definition 1.1: Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$. The Discrete Fourier Transform of f is the complex valued function $c_{f,\chi} : \mathbb{F}_q^n \to \mathbb{C}$ given by

$$c_{f,\chi}(\lambda) = \frac{1}{q^{n/2}} \sum_{x \in \mathbb{F}_q^n} \chi\big(f(x) - \lambda \cdot x\big)$$

where $\chi : \mathbb{F}_q \to \mathbb{C}$ is any non-trivial additive character on $\mathbb{F}_q$ and $\cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is the usual scalar dot product.

The polynomials we shall study within this paper are defined as follows.

Definition 1.2: A polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ is said to be *bent* if every Fourier coefficient has unit magnitude for any non-trivial character. Explicitly,

$$\left| \frac{1}{q^{n/2}} \sum_{x \in \mathbb{F}_q^n} \chi\big(f(x) - \lambda \cdot x\big) \right| = 1$$

for all $\lambda \in \mathbb{F}_q^n$ and for all $\chi \neq \chi_0$.

The reason for the term bent used in the above definition is historical. These polynomials can be viewed as a generalisation to finite fields of a well known class of functions called bent functions which have been previously defined only on $\mathbb{Z}_m^n$. These functions were first introduced by Rothaus [**10**] on $\mathbb{Z}_2^n$ and generalised to $\mathbb{Z}_m^n$ by Kumar, Scholtz and Welch in [**5**]. In those cases the motivation for studying bent functions lies with properties of these functions which are relevant to coding theory and cryptology. In this paper we consider bent polynomials as multivariate analogues of planar polynomials defined over a finite field.

2. Some General Properties

In this section we shall establish some properties of bent polynomials. In particular we shall discuss their permutation behaviour and how they act under composition with additive polynomials. We shall use the following concept for a multivariate polynomial (see [**6**, Definition 7.34]).

Definition 2.1: A polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ is called a *permutation polynomial* in n indeterminates over $\mathbb{F}_q$ if the equation

$$f(x_1, \dots, x_n) = a$$

has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $a \in \mathbb{F}_q$.

Bent functions have been closely associated with the class of functions called perfect non-linear functions, which we define here over finite fields.

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

DEFINITION 2.2: Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$. Then we call f *perfect non-linear* if for every $a \in \mathbb{F}_q^n$, $a \neq 0$, the difference polynomial $\Delta_{f,a}$ defined by

$$\Delta_{f,a}(X) = f(X+a) - f(X)$$

is a permutation polynomial.

Over $\mathbb{Z}_m^n$ bent functions and perfect non-linear functions have been shown to be closely linked. Nyberg in [8] proved that any perfect non-linear function must be bent, while a bent function must be perfect non-linear if m is prime. When dealing with a general finite field the connection between the two classes is much simpler. In fact, they are equivalent.

THEOREM 2.3. *A polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is perfect non-linear if and only if it is bent.*

PROOF: Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$. Then for arbitrary $\chi \neq \chi_0$,

$$\begin{aligned} |c_{f,\chi}(\lambda)|^2 &= c_{f,\chi}(\lambda)\overline{c_{f,\chi}(\lambda)} \\ &= \frac{1}{q^n}\sum_{x\in\mathbb{F}_q^n}\chi\big(f(x)-\lambda\cdot x\big)\overline{\sum_{y\in\mathbb{F}_q^n}\chi\big(f(y)-\lambda\cdot y\big)} \\ &= \frac{1}{q^n}\sum_{x\in\mathbb{F}_q^n}\chi\big(f(x)\big)\sum_{y\in\mathbb{F}_q^n}\chi\big(-f(y)-\lambda\cdot(x-y)\big) \\ &= \frac{1}{q^n}\sum_{x\in\mathbb{F}_q^n}\chi\big(f(x)\big)\sum_{z\in\mathbb{F}_q^n}\chi\big(-f(x-z)-\lambda\cdot z\big) \\ (1) \qquad &= \frac{1}{q^n}\sum_{z\in\mathbb{F}_q^n}\chi(-\lambda\cdot z)\sum_{x\in\mathbb{F}_q^n}\chi\big(f(x)-f(x-z)\big). \end{aligned}$$

Suppose f is a perfect non-linear polynomial. Then the inner sum of (1) is zero unless $z = 0$ in which case the inner sum has value q^n. Hence we have $|c_{f,\chi}(\lambda)|^2 = 1$ and f is a bent polynomial.

Now suppose f is a bent polynomial. Let

$$S_\chi(f,z) = \sum_{x\in\mathbb{F}_q^n}\chi\big(f(x+z)-f(x)\big).$$

Then (1) becomes

$$(2) \qquad \sum_{z\in\mathbb{F}_q^n}\chi(\lambda\cdot z)\overline{S_\chi(f,z)} = q^n$$

for all $\lambda \in \mathbb{F}_q^n$. We need to show that $S_\chi(f,z) = 0$ for all $z \in \mathbb{F}_q^n$, $z \neq 0$. From (2) we have q^n equations in q^n unknowns. Ordering the elements of $\mathbb{F}_q^n$ by $\alpha_0, \ldots, \alpha_{q^n-1}$ with

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

$\alpha_0 = 0$, we can express (2) as the following matrix equation.

$$\tag{3} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \chi(\alpha_1 \cdot \alpha_1) & \dots & \chi(\alpha_1 \cdot \alpha_{q^n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \chi(\alpha_{q^n-1} \cdot \alpha_1) & \dots & \chi(\alpha_{q^n-1} \cdot \alpha_{q^n-1}) \end{pmatrix} \begin{pmatrix} \overline{S_\chi(f,1)} \\ \overline{S_\chi(f,\alpha_1)} \\ \vdots \\ \overline{S_\chi(f,\alpha_{q^n-1})} \end{pmatrix} = \begin{pmatrix} q^n \\ q^n \\ \vdots \\ q^n \end{pmatrix}.$$

Let H denote the $q^n \times q^n$ matrix in the above equation. Then using the orthogonality relations for characters we have

$$\overline{H}^T H = q^n I.$$

Multiplying (3) by $\overline{H}^T$ on the left yields the q^n equations

$$\tag{4} \overline{S_\chi(f,\alpha_j)} = \sum_{i=0}^{q^n-1} \overline{\chi(\alpha_i \cdot \alpha_j)}$$

for $j = 0, \dots, q^n - 1$. However for $\alpha_j \neq 0$ the right hand side of (4) is zero. Hence $S_\chi(f,z) = 0$ for all $z \in \mathbb{F}_q^n$, $z \neq 0$, and so f is a perfect non-linear polynomial. ▯

As previously mentioned, equivalence in the prime case was established by Nyberg in [**8**]. We illustrate that the above result is a true generalisation of Nyberg's work. By choosing a basis $(y_1, \dots, y_r)$ of a general field $\mathbb{F}_q$, with $q = p^r$, viewed as a vector space over its prime subfield, a bent polynomial from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ is equivalent to a bent transformation from $\mathbb{F}_p^{rn}$ to $\mathbb{F}_p^r$. Thus the above result is fundamentally different to the result of Nyberg [**8**, Theorem 2.3] in that there the result is only shown for the case $r = 1$. In other words Nyberg proves the result for single valued polynomials on $\mathbb{F}_p$, not vector valued polynomials as is shown here.

A polynomial $L \in \mathbb{F}_q[X]$ is called *additive* on $\mathbb{F}_q$ if $L(x+y) = L(x)+L(y)$ for all $x, y \in \mathbb{F}_q$. Any such L can be regarded as an $\mathbb{F}_p$-linear transformation of $\mathbb{F}_q$. Polynomials which induce an $\mathbb{F}_p$-linear transformation are known in the literature as *linearised polynomials*. There is an explicit description of such polynomials: their reduced form has the shape

$$L(X) = \sum_{i=0}^{e-1} a_i X^{p^i}$$

where $a_i \in \mathbb{F}_q$. We note that the existence of an additive polynomial vector mapping $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ is equivalent to the existence of an additive polynomial over $\mathbb{F}_{q^n}$. Here, by an additive vector polynomial f we mean $f \in \mathbb{V}_q^n[X_1, \dots, X_n]$ with $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{F}_q^n$.

Since the polynomials may always be considered as reduced, we may assume that any additive polynomial has the above shape. These polynomials form a subset of the class of polynomials called *affine polynomials*. Affine polynomials have been studied extensively and we refer the reader to [**6**, pages 107-124] for their properties. The following result is well known, see [**6**, Theorem 7.9] for example.

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

Lemma 2.4. *Let $L \in \mathbb{F}_q[X]$ be defined by*

$$L(X) = \sum_{i=0}^{e-1} a_i X^{p^i}.$$

Then L is a permutation polynomial over $\mathbb{F}_q$ if and only if L has no roots in $\mathbb{F}_q$ other than 0.

If we choose a standard basis for $\mathbb{F}_q^n$ over $\mathbb{F}_q$ (for example, $1, z, z^2, \ldots$ with z a generator) then an additive polynomial vector will be a permutation polynomial vector if and only if it has no roots other than the zero vector. This can be shown by using the linear independence of the basis chosen and relating the additive polynomial vector back to its additive polynomial which must be a permutation polynomial.

In connection with Theorem 2.3 we shall define $\Delta_{f,a} \in \mathbb{F}_q[X_1, \ldots, X_n]$ by

$$\Delta_{f,a}(X) = f(X + a) - f(X) \tag{5}$$

where $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $a \in \mathbb{F}_q^n$. In light of Theorem 2.3 it is clear that we shall be particularly interested in $\Delta_{f,a}$ whenever a is not the all zeros vector. The following two results are the obvious generalisations of [**3**, Theorem 2.3] and as the proofs are the same as those given there we omit them.

Theorem 2.5. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ and let $L \in \mathbb{F}_q[X]$ be additive. Then $L(f)$ is bent if and only if f is bent and L is a permutation polynomial.*

Theorem 2.6. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ and let $L_n \in \mathbb{V}_q^n[X_1, \ldots, X_n]$ be an additive polynomial vector. Then $f\bigl(L_n(X)\bigr)$ is a bent polynomial if and only if f is bent and L_n is a permutation polynomial vector.*

3. Orthogonal Systems and the Single Variable Case

Definition 3.1: A system of polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $1 \leqslant m \leqslant n$, is said to be *orthogonal* in $\mathbb{F}_q$ if the system of equations

$$f_1(x_1, \ldots, x_n) = y_1, \ldots, f_m(x_1, \ldots, x_n) = y_m$$

has exactly q^{n-m} solutions in $\mathbb{F}_q^n$ for each $(y_1, \ldots, y_m) \in \mathbb{F}_q^m$. If $n = m$ then we shall call the system *maximal.*

Niederreiter in [7] showed that every polynomial in an orthogonal system must be a permutation polynomial. We now show that bent polynomials are also related to orthogonal systems.

Theorem 3.2. *Let $f \in \mathbb{F}_{q^n}[X]$ be a bent polynomial. Then f defines n distinct bent polynomials $f_1, \ldots, f_n$ over $\mathbb{F}_q^n$ such that the set of polynomials*

$$\{\Delta_{f_i,a} \in \mathbb{F}_q[X_1, \ldots, X_n] \mid \Delta_{f_i,a}(X) = f_i(X + a) - f_i(X),\ i = 1, \ldots, n\}$$

forms a maximal orthogonal system in $\mathbb{F}_q$ for each non zero $a \in \mathbb{F}_q^n$.

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

PROOF: Let f be a bent polynomial over $\mathbb{F}_{q^n}$. Then $f(X+a)-f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_{q^n}^*$. Select $(y_1, \dots, y_n)$, $y_i \in \mathbb{F}_{q^n}$, to be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then any $a \in \mathbb{F}_{q^n}$ can be written in the form

$$a = a_1y_1 + a_2y_2 + \cdots + a_ny_n$$

with each $a_i \in \mathbb{F}_q$. In particular we may write

$$f(X) = \sum_{i=1}^{n} f_i(X_1, \dots, X_n)y_i$$

where $f_i \in \mathbb{F}_q[X_1, \dots, X_n]$ for $i = 1, \dots, n$ and $X = \sum_{i=1}^{n} X_iy_i$. Similarly we have for any $a \in \mathbb{F}_{q^n}$

$$f(X+a) = \sum_{i=1}^{n} f_i(X_1 + a_1, \dots, X_n + a_n)y_i$$

and combining yields

$$f(X+a) - f(X) = \sum_{i=1}^{n} y_i\big(f_i(X_1 + a_1, \dots, X_n + a_n) - f_i(X_1, \dots, X_n)\big)$$

for all $a \in \mathbb{F}_{q^n}$. As f is bent we have that each f_i must be a bent polynomial on $\mathbb{F}_q^n$. Moreover, for f to be a bent polynomial, the set Δ_a given by

$$\{\Delta_{f_i,a} \in \mathbb{F}_q[X_1, \dots, X_n] \mid \Delta_{f_i,a}(X) = f_i(X+a) - f_i(X),\ i = 1, \dots, n\}$$

must form a maximal orthogonal system for each non-zero $a \in \mathbb{F}_q^n$. If $f_i = f_j$ for some $1 \leqslant i < j \leqslant n$ then none of the sets Δ_a could be orthogonal. Hence the n bent polynomials are distinct. $\square$

So a bent polynomial in one variable over $\mathbb{F}_{q^n}$ describes $q^n - 1$ not necessarily distinct maximal orthogonal systems in $\mathbb{F}_q$. A bent polynomial in one variable is also known as a planar polynomial or planar function.

Planar functions were first introduced by Dembowski and Ostrom in [4] in connection with projective planes satisfying certain properties. A recent paper by the authors [3] considered several aspects of planar functions over finite fields and the planes described by them. In particular, several classes of planar polynomials were identified and they can be listed as follows:

(i) $f(X) = X^2$, which gives the Desarguesian plane over $\mathbb{F}_q$, q odd.

(ii) $f(X) = X^{p^\alpha+1}$, which is planar over $\mathbb{F}_{p^e}$, p odd, if and only if $e/(\alpha, e)$ is odd.

(iii) $f(X) = X^{10} + X^6 - X^2$, which is planar over $\mathbb{F}_{3^e}$ if and only if $e = 2$ or e is odd.

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

(iv) $f(X) = X^{(3^\alpha+1)/2}$, which is planar over $\mathbb{F}_{3^e}$ if and only if $(\alpha, e) = 1$ and α is odd.

From experimental data it appears that all known planar polynomials are equivalent to one of these types in the sense that they can be obtained through multiple applications of Theorems 2.5 and 2.6, and through the addition of single variabled additive polynomials. (If $f \in \mathbb{F}_q[X]$ is a planar polynomial then so is $f + L$ for any additive polynomial $L \in \mathbb{F}_q[X]$.)

The study of planar functions has so far been motivated essentially by their connection with projective planes. They are also studied under the name of relative difference sets. Each planar function describes an affine plane whose projective closure satisfies certain properties, see [**4**] for details. Until recently all known finite planes described by planar functions were either semi-field planes or Desarguesian. However, in [**3**] a new class of planar polynomials was discovered (the fourth class in the list above) which described a class of planes which could not be coordinatised by quasi-fields. These planes were shown to be of Lenz-Barlotti class II (they have since been shown to be LB Class II.1 by Jill Yaqub). All previously known such planes had been obtained through derivation or lifting and so had square prime power order. The new class of planes contains at least one Lenz-Barlotti class II plane of order 3^e for each $e \geqslant 4$. We summarise with the following theorem which was implicitly proven in [**3**] but not explicitly stated.

THEOREM 3.3. *There exist planes of Lenz-Barlotti class II which have non-square order and hence cannot be obtained by derivation or lifting.*

This answers affirmatively a problem which has been in existence virtually since the introduction of the concept of derivation by Ostrom in the 1960's.

4. EXISTENCE

We end with some remarks on the existence of bent polynomials. As can be seen from the listing above, bent polynomials in one variable exist over $\mathbb{F}_q$ for all $q = p^e$ with p an odd prime – a simple argument shows that bent polynomials in one variable cannot exist when $p = 2$, see [**9**]. In particular, the polynomial X^2 is bent over all finite fields of odd order. The application of Theorem 3.2 to X^2 over $\mathbb{F}_{q^n}$ for any n shows that there must exist bent polynomials in n variables over $\mathbb{F}_q$ for any q odd.

The existence of bent functions over $\mathbb{Z}_q$ has been dealt with in many papers. In a similar vein to [**5, 10**] we have the following.

LEMMA 4.1. *Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ and $g \in \mathbb{F}_q[X_1, \dots, X_m]$. If f and g are bent then the polynomial $F = f + g \in \mathbb{F}_q[X_1, \dots, X_{n+m}]$ is bent. If q is prime then the converse holds also.*

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

PROOF: Let f and g be bent. We have

$$\begin{aligned} c_{F,\chi}(\lambda) &= \frac{1}{q^{(n+m)/2}} \sum_{z\in\mathbb{F}_q^{n+m}} \chi\bigl(F(z) - \lambda\cdot z\bigr) \\ &= \frac{1}{q^{(n+m)/2}} \sum_{x\in\mathbb{F}_q^n,\, y\in\mathbb{F}_q^m} \chi\bigl(f(x) + g(y) - (\lambda_n, \lambda_m)\cdot(x,y)\bigr) \\ &= \frac{1}{q^{n/2}q^{m/2}} \Bigl(\sum_{x\in\mathbb{F}_q^n} \chi\bigl(f(x) - \lambda_n\cdot x\bigr)\Bigr)\Bigl(\sum_{y\in\mathbb{F}_q^m} \chi\bigl(g(y) - \lambda_m\cdot y\bigr)\Bigr) \\ &= c_{f,\chi}(\lambda_n)c_{g,\chi}(\lambda_m). \end{aligned}$$

Clearly F is bent if f and g are. For the converse see [**5**, **10**]. □

For $q = 2$ this was first shown by Rothaus [**10**]. Kumar, Scholtz and Welch in [**5**] claimed the forward part of the above result for general $\mathbb{Z}_q$ without proof with the statement that it was a straight generalisation of Rothaus' proof. We note that as the converse part of Rothaus' proof can also be generalised it seems likely that Kumar, Scholtz and Welch meant to claim the full generalisation of Rothaus' Theorem. Thus for q an odd prime we attribute Lemma 4.1 to [**5**]. We have the following corollary.

COROLLARY 4.2. *Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ have the shape*

$$f(X_1, \dots, X_n) = \sum_{i=1}^{n} f_i(X_i),$$

with $f_i \in \mathbb{F}_q[X]$. Then f is bent if every f_i is a planar polynomial.

Of particular interest would be any bent polynomial constructed in this manner with $f_i(X_i) = X_i^{(3^\alpha+1)/2}$ for some i. As these planar monomials were only recently discovered it would be interesting to know whether any corresponding bent polynomials are already known and if so how they were constructed.

The characteristic 2 case requires special attention as no planar polynomials exist in this case. Results and constructions by Rothaus in [**10**] show that bent polynomials on $\mathbb{F}_q^n$ with $q = 2$ can only occur if n is even and that they do occur for every even n. It is a simple matter to prove the following.

LEMMA 4.3. *Let $q = 2^e$. Then the polynomial X_1X_2 is bent on $\mathbb{F}_q^2$.*

Thus it is clear that by multiple applications of Lemma 4.1 we can construct bent polynomials in characteristic 2 for any even number of variables. With the work of Rothaus just mentioned in mind this is perhaps not a surprising result. We note that if $q = 2^e$ then it is not possible for there to exist bent polynomials over $\mathbb{F}_q^n$ if ne is odd. To see this note that for $p = 2$ any additive character of $\mathbb{F}_q$ will only take values in the set $\{0, 1\}$. Thus the sums involved in the Fourier transform will be integers only. If ne is odd then q^n is not a square and so it is not possible for any Fourier coefficient to have unit magnitude.

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press

References

[1] A.S. Ambrosimov, 'Properties of bent functions of q-valued logic over finite fields', *Discrete Math. Appl.* **4** (1994), 341–350.

[2] R.S. Coulter, *Bent functions and their applications*, Honour's thesis (Department of Computer Science, University of Queensland, Australia, 1993).

[3] R.S. Coulter and R.W. Matthews, 'Planar functions and planes of Lenz-Barlotti class II', *Des. Codes Cryptogr.* **10** (1997), 167–184.

[4] P. Dembowski and T.G. Ostrom, 'Planes of order n with collineation groups of order n^2', *Math. Z.* **103** (1968), 239–258.

[5] 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.

[6] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl. **20** (Addison-Wesley, Reading, 1983).

[7] H. Niederreiter, 'Orthogonal systems of polynomials in finite fields', *Proc. Amer. Math. Soc.* **28** (1971), 415–422.

[8] K. Nyberg, 'Constructions of bent functions and difference sets', in *Eurocrypt '90*, Lecture Notes in Comput. Sci. **473** (Springer-Verlag, Berlin, Heidelberg, New York, 1991), **pp.** 151–160.

[9] L. Rónyai and T. Szőnyi, 'Planar functions over finite fields', *Combinatorica* **9** (1989), 315–320.

[10] O.S. Rothaus, 'On "Bent" functions', *J. Combin. Theory Ser. A* **20** (1976), 300–305.

Department of Computer Science
The University of Queensland
Queensland 4072
Australia
e-mail: shrub@cs.uq.edu.au

Department of Mathematics
University of Tasmania
GPO Box 252C
Hobart Tas 7000
Australia
e-mail: galois@hilbert.maths.utas.edu.au

https://doi.org/10.1017/S000497270003121X Published online by Cambridge University Press