Seminar
Planar functions versus bent functions

Enes Pasalic

Rogla, May 18, 2014

Planar functions versus bent functions - outline

- Introduction to Boolean and bent functions
- Correspondence to Cayley graphs
- Planar functions and relations to bent functions
- Finding nonquadratic planar mappings (some ideas)
- Final comments

Short introduction to (vectorial) Boolean functions

- Mathematical notation : $f : GF(2)^n \rightarrow GF(2)^m$ (Boolean if $m = 1$)
- Denote the set of Boolean respectively vectorial Boolean functions by $\mathfrak{B}_n$ and $\mathfrak{B}_n^m$.
- Finding optimal functions is elusive - the space is 2^{m2^n} !

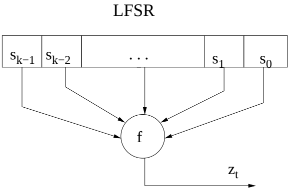
Short introduction to (vectorial) Boolean functions

- Mathematical notation : $f : GF(2)^n \to GF(2)^m$ (Boolean if $m = 1$)
- Denote the set of Boolean respectively vectorial Boolean functions by $\mathfrak{B}_n$ and $\mathfrak{B}_n^m$.
- Finding optimal functions is elusive - the space is 2^{m2^n} !
- Associate the mapping with a polynomial in a Boolean ring and define ANF of $f \in \mathfrak{B}_n$ e.g.

$$f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4,$$

where $f : GF(2)^4 \to GF(2)$, and f is bent in the sense defined pretty soon.

Some applications in cryptography



Nonlinear filtering generator

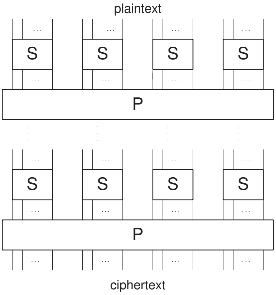


Figure : SP network using S-boxes - a block cipher

- S is nonlinear permutation substitution (S-box for **confusion**) and P is a linear permutation (**diffusion**):

$$S : \mathbb{F}_2^n \to \mathbb{F}_2^n \quad P : \mathbb{F}_2^t \to \mathbb{F}_2^t \quad t = rn; r \in \mathbb{N}.$$

Boolean functions - truth table and ANF

x_1	x_2	x_3	$f(x)$	$g(x)$
0	0	0	0	$*$
0	0	1	0	$*$
0	1	0	0	$*$
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	0	$*$
1	1	1	1	0

- The ANF (algebraic normal form) is $f(x) = x_1x_2 \oplus x_2x_3 \oplus x_3$ (**unique**). The degree is $\deg(f) = 2$, the maximum length of the terms in ANF.

Boolean functions - truth table and ANF

x_1	x_2	x_3	$f(x)$	$g(x)$
0	0	0	0	$*$
0	0	1	0	$*$
0	1	0	0	$*$
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	0	$*$
1	1	1	1	0

- The ANF (algebraic normal form) is $f(x) = x_1x_2 \oplus x_2x_3 \oplus x_3$ (**unique**). The degree is $\deg(f) = 2$, the maximum length of the terms in ANF.
- Cayley graph: Define the support of f - $S_f = \{x \in \mathbb{F}_2^n : f(x) = 1\}$
- Set of vertices $V_n = \mathbb{F}_2^n = GF(2)^n$ and set of edges

$$E_f = \{(u, w) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid f(\mathbf{u} \oplus \mathbf{w}) = 1\}.$$

- Any $\Gamma_f = (V_n, E_f)$ is $|S_f|$- regular (elementary additive Abelian group)

Bent functions - as a special class

- Favourite combinatorial objects (difference sets, coding ...).
- Fix a basis of $GF(2^n)$ to get isomorphism $GF(2^n) \cong GF(2)^n$ and define for $f : GF(2^n) \to GF(2)$, **Walsh transform**

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a \cdot x},$$

for $a \in \mathbb{F}_{2^n}$. If $|W_f(a)| = 2^{n/2}$ for all $a \in GF(2^n)$ then f is **bent**.

Bent functions - as a special class

- Favourite combinatorial objects (difference sets, coding ...).
- Fix a basis of $GF(2^n)$ to get isomorphism $GF(2^n) \cong GF(2)^n$ and define for $f : GF(2^n) \to GF(2)$, **Walsh transform**

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr(ax)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a \cdot x},$$

for $a \in \mathbb{F}_{2^n}$. If $|W_f(a)| = 2^{n/2}$ for all $a \in GF(2^n)$ then f is **bent**.

- Maximum distance (uniform) to affine functions $a \cdot x$, n even !!
- **Parseval's equality** : $\sum_{a \in \mathbb{F}_2^n} W_f(a)^2 = 2^{2n}$, for any $f \in \mathfrak{B}_n$!
- So what (as Miles Davis would put it) ?

Graph theoretic aspects

- Well, Γ_f is **strongly regular** with parameters (V_n, S_f, e, d) where :

  e : the number of vertices adjacent to both u and v if u, v are adjacent, **for all** $u, v \in V$

  d : the number of vertices adjacent to both u and v if u, v are nonadjacent, **for all** $u, v \in V$

Graph theoretic aspects

- Well, Γ_f is **strongly regular** with parameters (V_n, S_f, e, d) where :

  e : the number of vertices adjacent to both u and v if u, v are adjacent, **for all** $u, v \in V$

  d : the number of vertices adjacent to both u and v if u, v are nonadjacent, **for all** $u, v \in V$

- Furthermore, $f \in \mathfrak{B}_n$ is bent **IFF** $e = d$!

- For a bent function $f(x_1, \ldots, x_4) = x_1x_2 \oplus x_3x_4$, we have $|S_f| = 6$ (valency is 6) and $e = d = 2$!

Graph theoretic aspects

- Well, Γ_f is **strongly regular** with parameters (V_n, S_f, e, d) where :

  e : the number of vertices adjacent to both u and v if u, v are adjacent, **for all** $u, v \in V$

  d : the number of vertices adjacent to both u and v if u, v are nonadjacent, **for all** $u, v \in V$

- Furthermore, $f \in \mathfrak{B}_n$ is bent **IFF** $e = d$!

- For a bent function $f(x_1, \ldots, x_4) = x_1x_2 \oplus x_3x_4$, we have $|S_f| = 6$ (valency is 6) and $e = d = 2$!

- The Cayley graph of a **bent function** f is **not bipartite**.

- If Γ_f is **triangle-free** (no path of the form $uvwu$ for distinct $u, v, w \in V$) then f is **not bent**. Converse, not true !

Designing non-bent functions

- Assume you need $W_f(\mathbf{0}) = 0$, i.e., $\#\{x : f(x) = 0\} = \#\{x : f(x) = 1\} = 2^{n-1}$.
- Consequence : There exists $a \in \mathbb{F}_2^n$ so that $|W_f(a)| > 2^{n/2}$ (smaller distance to linear function $a \cdot x$!).

Designing non-bent functions

- Assume you need $W_f(\mathbf{0}) = 0$, i.e., $\#\{x : f(x) = 0\} = \#\{x : f(x) = 1\} = 2^{n-1}$.
- Consequence : There exists $a \in \mathbb{F}_2^n$ so that $|W_f(a)| > 2^{n/2}$ (smaller distance to linear function $a \cdot x$!).

Construction (ZhangPasalic) Let for $1 \leq i \leq n-1$, $E_i \subseteq \mathbb{F}_2^i$ and $E_i' = E_i \times \mathbb{F}_2^{n-i}$ such that $\bigcup_{i=1}^{n-1} E_i' = \mathbb{F}_2^n$, and

$$E_{i_1}' \cap E_{i_2}' = \emptyset, \quad 1 \leq i_1 < i_2 \leq n-1.$$

Let $X_n = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $X_i' = (x_1, \ldots, x_i) \in \mathbb{F}_2^i$ and $X_{n-i}'' = (x_{i+1}, \ldots, x_n) \in \mathbb{F}_2^{n-i}$. Let ϕ_i be a mapping from $\mathbb{F}_2^i$ to $\mathbb{F}_2^{n-i}$. A GMM type Boolean function $f \in \mathfrak{B}_n$ can be constructed as follows:

$$f(X_n) = \phi_i(X_i') \cdot X_{n-i}'' \oplus g_i(X_i'), \;\; \text{if } X_i' \in E_i, \;\; i = 1, \ldots, n-1, \qquad (1)$$

where $g_i \in \mathfrak{B}_i$.

Graph spectra

- Define Hadamard transform as $W_f^H(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x}$, then the spectra of f is $W_f^H = H_n f^T$, where H_n is the Hadamard matrix defined (recursively),

$$H_1 = \left(\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right), \quad H_n = \left(\begin{array}{cc} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{array} \right).$$

- Introduce ordering $W_f^H = \{W_f^H(0,\ldots,0), W_f^H(1,\ldots,0),\ldots, W_f^H(1,\ldots,1)\}$.

- The entries of H_n are $h_{i,j} = (-1)^{\mathbf{u}_i \cdot \mathbf{v}_j}$ for $i,j = 0,\ldots,2^n - 1$. Use binary representation of i,j e.g. $\mathbf{u}_3 = (1,1,0,\ldots,0)$.

Graph spectra

- Define Hadamard transform as $W_f^H(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x}$, then the spectra of f is $W_f^H = H_n f^T$, where H_n is the Hadamard matrix defined (recursively),

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}.$$

- Introduce ordering $W_f^H = \{W_f^H(0,\ldots,0), W_f^H(1,\ldots,0),\ldots,W_f^H(1,\ldots,1)\}$.
- The entries of H_n are $h_{i,j} = (-1)^{\mathbf{u}_i \cdot \mathbf{v}_j}$ for $i,j = 0,\ldots,2^n-1$. Use binary representation of i,j e.g. $\mathbf{u}_3 = (1,1,0,\ldots,0)$.

Theorem Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and let λ_i, $0 \le i \le 2^n - 1$ be the eigenvalues of its associated graph Γ_f. Then $\lambda_i = W_f(\mathbf{b}_i)$, for any i.

Proof: The eigenvectors of the Cayley graph Γ_f are the characters $Q_{\mathbf{w}}(x) = (-1)^{\mathbf{w} \cdot x}$ of $\mathbb{F}_2^n$ [?]. Moreover, the i-th eigenvalue of A_f (adjacency matrix), corresponding to the eigenvector $Q_{\mathbf{b}_i}$ is given by $\lambda_i = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{b}_i \cdot x} f(x) = W_f^H(\mathbf{b}_i)$. □

Diameter of the graph versus ANF

- The length $\max_{(u,v)} d(u,v)$ of the "longest shortest path" between any two graph vertices u, v of a graph - **diameter** of the graph.
- What about ANF of bent functions versus diameter ?

Diameter of the graph versus ANF

- The length $\max_{(u,v)} d(u,v)$ of the "longest shortest path" between any two graph vertices u, v of a graph - **diameter** of the graph.
- What about ANF of bent functions versus diameter ?
- We had $f(x_1, \ldots, x_4) = x_1x_2 \oplus x_3x_4$ and $\deg(f) = 2$. What is connected here ?
- Consider "primitive cubes" (a canonical basis of $\mathbb{F}_2^4$ if you want) $u = (1000)$ and $v = (0100)$. u and v are connected (edge between them) since $f(u \oplus v) = f(1100) = 1$!
- Is there a path between $u = (1000)$, $v = (0100)$ and $w = (0010)$. NO !
- Diameter $= \deg(f)$

Equivalence classes - groups of automorphisms

- **Affine Equivalence (EA)** in cryptography defined as $f \sim g$ for $f, g \in \mathfrak{B}_n$ IFF

$$g(x) = f(Ax + b) + \mu \cdot x + \epsilon \text{ for all } x \in \mathbb{F}_2^n, \tag{2}$$

  where $A \in GL(V_n)$, $b, \mu \in \mathbb{F}_2^n$.
- FACTS : Hard problem since checking if $f \sim g$ requires $O(2^{n^2})$ operations !
- EA preserves the degree of f and only permutes Walsh spectra (some other parameters invariant as well)

Equivalence classes - groups of automorphisms

- **Affine Equivalence (EA)** in cryptography defined as $f \sim g$ for $f, g \in \mathfrak{B}_n$ IFF

$$g(x) = f(Ax + b) + \mu \cdot x + \epsilon \text{ for all } x \in \mathbb{F}_2^n, \quad (2)$$

  where $A \in GL(V_n),\ b, \mu \in \mathbb{F}_2^n$.

- FACTS : Hard problem since checking if $f \sim g$ requires $O(2^{n^2})$ operations !
- EA preserves the degree of f and only permutes Walsh spectra (some other parameters invariant as well)

Group of automorphisms - group of permutations (under composition) of vertices preserving adjacency. Correspondence :

- Composition of permutations - product of invertible matrices in $GL(V_n)$
- Should be the case the spectra of Γ_f is not affected by applying automorphism to a graph.
- Diameter of a graph is invariant under action of $Aut(\Gamma_f)$.

Equivalence classes - example

- Let us, for $n = 2k$, identify $\mathbb{F}_2^n$ with $\mathbb{F}_2^k \times \mathbb{F}_2^k$. Suppose $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and $g \in \mathfrak{B}_k$. Then, $f : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2$ defined by

$$f(x, y) = x \cdot \pi(y) + g(y), \text{ for all } x, y \in \mathbb{F}_2^k, \tag{3}$$

  is a bent function. Let now $S_g = \cup_{i=1}^{2^{k-1}} u_i \mathbb{F}_{2^k}$, where $u_i = \alpha^{i(2^k-1)}$ and α primitive in $\mathbb{F}_{2^n}$.

- Notice $\mathcal{U} = \{u_0, u_1, \ldots, u_{2^k}\}$ is the cyclic group of $(2^k + 1)$-th roots of unity.

Equivalence classes - example

- Let us, for $n = 2k$, identify $\mathbb{F}_2^n$ with $\mathbb{F}_2^k \times \mathbb{F}_2^k$. Suppose $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and $g \in \mathfrak{B}_k$. Then, $f : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2$ defined by

$$f(x,y) = x \cdot \pi(y) + g(y), \text{ for all } x, y \in \mathbb{F}_2^k, \tag{3}$$

  is a bent function. Let now $S_g = \cup_{i=1}^{2^{k-1}} u_i \mathbb{F}_{2^k}$, where $u_i = \alpha^{i(2^k-1)}$ and α primitive in $\mathbb{F}_{2^n}$.
- Notice $\mathcal{U} = \{u_0, u_1, \ldots, u_{2^k}\}$ is the cyclic group of (2^k+1)-th roots of unity.
- Then $f \not\sim g$! HOW ??
- Compare the second order derivatives !! **Derivative** (1st order) of f at a is $D_f(a) = f(x) \oplus f(x+a)$ again Boolean function of course !
- How are graphs of $f(x)$ and $f(x+a)$ related to the graph of $D_f(a)$??

Multiple output bent functions

- Nyberg proved in 1992 that for $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^k$ the maximum output bent space is $n/2$ in binary case !

Multiple output bent functions

- Nyberg proved in 1992 that for $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ the maximum output bent space is $n/2$ in binary case !

- Meaning: One can find $f_1, \ldots, f_k$, $f_i : GF(2)^n \to GF(2)$, $k \le n/2$, (multiple bent $F : GF(2)^n \to GF(2)^k$) such that

$$a_1 f_1 + \ldots + a_k f_k \quad \text{is bent } \forall a \in GF(2)^k \setminus \{0\}.$$

- Hence at most $2^{n/2} - 1$ SRG graphs related to a single vectorial bent function !

Finding vectorial bent functions

- How to find such classes ?
- Use the relative trace $Tr_k^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-k}}$, a function from $GF(2^n) \to GF(2^k)$.
- Consider $F(x) = Tr_k^n(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$, where $a_i \in \mathbb{F}_{2^n}$

Finding vectorial bent functions

- How to find such classes ?
- Use the relative trace $Tr_k^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-k}}$, a function from $GF(2^n) \to GF(2^k)$.
- Consider $F(x) = Tr_k^n(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$, where $a_i \in \mathbb{F}_{2^n}$

Theorem [MPB] Let $n = 2k$, and define $F(x) = Tr_k^n(P(x))$, where $P(x) = \sum_{i=1}^{t} a_i x^{i(2^k-1)}$ and $t \le 2^k$. Then the following conditions are equivalent:

1. F is a vectorial bent function of dimension k.
2. $\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} = 1$ for all $\lambda \in K^*$.
3. There are two values $u \in \mathcal{U}$ such that $F(u) = 0$, and furthermore if $F(u_0) = 0$, then F is one-to-one and onto from $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ to K.

All credits go to Dillon !

- The exponent $2^k - 1$ is known as Dillon's exponent, and for $n = 2k$ we have $2^n - 1 = (2^k - 1)(2^k + 1)$.

- Note that $\#GF(2^k) \setminus 0 = 2^k - 1$, and there is a cyclic group U of $(2^k + 1)$th roots of unity of size $2^k + 1$!!

- Take a primitive $\alpha \in GF(2^n)$ and consider: $\{\alpha^{(2^k-1)i} : i = 0, \ldots 2^k\} = U$.

All credits go to Dillon !

- The exponent $2^k - 1$ is known as Dillon's exponent, and for $n = 2k$ we have $2^n - 1 = (2^k - 1)(2^k + 1)$.

- Note that $\#GF(2^k) \setminus 0 = 2^k - 1$, and there is a cyclic group U of $(2^k + 1)$th roots of unity of size $2^k + 1$!!

- Take a primitive $\alpha \in GF(2^n)$ and consider: $\{\alpha^{(2^k-1)i} : i = 0, \ldots 2^k\} = U$.

- **Meaning:** $GF(2^n)^* = \cup_{u \in U} uGF(2^k)^*$ so that $x = uy$, for $u \in U$, $y \in \mathbb{F}_{2^k}$ and

$$P(uy) = \sum_{i=1}^{t} a_i (uy)^{i(2^k-1)} = \sum_{i=1}^{t} a_i u^{i(2^k-1)} = P(u),$$

  as $y^{i(2^k-1)} = 1$ for any y because $y \in \mathbb{F}_{2^k}^*$.

- Recent result : we can count all bent F of this form and compute a_i explicitly [MPR2014] !!

Planar mappings

- From quadratic planar mappings you get commutative semifields (not associative) and affine/projective planes !
- Definition:

$$F(x + a) - F(x),$$

a permutation for any nonzero $a \in \mathbb{F}_q$ and $F : \mathbb{F}_q \to \mathbb{F}_q$!

Planar mappings

- From quadratic planar mappings you get commutative semifields (not associative) and affine/projective planes !
- Definition:

$$F(x+a)-F(x),$$

a permutation for any nonzero $a \in \mathbb{F}_q$ and $F : \mathbb{F}_q \to \mathbb{F}_q$!

- **Example :**$F(x) = x^2$ is planar **over any field of odd characteristic.**

- **PROOF:** $F(x+a)-F(x) = x^2+2ax+a^2-x^2 = 2ax+a^2$, permutation since any linear polynomial is permutation ! But $F(x)$ CANNOT be a permutation, check for x^2, $\gcd(2, p^n-1) = 2 \neq 1$!

Planar mappings

- From quadratic planar mappings you get commutative semifields (not associative) and affine/projective planes !
- Definition:

$$F(x+a) - F(x),$$

  a permutation for any nonzero $a \in \mathbb{F}_q$ and $F : \mathbb{F}_q \to \mathbb{F}_q$!
- **Example :**$F(x) = x^2$ is planar **over any field of odd characteristic.**

- **PROOF:** $F(x+a) - F(x) = x^2 + 2ax + a^2 - x^2 = 2ax + a^2$, permutation since any linear polynomial is permutation ! But $F(x)$ CANNOT be a permutation, check for x^2, $\gcd(2, p^n - 1) = 2 \neq 1$!

- What if the characteristic of $\mathbb{F}_q$ is $p = 2$?

Planar mappings

- From quadratic planar mappings you get commutative semifields (not associative) and affine/projective planes !
- Definition:

$$F(x+a) - F(x),$$

  a permutation for any nonzero $a \in \mathbb{F}_q$ and $F : \mathbb{F}_q \to \mathbb{F}_q$!
- **Example :**$F(x) = x^2$ is planar **over any field of odd characteristic.**

- **PROOF:** $F(x+a) - F(x) = x^2 + 2ax + a^2 - x^2 = 2ax + a^2$, permutation since any linear polynomial is permutation ! But $F(x)$ CANNOT be a permutation, check for x^2, $\gcd(2, p^n - 1) = 2 \neq 1$!

- What if the characteristic of $\mathbb{F}_q$ is $p = 2$?

- NO planar mappings over $GF(2^n)$ since for any b if x_0 is a solution to $F(x+a) + F(x) = b$ so is $x_0 + a$

Bent versus planar mappings

- **CONCLUSION:** Planar = Multiple bent of dimension n !!

Bent versus planar mappings

- **CONCLUSION:** Planar = Multiple bent of dimension n !!
- For $p = 2$ there are no planar mappings, but there are no bent functions of full space, recall bent space $\leq n/2$
- **PROBLEM:** Define a set of bent functions

$$f_i : GF(p^n) \to GF(p), \quad i = 1, \ldots, n,$$

  so that all linear combinations are bent = PLANAR FUNCTION !!
- If F is planar then F is not a permutation – bent functions are not balanced either !!

Known planar mappings

- By quadratic polynomials we mean Dembrovski-Ostrom polynomials

$$F(x) = \sum_{0 \le k,j < n} \lambda_{k,j} x^{p^k + p^j}, \quad \lambda_{k,j} \in \mathbb{F}_{p^n},$$

added an affine function $A(x) = \sum_{0 \le i < n} a_i x^{p^i}$

Known planar mappings

- By quadratic polynomials we mean Dembrovski-Ostrom polynomials

$$F(x) = \sum_{0 \le k,j < n} \lambda_{k,j} x^{p^k + p^j}, \quad \lambda_{k,j} \in \mathbb{F}_{p^n},$$

added an affine function $A(x) = \sum_{0 \le i < n} a_i x^{p^i}$

- Derivatives are linearized polynomials, easy to handle !

- Nontrivial interesting class of planar mappings is: $F(x) = x^{\frac{3^t+1}{2}}$ over $\mathbb{F}_{3^n}$, where t is odd and $\gcd(t, n) = 1$.

- The only example of nonquadratic planar mappings - hard to find !!!

Open problem : Let $n \ge 8$ be **even**. Find a permutation F over $GF(2^n)$ such that $F(x) + F(x + a) = b$ has either 0 or 2 solutions for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$. **Publish anywhere !!**

Dillon's exponents - generalization

- **IDEA:** Use Dillon's exponents for $p > 2$! Can we derive planar mappings as $F(x) = \sum_{i=0}^{p^{n/2}} b_i x^{i(p^{n/2}-1)}$?

- For even $n = 2k$ we consider $Tr(\lambda \sum_{i=0}^{p^{n/2}} b_i x^{i(p^{n/2}-1)})$, and show that such a function from $GF(p^n)$ to $GF(p)$ is bent for any nonzero λ, i.e.,

$$|\mathcal{F}_F(a)| = |\sum_{x \in \mathbb{F}_p^n} \omega^{Tr(F(x))+Tr(ax)}| = p^{n/2}, \quad \omega = e^{\frac{2\pi \imath}{p}}$$

Dillon's exponents - generalization

- **IDEA:** Use Dillon's exponents for $p > 2$! Can we derive planar mappings as $F(x) = \sum_{i=0}^{p^{n/2}} b_i x^{i(p^{n/2}-1)}$?

- For even $n = 2k$ we consider $Tr(\lambda \sum_{i=0}^{p^{n/2}} b_i x^{i(p^{n/2}-1)})$, and show that such a function from $GF(p^n)$ to $GF(p)$ is bent for any nonzero λ, i.e.,

$$|\mathcal{F}_F(a)| = |\sum_{x \in \mathbb{F}_p^n} \omega^{Tr(F(x))+Tr(ax)}| = p^{n/2}, \quad \omega = e^{\frac{2\pi\imath}{p}}$$

- Cannot use U any longer since $\gcd(p^k - 1, p^k + 1) = 2$.

- Use a set $V = 1, \alpha, \ldots, \alpha^{p^k}$ and $\mathbb{F}^*_{p^k}$ as α^i can be written as

$$\alpha^{(p^k-1)m}\alpha^l, \; 0 \leq l \leq p^k - 2, \; 0 \leq m \leq p^k.$$

- We specified the conditions that $F(x) = Tr_k^n \sum_{i=0}^{p^{n/2}} b_i x^{i(p^{n/2}-1)}$ is vectorial bent [BPRG2014]. But dimension is only $n/2$!!

Some concluding remarks

- What these generalized bent functions ($p > 2$) has to do with graphs ?
- Well, a LOT !! Again the graphs are strongly regular and are related to **association schemes** ! Some of these classes gives you new classes of SRG non-isomorphic to known classes !!
- Planar mappings are nice and elegant problem, surprisingly small number of nontrivial (nonquadratic) examples.
- We expect (hopefully) that a vivid research will be activated if managing to propose a single nontrivial example.

Some concluding remarks II

- Can we define suitable graphs for permutations over finite fields ?
- Well, a collection of n Cayley graphs w.r.t. component functions ?
- We lose the property of being strongly regular but important to investigate e.g. x^{-1} over $GF(2^8)$. All encryption today is done using this permutation as S-box.
- Does it make sense to define graphs to investigate $F(x) + F(x + a) = b$? For a fixed $a \neq 0$ and b we may say a and b are connected via x_0 iff x_0 is a solution to $F(x) + F(x + a) = b$?! What kind of graph is that ?
- Research ideas : Correspondence of graphs to derivatives, planar mappings, equivalence classes, minimal ANF representation ...