Projective equivalence of ovals and EA-equivalence of Niho bent functions

Lilya Budaghyan, Claude Carlet, Tor Helleseth, Alexander Kholosha, Tim Penttila

Department of Informatics
University of Bergen,
Department of Mathematics
University of Paris 8 and University of Paris 13
Department of Mathematics
Colorado State University

Finite Geometries
Fourth Irsee Conference
September 14-20, 2014

Bent functions have appeared in a lot of contexts.

We take a chronological tour of some of the highlights.

Difference sets and designs

In 1949, building on work on cyclic projective planes of Hall from 1947, Chowla introduced difference sets in cyclic groups. By 1955, Bruck had extended the concept to any finite group.

A **bent function** is the characteristic function of a

$$(2^n, 2^{n-1} - 2^{(n-2)/2}, 2^{n-2} - 2^{(n-2)/2})$$

difference set in an elementary abelian 2-group of order 2^n, n even.

Thus there are **symmetric designs admitting regular elementary abelian 2-groups** arising from bent functions.

In 1976, Rothaus formally introduced bent functions based on work of his from the 1960's.

A function $f : GF(2)^n \to GF(2)$ is **bent** if the Fourier coefficients of $x \mapsto (-1)^{f(x)}$ are all ± 1.

Today, this would normally be rewritten (with a different scaling) as follows: Let f be an n-variable Boolean function. Its **"sign" function** is the integer-valued function $\chi_f(x) := (-1)^{f(x)}$. The **Walsh transform** of f is the discrete Fourier transform of χ_f whose value at point $w \in GF(2^n)$ is defined by

$$\widehat{\chi}_f(w) = \sum_{x \in GF(2^n)} (-1)^{f(x)+\mathrm{Tr}_n(wx)} \ ,$$

where Tr_n **is the absolute trace map** $GF(2^n) \to GF(2)$**, with**

$$Tr_n(x) = x + x^2 + \cdots + x^{2^{n-1}}.$$

For even n, a Boolean function f in n variables is said to be **bent** if for any $w \in GF(2^n)$ we have $\widehat{\chi}_f(w) = \pm 2^{n/2}$.

In 1976, Rothaus characterised bent functions.

Theorem (Rothaus 1976)

A function $f : GF(2)^n \to GF(2)$ is bent if and only if the matrix with entry $(-1)^{f(x+y)}$ in row x and column y is a Hadamard matrix.

In 1982, Olsen, Scholtz and Welch used bent functions to construct a new family of **nonlinear binary signal sets** which achieve the lower bound of Welch 1974 on *simultaneous cross correlation and autocorrelation magnitudes*.

These signal sets have the same parameters as Kasami codes, but have important advantages for use in **spread spectrum multiple access communication systems**.

In 1990, Meier and Staffelbach introduced a criterion for Boolean functions in terms of their Hamming distance from the set of all affine functions, which they called the **nonlinearity** of the function. They made it clear that, in cryptographic applications, it was desirable that the nonlinearity be large, in order to avoid fast correlation attacks.

Since the set of all affine Boolean functions in n variables is the Reed-Muller code $R(1, n)$, by the covering radius bound we obtain

Theorem

A function $f : GF(2)^n \to GF(2)$ has its nonlinearity bounded above by $2^{n-2} - 2^{(n-2)/2}$. Equality occurs if and only if f is bent.

In 1991, Nyberg generalised the work of Meier and Staffelbach.
A function $f : Z_q^n \to Z_q$ is **perfect non-linear** if for every fixed $w \in Z_q^n$, $w \neq 0$, the difference

$$f(x+w) - f(x)$$

takes each value in Z_q for exactly q^{n-1} values of $x \in Z_q^n$.

Theorem

A function $f : GF(2)^n \to GF(2)$ is perfect nonlinear if and only if f is bent.

Nyberg used his generalisation of the work of Meier and Staffelbach in similar cryptographic applications.

A **quasi-quadric** of $\mathrm{PG}(2m-1,q)$ is a set of points that has the same number of points as a non-degenerate quadric Q and the same intersection numbers with respect to hyperplanes as Q. Quasi-quadrics were introduced in 2000 by De Clerck-Hamilton-O'Keefe-P, building on work of Tonchev 1993, which, in turn used work of Dillon-Shatz 1987 and Kantor 1983. Note that these are **two-intersection sets**, and so related to **strongly regular graphs** and to **two-weight error-correcting codes**, by work of Delsarte in several papers in the 1970's.

Theorem (Tonchev 1993/Kantor 1983/Dillon 1974)

To each quasi-quadric of $\mathrm{PG}(2m-1,2)$, *there corresponds a bent function* $GF(2)^{2m} \to GF(2)$, *and conversely.*

Many constructions of quasi-quadrics were given in the paper that introduced them. There is also a connection between quasi-quadrics of $\mathrm{PG}(2m-1,2)$ and **symmetric designs with the symmetric difference property** (that the symmetric difference of any three blocks is either a block or the complement of a block). Kantor showed in 1983 that such designs have parameters $(2^{2m}, 2^{2m-1}+2^{m-1}, 2^{2m-2}+2^{m-1})$ that *the number of isomorphism classes of such designs grows exponentially with* m.

A class of bent functions introduced in John Dillon's Ph. D. thesis in 1974 was extended by Carlet and Mesnager in 2011 and the extended class called *Niho* bent functions. We give them in **bivariate form**. Let $n = 2m$. Identifying $GF(2)^n$ with $GF(2^m)^2$, a (normalised) **Niho bent function** is a bent function of the form $Tr_m(xG(y/x))$, where $G: GF(2^m) \to GF(2^m)$ with $G(0) = 0$ and $G(1) = 1$.

In the same paper, Carlet and Mesnager proved that $Tr_m(xG(y/x))$ is a bent function if and only if $\{(1, x, G(x)) : x \in GF(2^m)\} \cup \{(0,1,0),(0,0,1)\}$ is a **hyperoval** of $\mathrm{PG}(2, 2^m)$ (a set of $2^m + 2$ points, no three collinear). A function $G: GF(2^m) \to GF(2^m)$ with $G(0) = 0$ and $G(1) = 1$ and such that $\{(1, x, G(x)) : x \in GF(2^m)\} \cup \{(0,1,0),(0,0,1)\}$ is a hyperoval of $\mathrm{PG}(2, 2^m)$ is called an **o-polynomial**.

Theorem (Carlet-Mesnager 2011)

Niho bent functions define o-polynomials and, conversely, every o-polynomial defines a Niho bent function.

Bentness is preserved by extended-affine (EA) equivalence. Two Boolean functions f and g are called **EA-equivalent** if there exists an affine automorphism A and an affine Boolean function ℓ such that $f = g \circ A + \ell$. Two hyperovals of $\mathrm{PG}(2, 2^m)$ are **projectively equivalent** if they are in the same orbit of the automorphism group $P\Gamma L(3, 2^m)$ of $\mathrm{PG}(2, 2^m)$.

Carlet and Mesnager 2011 also discovered that projectively equivalent hyperovals can lead to EA-inequivalent Niho bent functions.

So the two concepts of equivalence don't match.

Here are (up to projective equivalence of hyperovals) the known o-polynomials over $GF(2^m)$.

1. $F(z) = z^{2^i}$ with $\gcd(i,m) = 1$ [Segre (1957)].
2. $F(z) = z^6$ with m odd [Segre (1962),Segre-Bartocci (1971)].
3. $F(z) = z^{3\cdot 2^k+4}$ with $m = 2k-1$ [Glynn (1983)].
4. $F(z) = z^{2^k+2^{2k}}$ with $m = 4k-1$ [Glynn (1983)].
5. $F(z) = z^{2^{2k+1}+2^{3k+1}}$ with $m = 4k+1$ [Glynn (1983)].
6. $F(z) = z^{2^k} + z^{2^k+2} + z^{3\cdot 2^k+4}$ with $m = 2k-1$ [Cherowitzo (1998)].
7. $F(z) = z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$ with m odd [Payne(1985)].
8. $F(z) = \frac{d^2(z^4+z)+d^2(1+d+d^2)(z^3+z^2)}{z^4+d^2z^2+1} + z^{1/2}$, where $Tr_m(d) = 1, d^2+d+1 \neq 0$ [Cherowitzo-P-Pinneri-Royle (1996) *Subiaco* **plus a slight variant** for $m = 2 \pmod 4$].
9. $F(z) =$ *even more complicated*, m even [Cherowitzo-O'Keefe-P (2003), *Adelaide*].
10. $F(z) = z^4 + w^{11}z^6 + w^{20}z^8 + w^{11}z^{10} + w^6z^{12} + w^{11}z^{14} + z^{16} + w^{11}z^{18} + w^{20}z^{20} + w^{11}z^{22} + w^6z^{24} + w^{11}z^{26} + z^{28}$, where $w^5 = w^2+1, m = 5$ [O'Keefe-P (1991)].

An *o-permutation* is a non-zero scalar multiple of an o-polynomial. An *oval* of $\mathrm{PG}(2,2^m)$ is a set of 2^m+1 points, no three collinear.
In 2002 O' Keefe and P introduced an action of $P\Gamma L(2,2^m)$ on the vector space V of functions with domain and codomain $GF(2^m)$ we called the *magic action*. The magic action was shown to take o-permutations to o-permutations. The focus of that paper on certain sets of ovals called herds (and the corresponding generalised quadrangles) led to the emphasis on o-permutations rather than on o-polynomials. We hereby introduce a slight modification of the magic action that takes o-polynomials to o-polynomials. It is most easily specified by giving generators:

$\phi\colon f \mapsto \phi f : x \mapsto xf(x^{-1})$;
$\rho_\gamma\colon f \mapsto \rho_\gamma f : x \mapsto \gamma \circ f \circ \gamma^{-1}$, for $\gamma \in Aut(GF(2^m))$;
$\sigma_a\colon f \mapsto \sigma_a f : x \mapsto \frac{f(ax)}{f(a)}$, for $a \in GF(2^m)^*$;
$\tau_c\colon f \mapsto \tau_c f : x \mapsto \frac{f(x+c)+f(c)}{f(1+c)+f(c)}$, for $c \in GF(2^m)$.

Since the only alterations to the maps are to multiply σ_a and τ_c by appropriate constants, the two actions are identical on the projective space $\mathcal{P}V$ and since the new maps preserve the property $f(1) = 1$, we have:

Theorem (BCHKP)

The modified magic action is an action of $P\Gamma L(2, 2^m)$ which takes o-polynomials to o-polynomials.

In that same paper of O'Keefe-P, an equivalence of o-permutations under the magic action is shown to be induced by an explicit collineation taking the corresponding hyperovals to one another and fixing $(0, 0, 1)$ (and hence taking the ovals obtained by deleting (0,0,1) to one another). By following this collineation by an appropriately chosen homology with centre $(0, 0, 1)$ and axis $z = 0$, it follows that an equivalence of o-polynomials under the modified magic action is induced by an explicit collineation taking the corresponding hyperovals to one another and fixing $(0, 0, 1)$.

Thus the magic action (and the modified magic action) transfer *oval* equivalence to o-permutation equivalence (and o-polynomial equivalence). We now extend the modified magic action in order to transfer *hyperoval* equivalence to o-polynomial equivalence.
Let G be the group generated by

$$\{\phi, \rho_\gamma, \sigma_a, \tau_c : \gamma \in Aut(GF(2^m)), a \in GF(2^m)^*, c \in GF(2^m)\}$$

and the inversion map $f \mapsto f^{-1}$. Suppose f and g are o-polynomials in the same orbit under G. Then since the generators of G take hyperovals arising from o-polynomials to equivalent hyperovals arising from the image o-polynomials, the hyperovals arising from f and g are equivalent. Conversely, if the hyperovals H arising from f and H' arising from g are equivalent via a collineation, then consider the preimage of $(0,0,1)$ under that collineation. If it is $(0,0,1)$, then by Theorem 4 of O'Keefe-P 2002 and its slight modification above, f and g are in the same orbit of G.

If the preimage of $(0,0,1)$ is $(0,1,0)$ then apply inversion to H to obtain a hyperoval H'' equivalent to H' where the preimage of $(0,0,1)$ is $(0,0,1)$ and apply the above argument again: f and g are in the same orbit of G. If the preimage of $(0,0,1)$ is $(1,t,f(t))$, then choose an element of $P\Gamma L(2,2^m)$ taking $(1,t)$ to $(0,1)$, and apply this element via the modified magic action to f to obtain a hyperoval H''' equivalent to H' where the preimage of $(0,0,1)$ under the new collineation is $(0,1,0)$ and apply the immediately preceding argument: f and g are in the same orbit of G.

Theorem (o-polynomial equivalence and hyperoval equivalence)

Two o-polynomials f and f' arise from equivalent hyperovals of $\mathrm{PG}(2,2^m)$ if and only if they lie in the same orbit of the group generated by

$$\{\phi, \rho_\gamma, \sigma_a, \tau_c : \gamma \in Aut(GF(2^m)), a \in GF(2^m)^*, c \in GF(2^m)\}$$

and the inversion map $f \mapsto f^{-1}$.

The corresponding concepts for Niho bent functions are called **restricted o-equivalence** (for the modified magic action) and **o-equivalence** (for the extended modified magic action).

A **spread** of a vector space of dimension $2m$ is a collection of subspaces of dimension m that pairwise meet in the zero vector and whose union is the whole vector space. Given a spread, the incidence structure with points the vectors of the vector spaces and with line the additive cosets of the elements of the spread is an affine plane.

A spread is **Desarguesian** is the affine plane arising from it is Desarguesian. In order to admit affine maps, we move to the projective perspective, and view the spread in the hyperplane at infinity. Affine maps take spreads to spreads, and Desarguesian spreads to Desarguesian spreads.

A necessary and sufficient condition for a bent function f to be Niho is that there exists a Desarguesian spread such that the restriction of f to each element of the spread is linear (Carlet-Mesnager (2011),p. 2398.) (In the definition of Niho bent functions the spread is $\{\{(x, ax) : x \in GF(2^m)\} : a \in GF(2^m)\} \cup \{\{(0, y) : y \in GF(2^m)\}$.)

So the question arises: *For a Niho bent function, is the associated Desarguesian spread fixed by the group of the bent function?* As is often the case in finite geometry, the classical case behaves differently.

The stabiliser of the Niho bent function arising from the conic $\{(1,x,x^{1/2})) : x \in GF(2^m)\} \cup \{(0,1,0)\}$ does not fix the associated Desarguesian spread. It turns out that the support of the Niho bent function is the complement in $\mathrm{PG}(2m-1,2)$ of the hyperbolic quadric $Tr_m(xy) = 0$. Such Niho bent functions form a single EA-equivalence class $\mathcal{C}$, for $PGL(2m,2)$ is transitive on hyperbolic quadrics. We will need to isolate this case via a characterisation in turn of symmetry. We also need the observation that the union of an elliptic quadric in $\mathrm{PG}(2m-1,2)$ with the origin is the support of a bent function, and that bent function also lies in $\mathcal{C}$.

Theorem

A Niho bent function $GF(2)^{2m} \to GF(2)$ with stabiliser in $GL(2m,2)$ containing $\Omega^{\pm}(2b,2^a)$, for some a,b with $m = ab$ and $b > 1$ arises from a conic.

Proof: There's only one $\Omega^{\pm}(2b,2^a)$-invariant set of the right size to be the support of a bent function; since $\Omega^{\pm}(2b,2^a) \leq \Omega^{\pm}(2m,2)$, it arises from a conic.

Theorem

A Niho type bent function that does not arise from a conic has an associated Desarguesian spread fixed by its stabiliser.

Proof: Suppose not. It was shown by Carlet-Mesnager (2001), 3.1.2 that there are elements of the extended affine equivalence group, inducing a subgroup H of $AGL(2m,2)$ isomorphic to $P\Gamma L(2,2^m)$, which induces equivalence of ovals (that is, the modified, but not extended, magic action) in its action on Niho bent functions. H stabilises a Desarguesian spread Σ in the hyperplane at infinity which is associated to each corresponding Niho bent function. Let O be an orbit of (cosets of the set A of affine functions with representatives) Niho bent functions under H and let G_1 be the group induced on the hyperplane at infinity by the subgroup G of $AGL(2m,2)$ induced by the stabiliser of O in the extended affine equivalence group. Let $f+A \in O$. G_1 is a proper overgroup of $P\Gamma L(2,2^m)$ in $GL(2m,2)$. The main theorem of Guralnick-P-Praeger-Saxl 1999 lists all possibilities for G_1. We also know that O has size dividing $|P\Gamma L(2,2^m)|$ and so the stabiliser S of f in the extended affine equivalence group has size divisible by $|G_1|/|P\Gamma L(2,2^m)|$.

Applying the main theorem of Guralnick-P-Praeger-Saxl 1999 again, this time to the group K induced by S on the hyperplane at infinity, eventually reduces to the cases where $PSp(2b, 2^a) \triangleleft G_1$, $\Omega^{\pm}(2b, 2^a) \triangleleft K$, where $m = ab, b > 1$. (The two cases correspond to whether or not the support of f contains the origin or not.) The preceding theorem applied to f shows that the oval is a conic. *Unfortunately, this proof depends on the classification of finite simple groups.*

Corollary

Given two Niho bent functions in bivariate form not arising from a conic, the affine map in any EA-equivalence between them is in $A\Gamma L(2, 2^m)$.

Proof: The affine map is an automorphism of the affine plane $AG(2, 2^m)$ arising from the (common) Desarguesian spread. Hence it is in $A\Gamma L(2, 2^m)$, by the fundamental theorem of affine geometry.

We also need to remark that, for $m > 2$, the Niho bent functions $Tr_m(xy)$ and $Tr_m(x^2 y^{2^m-2})$ are inequivalent, in order to deal with Niho bent functions arising from a regular hyperoval.

Main theorem

Theorem

Given two Niho bent functions, they are EA-equivalent if and only if the corresponding **ovals** *are projectively equivalent. Hence, the number of EA-equivalence classes of Niho bent functions arising from a hyperoval of* $\mathrm{PG}(2,2^m)$ *is the number of orbits of the collineation stabiliser of the hyperoval on the points of the hyperoval.*

Proof: Suppose that two ovals arising from Niho bent functions not arising from a conic are projectively equivalent. Let f, g be their o-polynomials. Then, by Theorem 4 of O'Keefe-P 2002, there is an element of $P\Gamma L(2,2^m)$ such that, under the magic action, it takes f to g. This gives an EA-equivalence between the Niho bent functions. Conversely, by the preceding Corollary, an EA-equivalence between the Niho bent functions gives an element of $P\Gamma L(2,2^m)$ taking the first o-polynomial to the second in the (modified) magic action. Hence, by Theorem 4 of O'Keefe-P 2002, the ovals are projectively equivalent.

Known Niho bent functions

By combining the results of the survey article O'Keefe-P 1994 with:
Gevaert-Payne-Thas 1988,
O'Keefe-P 1991,
Payne-P-Pinneri 1995,
O'Keefe-Thas 1996,
Payne-Thas 2005,
Bayens-Cherowitzo-P 2007/8,
the groups of the known hyperovals in finite Desarguesian planes are known. From each of the groups' orbits on points of the hyperoval, *the projective equivalence classes of known ovals in finite Desarguesian planes are known*.

In principle, this allows us to give *explicit bent functions for all the known Niho bent functions*.

Related structures

1. Difference sets; symmetric designs with a regular elementary abelian 2-group; Strongly regular graphs.
2. Walsh transforms taking two values; Hadamard matrices.
3. Signal sets with minimal simultaneous cross correlation and autocorrelation magnitudes; Signalling applications.
4. Meets upper bound of nonlinearity from covering radius bound for Reed-Muller code; Cryptographic applications.
5. Perfect non-linear functions; Cryptographic applications.
6. Quasi-quadrics; Two-intersection sets; Two weight codes; Uniformly packed codes (Goethals-van Tilborg; Mesnager).
7. Symmetric and quasi-symmetric designs with the symmetric difference property (Jungnickel, Tonchev for the quasi-symmetric designs).
8. Hyperovals; Doubly dual dimensional dual hyperovals (Dempwolff).
9. Generalised quadrangles (Tits; Ahrens-Szekeres; Hall; Payne).
10. Partial geometries (Wallis;Thas); Howell designs (Anderson).
11. Semibent functions (Carlet, Mesnager); Vectorial bent functions (Mesnager); Constant weight codes (Mesnager); S-boxes (Mesnager).

Quotes

"We have obtained a large number of potentially new bent functions (more precisely, infinite classes of bent functions, since their numbers of variables range over infinite sets) whose bivariate expressions are explicit, after noticing that the condition for a function to be in this class is equivalent to the fact that a polynomial directly related to its definition is an o-polynomial (a notion from finite geometry), and thanks to an abundant literature on these polynomials. "

Claude Carlet, Sihem Mesnager 2011

"Theorem 1 provides several new classes of infinite (optimal) bent vectorial functions thanks to the hard work of the geometers over approximately 40 years."

Sihem Mesnager 2014

An e-error-correcting code C in $GF(q)^n$ is said to be **uniformly packed** with parameters λ and μ if for $x \in GF(q)^n$ we have
(1) if $d(x, C) = e$ then $B(x, e+1) = \lambda$, and
(2) if $d(x, C) = e+1$ then $B(x, e+1) = \mu$, where
$\lambda < (n-e)(q-1)/(e+1)$.
(The last inequality just says that the code is not perfect, and $B(x, i)$ is the number of codewords at distance i from x.) By a theorem of Goethals and van Tilborg, an e-error correcting code is uniformly packed if and only if its dual code has exactly $e+1$ weights.

Let n and s be integers where $n \leq s \leq 2n-1$. A square of side s such that each cell is empty or contains an unordered pair of integers from amongst $1, 2, \ldots, 2n$ is called a **Howell design** of type $H(s, 2n)$, provided:
(1) each integer from 1 to 2n appears exactly once in each row and each column and
(2) every unordered pair of integers appears at most once in a cell of the square. The range of possible values of s is $n \leq s \leq 2n-1$.