Nonlinear Functions — A topic in Designs, Codes and Cryptography

Alexander Pott

Otto-von-Guericke-Universität Magdeburg

September 21, 2007

Content

- Designs and their groups.
- Planar (or perfect nonlinear) functions and projective planes.
- Almost perfect nonlinear functions (APN).
  - Semi-Biplanes
  - Crooked functions
  - Bent functions
  - Codes

Goal: Connection between APN's and designs.

What is a design $\mathcal{D}$

- point set $\mathcal{P}$, block set $\mathcal{B}$
- incidence relation $I \subseteq \mathcal{P} \times \mathcal{B}$.
- **Description** using incidence matrix $\mathbf{M}(\mathcal{D})$.
  - rows indexed by points p
  - columns indexed by blocks B
  - (p, B)-entry is 1 if $(p, B) \in I$, otherwise 0.

Assumption: All rows and columns are different.

Examples of incidence matrices / Designs

0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
1	0	1	1	0	1	0	0	0	1	0	0	0	1	0	0
1	1	0	1	0	0	1	0	0	0	1	0	0	0	1	0
1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1
1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0
0	1	0	0	1	0	1	1	0	1	0	0	0	1	0	0
0	0	1	0	1	1	0	1	0	0	1	0	0	0	1	0
0	0	0	1	1	1	1	0	0	0	0	1	0	0	0	1
1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0
0	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0
0	0	1	0	0	0	1	0	1	1	0	1	0	0	1	0
0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1
1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1
0	1	0	0	0	1	0	0	0	1	0	0	1	0	1	1
0	0	1	0	0	0	1	0	0	0	1	0	1	1	0	1
0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0

16 points and 16 blocks, blocksize 6, any two different points are joined by precisely 2 blocks ... and vice versa.

Examples of incidence matrices / Designs

1	1	1	1	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	1	1	1	0	0	0
1	0	0	0	0	0	0	0	0	0	1	1	1
0	1	0	0	1	0	0	0	1	1	0	0	0
0	1	0	0	0	1	0	1	0	1	0	0	0
0	1	0	0	0	0	1	1	1	0	0	0	0
0	0	1	0	0	0	0	1	0	0	0	1	1
0	0	1	0	0	0	0	0	1	0	1	0	1
0	0	1	0	0	0	0	0	0	1	0	1	1
0	0	0	1	0	1	1	0	0	0	1	0	0
0	0	0	1	1	0	1	0	0	0	0	1	0
0	0	0	1	1	1	0	0	0	0	0	0	1

13 points and 13 blocks, blocksize 4, any two different points are joined by precisely 1 block ... and vice versa.

Iso-/Automorphisms

$\mathcal{D}$ and $\mathcal{D}'$ are isomorphic if and only if there is an incidence preserving map between the point sets of $\mathcal{D}$ and $\mathcal{D}'$.

In matrix terms:

$$\mathbf{M}' = \mathbf{P} \cdot \mathbf{M} \cdot \mathbf{Q}$$

for permutation matrices **P**, **Q**.

Automorphisms, Automorphism group

Invariants for isomorphic designs

Problem: Distinguish non-isomorphic designs!

- Rank of incidence matrix.
- Smith Normal Form of incidence matrix (Q. XIANG).
- Automorphism groups.
- intersection patterns (triple intersection numbers).

Regular automorphism groups

In our examples: There is an automorphism group acting regularly on points and blocks: regular: For two points p, q, there is precisely one $g \in G$ such that $g(p) = q$.

- Points can be identified with group elements, after fixing some base point.
- Blocks are subsets of G. Let D be the set of points corresponding to some base block.
- Two points g and h are joined by λ blocks if and only if $g - h$ has λ representations $g - h = d - d'$ with $d, d' \in D$.

Regular automorphism groups II

- All information about the design is stored in D.
- The design can be reconstructed from D:
  - point set G.
  - blocks: $D + g := \{d + g \ : \ d \in D\}$

  development of D.
- difference representations = joining numbers.
- Construction method for designs.

Example

0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0
1	0	1	1	0	1	0	0	0	1	0	0	0	1	0	0
1	1	0	1	0	0	1	0	0	0	1	0	0	0	1	0
1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1
1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	0
0	1	0	0	1	0	1	1	0	1	0	0	0	1	0	0
0	0	1	0	1	1	0	1	0	0	1	0	0	0	1	0
0	0	0	1	1	1	1	0	0	0	0	1	0	0	0	1
1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0
0	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0
0	0	1	0	0	0	1	0	1	1	0	1	0	0	1	0
0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1
1	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1
0	1	0	0	0	1	0	0	0	1	0	0	1	0	1	1
0	0	1	0	0	0	1	0	0	0	1	0	1	1	0	1
0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0

$$D = \left\{ \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\end{pmatrix} \right\} \subset \mathbb{F}_2^4$$

Relative difference sets

$G = H \times N$ splitting abelian group.

- $|N| = n, \quad |G| = m \cdot n$
- $D \subseteq G, |D| = m$
- $\{* \, d - d' \mid d, d' \in D, d \neq d' \, *\} = \frac{m}{n}(G \setminus N)$.

$(m, n, m, \frac{m}{n})$ relative difference set.

Constructions from designs (projective planes!) with regular automorphism group.

D also defines a function $f : H \to N$, and vice versa any function defines a set (graph of f)

$$D(f) := \{(x, f(x)) \; : \; x \in H\} \subset H \times N$$

Example

- $|N| = 2$: classical bent functions.
- $\{(0,0),(1,1),(2,1)\}$ is a $(3,3,3,1)$ relative difference set.

Bent functions

$f : H \to N$ bent function or perfect nonlinear if

$$|\{x \in H \ : \ f(x+a) - f(x) = b\}|$$

is $|H|/|N|$ for all $a \neq 0$.

$f : H \to N$ bent if and only if

$$D(f) := \{(x, f(x)) \ : \ x \in H\} \subset H \times N$$

is a relative difference set.

Bent functions correspond to designs!

Equivalence of functions

Let $f, f' : H \to N$, $\quad D(f) = \{(x, f(x)) \ : \ x \in H\}$
equivalent if there is $\varphi \in \mathrm{Aut}(H \times N)$ such that

$$\varphi(D(f)) = D(f') + (a, b).$$

$\varphi(N) = N$: affine equivalence. Necessary if f bent!

f, f' equivalent $\quad \Rightarrow \quad$ developments of $D(f)$ and $D(f')$ are isomorphic, but <u>not</u> vice versa

Projective planes

A **projective plane** is an incidence structure where

- $\sharp$ points = $\sharp$ blocks
- Any two different points are on a unique line (block).
- Constant line size $n+1$.
- There is a quadrangle (to avoid trivial cases).

Remarks:

- n: order.
- n^2+n+1: $\sharp$ points.
- $n+1$ lines through any point.

Example

development of $D=\{1,2,4\} \subset \mathbb{Z}_7$ describes a projective plane of order 2.

“Classical” constructions for all prime powers n.

Residual planes / nets

Π projective plane, (p, L) incident point-line pair. Delete all lines through p and all points on L.

- Residual incidence structure contains n^2 points and lines.
- Point set can be partitioned uniquely into point classes of points not joined.
- Residual design (net) may have an automorphism group $H \times N$ acting regular on points and lines.
- Difference set description via $(n, n, n, 1)$ relative difference set.
- Bent functions $\mathbb{F}_n \to \mathbb{F}_n$ (n odd prime power).
- Impossible if n even.

(Bent) functions corresponding to planes: planar functions

Examples $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$

f: planar functions (PN perfect nonlinear)

Power PN mappings

function	conditions	Proved in
x^2	none	trivial
$x^{\frac{p^k+1}{2}}$	$p = 3$, $\gcd(n,k) = 1$, k is odd	COULTER, MATTHEWS (1997) HELLESETH, MARTINSEN (1997)
x^{p^k+1}	$n/\gcd(n,k)$ is odd	DEMBOWSKI, OSTROM (1968)

Difference set $\{(x, x^2) : x \in \mathbb{F}_q\}$ describes the classical planes.

function	conditions	Proved in
$x^{10} - x^6 - x^2$	$p = 3$, n odd	DING, YUAN (2006)
$x^{10} + x^6 - x^2$	$p = 3$, n odd	COULTER, MATTHEWS (1997)

Dembowski-Ostrom polynomials $\mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$

$$f(x) = \sum_{i,j} a_{i,j} x^{p^i + p^j} \quad \text{in} \quad \mathbb{F}_{p^n}[x]$$

- $f(x+a) - f(x) - f(a)$ is linear if and only if f is Dembowski-Ostrom.
- If f planar Dembowski-Ostrom polynomial, then p odd and

  $$L_a := \{(x, f(x+a) - f(x) - f(a)\}$$

  are p^n disjoint subspaces in $\mathbb{F}_p^{2n}$ of dimension n.
- Cosets of L_a's form a (residual) projective plane $T(f)$ (translation plane).
- The two planes $T(f)$ and $D(f)$ are isomorphic!
- Translation plane + planar function = commutative semifield plane.
- commutative semifield plane: f must be Dembowski-Ostrom (Pierce, Kallaher (2005)).

More examples, but no "easy" description (Dickson semifields)

New results and problems on planar functions

- Some more (new) sporadic examples (Gaobing Weng)
- Infinite family of binomials (Helleseth, Kyureghyan, Ness, Pott (2007).
- Constructions of Hadamard matrices / Paley type difference sets (Ding, Yuan (2006))
- Find more!
- Characterize monomial x^d or binomial $x^{d_1} + \alpha x^{d_2}$ planar functions!

Planar functions or bent functions on $\mathbb{F}_{2^n}$?

No planar functions $H \to N$ if $|H| = |N|$ is even SCHMIDT (2000), NYBERG (1994).

More generally: No relative difference sets / bent functions with parameters

$$(2^n, 2^m, 2^n, 2^{n-m})$$

if $2m > n$.

Almost perfect nonlinear functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Optimal case for $n = m$:

$$|\{x \ : \ f(x+a) + f(x) = b\}| \in \{0, 2\}$$

for all $a \neq 0$ (almost perfect nonlinear).

- Incidence structure corresponding to the development of

  $$D(f) = \{(x, f(x)) \ : \ x \in \mathbb{F}_{2^n}\}$$

  is a semi-biplane: Two different points are on 0 or 2 lines.
- Relation “joined” defines a graph!
- There is a design behind an APN function.
- Characterization of those semi-biplanes which correspond to APN functions, GÖLOĞLU, POTT (2007).

Power APN's $f(x) = x^d$, $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$

	d	Condition
GOLD	$2^i + 1$	$\gcd(i, n) = 1$
KASAMI	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
WELCH	$2^t + 3$	$n = 2t + 1$
NIHO	$2^t + 2^{\frac{t}{2}} - 1$, t gerade $2^t + 2^{\frac{3t+1}{2}} - 1$, t ungerade	$n = 2t + 1$
inverse	$2^{2t} - 1$	$n = 2t + 1$
DOBBERTIN	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

GOLD: Quadratic or Dembowski-Ostrom: $f(x + a) - f(x) - f(a)$ is linear.

On the equivalence of APN's

- f and f' are CCZ-equivalent if there is an automorphism φ of $\mathbb{F}_2^{2n}$ such that $\varphi(D(f)) = D(f') + (a,b)$. (CCZ = CARLET, CHARPIN, ZINOVIEV (1998))
- CCZ automorphism group (or multiplier group):
$$\{\varphi \ : \ \varphi(D(f)) = D(f) + (a,b)\}.$$
- f and f' are affine equivalent if $\varphi(D(f)) = D(f') + (a,b)$ and $\varphi(N) = N$.
- affine group: $\{\varphi : \varphi(D(f)) = D(f) + (a,b),\ \varphi(N) = N\}$
- If f is bijective, we may interchange H and N (Subcase of CCZ equivalence).

Results, Problems, Questions I

- CCZ is "strictly" more general than affine equivalence BUDAGHYAN, CARLET, POTT (2005).
- The known APN functions are affine inequivalent.
- There are a lot more CCZ inequivalent quadratic APN polynomials BUDAGHYAN, CARLET, DILLON, EDEL, FELKE, KYUREGHYAN, LEANDER, POTT.
- The GOLD and KASAMI APN functions are CCZ inequivalent BUDAGHYAN, CARLET, FELKE, LEANDER.
- The newly constructed APN's are CCZ inequivalent to GOLD and KASAMI.
- CCZ groups?
- GOLD: affine automorphism group = CCZ group? (true in small cases $n > 3$, EDEL).
- non GOLD: affine equivalence = CCZ equivalence? (true in small cases, EDEL).
- CCZ equivalence does not preserve the size of the affine group.

Results, Problems, Questions II

- Not much is known about the non-isomorphism of the corresponding semi-biplanes!
- “CCZ Equivalence” implies “Isomorphism of semi-biplanes”. Converse? I believe NO.
- Automorphism groups of semi-biplanes?
- Find new invariants and/or compute the known invariants.
- Using ranks of incidence matrices, EDEL, KYUREGHYAN and POTT (2005) have shown that the semi-biplanes of small examples are non isomorphic (different approach than BCFL which show “only” inequivalence).

Crooked functions

$f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is crooked if

$$\{f(x+a) - f(x) - f(a) \ : \ x \in (\mathbb{F}_2)^n\}$$

is a subspace of dimension $n-1$ for all $a \neq 0$.

Examples: Quadratic functions (Dembowski-Ostrom).

Main Problem: Nonquadratic crooked functions? NO for monomials and binomials, BIERBRAUER, KYUREGHYAN (2007).

Problems and results on crooked functions

- Formulation of "crooked" such that it is invariant under CCZ equivalence, GÖLOĞLU, POTT (2007).
- Crooked is the analogue of translation plane + planar function (commutative semifield).
- All recently constructed APN's are crooked.
- Does the number of inequivalent crooked functions grow exponentially?

Almost perfect nonlinear and bent functions $f : H \rightarrow N$

Bent: $|\{x \ : \ f(x+a) - f(x) = b\}| = const.$

Let $H = N = \mathbb{F}_2^n$, $f : H \rightarrow N$ arbitrary, and $U \leq \mathbb{F}_2^n$.

$$f_U := H \rightarrow N/U, \quad x \mapsto f(x) + N$$

Question: Is it possible that f_U is bent, in particular if f is APN?

Necessary condition: n even, $|U| \geq 2^{n/2}$.

If $\dim(U) = n - 1$, then f_U is classical bent function.

Observations, Results, Questions

- If $\dim(U) = n - 1$, projections may be described by trace function. This is not true if $\dim(U)$ is smaller.
- Start with power (APN) mappings.
- In some small cases, GOLD and KASAMI exponents yield bent functions $(\mathbb{F}_2)^n \to (\mathbb{F}_2)^{n/2}$, POTT.
- Bent functions using other power mappings? Problem: There are many, many subspaces U!
- There are investigations if $\dim(U) = n - 1$ DILLON, DOBBERTIN (2004), LANGEVIN, LEANDER, CHARPIN, KYUREGHYAN

APN and Codes

Consider the code with the $(2n+1) \times 2^n$ parity check matrix

$$\begin{pmatrix} 1 & \cdots & \cdots & 1 \\ 0 & \cdots & x & \cdots \\ 0 & \cdots & f(x) & \cdots \end{pmatrix}$$

Rank $2m+1$: the kernel of **H** is a $[2^n, 2^n - 2n + 1, d]_2$ code.

Theorem (Dodunekov, Zinoviev 1987; Brouwer, Tolhuizen 1993)

Minimum distance ≤ 6. Equality if and only if f is APN.

Code and CCZ equivalence

Consider code with generator matrix

$$\begin{pmatrix} 1 & \cdots & \cdots & 1 \\ 0 & \cdots & x & \cdots \\ 0 & \cdots & f(x) & \cdots \end{pmatrix}$$

- CCZ equivalence is code equivalence.
- CCZ equivalence is more than affine equivalence if the code contains more than just one Simplex code!
- If f is bijective, there are (trivially) two Simplex codes!
- CCZ group is automorphism group of the code!

Conclusion

- Problems on planar functions.
- Problems on APN functions.
- Similarities between both cases from a design theoretic (geometric) perspective.
- Relevance of the designs?