Some recent results and ideas on bent functions and their graph theoretic aspects

Enes Pasalic

Topics (roughly)

- Some recent results on vectorial bent functions
- Z-bent and generalized bent as "non-weird" stuff
- Graph theoretic aspects of Boolean functions
- Homogeneous bent functions (if time permits)

Hyperbent functions in the PS_{ap} class

- Let $k|n$, $k < n$, and $GF(2^n)$ be a finite field, then

$$Tr_k^n(x) = x + x^2 + x^{2^2} + \ldots + x^{n/k-1},$$

is a function from $GF(2^n) \to GF(2^k)$.

- Monomial (vectorial) bent functions $F(x) = Tr_k^n(ax^r)$ "easy".

- We can define a Boolean function $f : GF(2^n) \to GF(2)$ as

$$f(x) = Tr(ax^{2^k-1} + bx^{r(2^k-1)})$$

for $n = 2k$, but also

$$F(x) = Tr_k^n(ax^{2^k-1} + bx^{r(2^k-1)})$$

Hyperbent functions in the PS_{ap} class

- Let $k|n$, $k < n$, and $GF(2^n)$ be a finite field, then

$$Tr_k^n(x) = x + x^2 + x^{2^2} + \ldots + x^{n/k-1},$$

is a function from $GF(2^n) \to GF(2^k)$.

- Monomial (vectorial) bent functions $F(x) = Tr_k^n(ax^r)$ "easy".

- We can define a Boolean function $f : GF(2^n) \to GF(2)$ as

$$f(x) = Tr(ax^{2^k-1} + bx^{r(2^k-1)})$$

for $n = 2k$, but also

$$F(x) = Tr_k^n(ax^{2^k-1} + bx^{r(2^k-1)})$$

Dillon exponent - easy to treat

- 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 $2^k + 1$!!

$$\{\alpha^{(2^k-1)i} : i = 0, \dots 2^k\} = U.$$

- And

$$GF(2^n)^* = \cup_{u \in U} uGF(2^k)^*$$

Application of the unity circle

- We were interested in the functions of type

$$f_{a,b,r}(x) = Tr(ax^{2^k-1} + bx^{r(2^k-1)})$$

Write any $x \in GF(2^n)^*$ as $x = uy$ for $u \in U$, $y \in GF(2^k)^*$

$$\begin{aligned} f_{a,b,r}(x) &= f_{a,r}(yu) \\ &= Tr_1^n(u^{2^k-1}y^{2^k-1} + au^{(2^k-1)r}y^{(2^k-1)r}) \\ &= Tr_1^n(u^{2^k-1} + au^{(2^k-1)r}) \\ &= f_{a,b,r}(u), \end{aligned}$$

- Generalize to $F(x) = Tr_k^n(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$!!

Application of the unity circle

- We were interested in the functions of type

$$f_{a,b,r}(x) = Tr(ax^{2^k-1} + bx^{r(2^k-1)})$$

Write any $x \in GF(2^n)^*$ as $x = uy$ for $u \in U$, $y \in GF(2^k)^*$

$$\begin{aligned} f_{a,b,r}(x) &= f_{a,r}(yu) \\ &= Tr_1^n(u^{2^k-1}y^{2^k-1} + au^{(2^k-1)r}y^{(2^k-1)r}) \\ &= Tr_1^n(u^{2^k-1} + au^{(2^k-1)r}) \\ &= f_{a,b,r}(u), \end{aligned}$$

- Generalize to $F(x) = Tr_k^n(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$!!

Specifying (hyper)bent vectorial functions in PS_{ap}

Theorem (EP et al. 2013)

Let $n = 2k$, $K = GF(2^k)$ *and* $L = GF(2^n)$. *Define*

$$F(x) = Tr_k^n\left(\sum_{i=1}^{t} a_i x^{r_i(2^k-1)}\right)$$

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* $u \in \mathcal{U}$ *s. t.* $F(u) = 0$. *If* $F(u_0) = 0$, *then* F *is one-to-one and onto from* $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ *to* K.
4. *The elementary symmetric polynomials* σ_e, *used as coefficients in the expansion of* $\prod_{u\in\mathcal{U}}(x - F(u))$, *satisfy the following: for any odd* e, $1 \le e \le 2^k + 1$, *we must have* $\sigma_{2^k-1} = 1$, *and* $\sigma_e = 0$ *otherwise.*

Specifying (hyper)bent vectorial functions in PS_{ap}

Theorem (EP et al. 2013)

Let $n = 2k$, $K = GF(2^k)$ *and* $L = GF(2^n)$. *Define*

$$F(x) = Tr_k^n(\sum_{i=1}^{t} a_i x^{r_i(2^k-1)})$$

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 $u \in \mathcal{U}$ s. t. $F(u) = 0$. If $F(u_0) = 0$, then F is one-to-one and onto from $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ to K.*
4. *The elementary symmetric polynomials σ_e, used as coefficients in the expansion of $\prod_{u\in\mathcal{U}}(x - F(u))$, satisfy the following: for any odd e, $1 \le e \le 2^k + 1$, we must have $\sigma_{2^k-1} = 1$, and $\sigma_e = 0$ otherwise.*

Specifying (hyper)bent vectorial functions in PS_{ap}

Theorem (EP et al. 2013)

Let $n = 2k$, $K = GF(2^k)$ and $L = GF(2^n)$. Define

$$F(x) = Tr_k^n(\sum_{i=1}^{t} a_i x^{r_i(2^k-1)})$$

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 $u \in \mathcal{U}$ s. t. $F(u) = 0$. If $F(u_0) = 0$, then F is one-to-one and onto from $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ to K.*
4. *The elementary symmetric polynomials σ_e, used as coefficients in the expansion of $\prod_{u\in\mathcal{U}}(x - F(u))$, satisfy the following: for any odd e, $1 \le e \le 2^k + 1$, we must have $\sigma_{2^k-1} = 1$, and $\sigma_e = 0$ otherwise.*

Specifying (hyper)bent vectorial functions in PS_{ap}

Theorem (EP et al. 2013)

Let $n = 2k$, $K = GF(2^k)$ *and* $L = GF(2^n)$. *Define*

$$F(x) = Tr_k^n\Big(\sum_{i=1}^{t} a_i x^{r_i(2^k-1)}\Big)$$

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* $u \in \mathcal{U}$ *s. t.* $F(u) = 0$. *If* $F(u_0) = 0$, *then* F *is one-to-one and onto from* $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ *to* K.
4. *The elementary symmetric polynomials* σ_e, *used as coefficients in the expansion of* $\prod_{u\in\mathcal{U}}(x - F(u))$, *satisfy the following: for any odd* e, $1 \le e \le 2^k + 1$, *we must have* $\sigma_{2^k-1} = 1$, *and* $\sigma_e = 0$ *otherwise.*

Specifying (hyper)bent vectorial functions in PS_{ap} II

- Second equivalence leads to the whole class of vectorial (hyper)bent functions. $F(x) = Tr_k^n(\sum_{i=1}^{t} a_i x^{r_i(2^k-1)})$!!
- Let $P(x) = \sum_{t=0}^{2^k} a_t x^t$ so that $F(x) = Tr_k^n(P(x^{2^k-1}))$.

Facts

- *Assume* $Tr_k^n(u_s) \neq 0$, *where* $u_s = \alpha^{(2^k-1)s}$. *Then,*

$$\{Tr_k^n(zu_s) = zTr_k^n(u_s) : z \in K\} = K.$$

- *Let* $\theta : \{0, 1, 2, \ldots, 2^k\} \to K$ *be a surjective function and 0 is taken twice.*

- *Interpolate* $(u_i, u_s\theta(i))$ *by* $P(x)$, *that is,* $P(x)$ *will satisfy* $P(u_i) = u_s\theta(i)$ *for all* $u_i \in \mathcal{U}$. *This* $P(x)$ *satisfies item 3, that is,* $Tr_k^n(\sum_{t=0}^{2^k} a_t u^t)$ *maps* $\mathcal{U}$ *to* $K \cup \{0\}$ *!!*

Main existence and counting result

Theorem (EP et al. 2014)

There are exactly $(2^k+1)!\,2^{k-1}$ vectorial (hyper)bent functions of the above form.

Let $\Phi : \{0,1,\ldots,2^k\} \to L$ be given by $\Phi(i) = u_s\theta(i)$, $i = 0,1,\ldots,2^k$, where $\theta : \{0,1,2,\ldots,2^k\} \to K$ is a surjective function that takes the zero value two times. The coefficients of the interpolating polynomial $P(x) = \sum_{t=0}^{2^k} a_t x^t$ of the points $(u_i, \Phi(i))$, $i = 0,1,\ldots,2^k$, are given by

$$a_{2^k-t} = u_s \sum_{i=0}^{2^k} u_i^{t+1}\theta(i) \ \text{ for } \ t = 0,1,\ldots 2^k. \tag{1}$$

Sparse polynomial forms

- Any surjective $\theta : \{0, 1, 2, \ldots, 2^k\} \rightarrow K$ such that 0 is taken twice gives a vectorial bent function.

Open problem:

Specify those θ that give binomial or trinomial bent functions ! We tried something in this direction but ended up only in ensuring that a small portion of coefficients is zero.

Symmetric polynomials - nonexistence results

Open (solved) problem:

Let $n = 2k \equiv 0 \pmod 4$, where $k \geq 2$ is even, and let D odd given by $2^k + 1 = 3D + 2$. Show that the condition

$$(Tr_k^n(\gamma^{D+1}))^{-8} = Tr_k^n(\gamma^{D-2})$$

is never satisfied for any n, and for any $\gamma \in \mathcal{U}$. Then, $F(x) = Tr_k^n(x^{2^k-1} + ax^{r(2^k-1)})$ is not vectorial bent !!

- Solved recently EP 2014, was an easy open problem :)

Open problem:

Using similar approach derive similar (more complicated) conditions for trinomials ...

Making "good" S-boxes out of bent functions

- Assume $F(K) = 0$ and replace all-zero values on K by a permutation and call it $\tilde{F}$!
- Denote by $\delta_{\tilde{F}}(a, b) = \#\{x \in \mathbb{F}^n,\ F(X_n + a) + F(X_n) = b\}$, for $n = 8$ we have:

$\delta_{\tilde{F}}(a, b)$	0	14	16	18	20	22	24	26
Number	15	1421	1511	815	243	61	13	1

- For $n = 8$ and $G(x) = x^{-1}$ deleting last 4 coordinate functions we have:

Table : The differential property of $G_1 = (g_1, g_2, g_3, g_4)$

$\delta_{G_1}(a, b)$	2	4	6	8	10	12	14	16	18	20	22	24	26	28
Nmb.	1	4	30	117	263	488	749	806	699	495	283	103	39	3

A few words on "forgotten" classes of Carlet

- In 1994 Carlet proposed two new classes (extending Maiorana-McFarland) of bent functions called C and D.
- In particular, the subclass D_0 defined by

$$(x, y) \to \prod_{i=1}^{k}(x_i + 1) + x \cdot \pi(y), \quad x, y \in \mathbb{F}_2^k,$$

is not in completed MM or PS class !!!

- We recently analyzed bent conditions of C class defined by,

$$x \cdot \pi(y) + 1_{L^\perp}(x),$$

– L linear subspace of $a \in GF(2)^k$.

– π any permutations s.t. $\pi^{-1}(L + a)$ is a flat $\forall a \in GF(2)^k$.

A few words on "forgotten" classes of Carlet

- In 1994 Carlet proposed two new classes (extending Maiorana-McFarland) of bent functions called C and D.
- In particular, the subclass D_0 defined by

$$(x, y) \to \prod_{i=1}^{k}(x_i + 1) + x \cdot \pi(y), \quad x, y \in \mathbb{F}_2^k,$$

is not in completed MM or PS class !!!

- We recently analyzed bent conditions of C class defined by,

$$x \cdot \pi(y) + 1_{L^\perp}(x),$$

– L linear subspace of $a \in GF(2)^k$.

– π any permutations s.t. $\pi^{-1}(L + a)$ is a flat $\forall a \in GF(2)^k$.

A few words on "forgotten" classes of Carlet II

- **Conclusion :** Hard problem to find L and π satisfying "simple" conditions !!

Example

Denote $\phi = \pi^{-1}$. Consider $\dim(L) = 2$ (easiest case) and $\phi(x) = x^{1+2^r+2^s}$ (for suitable r, s). No such 2-dimensional space L

Example

Suppose $\phi(x) = x^{2^i+1}$, for all $x \in \mathbb{F}_{2^k}$, where $\gcd(i,k) = e$, k/e is odd. Then, $L = \langle u, cu \rangle$ where $c, u \in \mathbb{F}_{2^k}^*$ satisfies the bent condition !

Open problem:

Find more (L, π) and deduce whether we get new bent functions !

A few words on "forgotten" classes of Carlet II

- **Conclusion :** Hard problem to find L and π satisfying "simple" conditions !!

Example

Denote $\phi = \pi^{-1}$. Consider $\dim(L) = 2$ (easiest case) and $\phi(x) = x^{1+2^r+2^s}$ (for suitable r, s). No such 2-dimensional space L

Example

Suppose $\phi(x) = x^{2^i+1}$, for all $x \in \mathbb{F}_{2^k}$, where $\gcd(i,k) = e$, k/e is odd. Then, $L = \langle u, cu \rangle$ where $c, u \in \mathbb{F}^*_{2^k}$ satisfies the bent condition !

Open problem:

Find more (L, π) and deduce whether we get new bent functions !

A few words on "forgotten" classes of Carlet II

- **Conclusion :** Hard problem to find L and π satisfying "simple" conditions !!

Example

Denote $\phi = \pi^{-1}$. Consider $\dim(L) = 2$ (easiest case) and $\phi(x) = x^{1+2^r+2^s}$ (for suitable r, s). No such 2-dimensional space L

Example

Suppose $\phi(x) = x^{2^i+1}$, for all $x \in \mathbb{F}_{2^k}$, where $\gcd(i,k) = e$, k/e is odd. Then, $L = \langle u, cu \rangle$ where $c, u \in \mathbb{F}_{2^k}^*$ satisfies the bent condition !

Open problem:

Find more (L, π) and deduce whether we get new bent functions !

A very few words on Z-bent functions

- Z-bent framework - a nice approach to bent functions - an open problem of **Dobbertin and Leander** of finding non-splitting Z-bent functions was solved recently EP et al.
- Recall $f : \mathbb{F}_2^n \to W_r \subset \mathbb{Z}$ is Z-bent of level r if both image and NFT values lies in

$$\begin{aligned} W_0 &= \{-1, 1\} \\ W_r &= \{w \in \mathbb{Z} \mid -2^{r-1} \le w \le 2^{r-1}\} \end{aligned}$$

Gangopadhyay et al., 2013, construct all bent functions for $n = 6$ by considering PS-type Z-bent functions !! A case of non-equivalence to MM and PS_{ap} when $n = 8$.

Open problem:

Derive more interesting bent classes from Z-bent functions.

A very few words on Z-bent functions

- Z-bent framework - a nice approach to bent functions - an open problem of **Dobbertin and Leander** of finding non-splitting Z-bent functions was solved recently EP et al.
- Recall $f : \mathbb{F}_2^n \to W_r \subset \mathbb{Z}$ is Z-bent of level r if both image and NFT values lies in

$$
\begin{aligned}
W_0 &= \{-1, 1\} \\
W_r &= \{w \in \mathbb{Z} \mid -2^{r-1} \leq w \leq 2^{r-1}\}
\end{aligned}
$$

Gangopadhyay et al., 2013, construct all bent functions for $n = 6$ by considering PS-type Z-bent functions !! A case of non-equivalence to MM and PS_{ap} when $n = 8$.

Open problem:

Derive more interesting bent classes from Z-bent functions.

Even less than a few words on generalized bent functions

- Define $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_q$, call it gbent function if

$$|H_f(\omega|) = |2^{-\frac{n}{2}} \sum_{x \in \mathbb{Z}_2^n} \zeta^{f(x)} (-1)^{\omega \cdot x}| = 1.$$

- FOLKLORE: If $q = 4$, then $f(x) = a(x) + 2b(x)$ is gbent IFF a and $a + b$ are standard bent !!

- What if $f(x) = c_1 a(x) + c_2 b(x)$ and q arbitrary ?

Then we show that (mostly) $c_1 = q/2$ and $c_2 = q/4$ or $c_2 = 3q/4$, for $q = 4s$ - necessary condition ! Also, the cases both $a(x)$ and $b(x)$ are Boolean or $a(x)$ and $b(x)$ are gbent or a mixture of the two are considered, EP and S. Hodzic, 2014.

Open problem:

Other direction, construct gbent f and decompose into bent functions, e.g. $q = 2^r$!

Even less than a few words on generalized bent functions

- Define $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$, call it gbent function if

$$|H_f(\omega|) = |2^{-\frac{n}{2}} \sum_{x \in \mathbb{Z}_2^n} \zeta^{f(x)}(-1)^{\omega \cdot x}| = 1.$$

- FOLKLORE: If $q = 4$, then $f(x) = a(x) + 2b(x)$ is gbent IFF a and $a + b$ are standard bent !!

- What if $f(x) = c_1 a(x) + c_2 b(x)$ and q arbitrary ?

Then we show that (mostly) $c_1 = q/2$ and $c_2 = q/4$ or $c_2 = 3q/4$, for $q = 4s$ - necessary condition ! Also, the cases both $a(x)$ and $b(x)$ are Boolean or $a(x)$ and $b(x)$ are gbent or a mixture of the two are considered, EP and S. Hodzic, 2014.

Open problem:

Other direction, construct gbent f and decompose into bent functions, e.g. $q = 2^r$!

Even less than a few words on generalized bent functions

- Define $f: \mathbb{Z}_2^n \to \mathbb{Z}_q$, call it gbent function if

$$|H_f(\omega|) = |2^{-\frac{n}{2}} \sum_{x \in \mathbb{Z}_2^n} \zeta^{f(x)} (-1)^{\omega \cdot x}| = 1.$$

- FOLKLORE: If $q = 4$, then $f(x) = a(x) + 2b(x)$ is gbent IFF a and $a + b$ are standard bent !!
- What if $f(x) = c_1 a(x) + c_2 b(x)$ and q arbitrary ?

Then we show that (mostly) $c_1 = q/2$ and $c_2 = q/4$ or $c_2 = 3q/4$, for $q = 4s$ - necessary condition ! Also, the cases both $a(x)$ and $b(x)$ are Boolean or $a(x)$ and $b(x)$ are gbent or a mixture of the two are considered, EP and S. Hodzic, 2014.

Open problem:

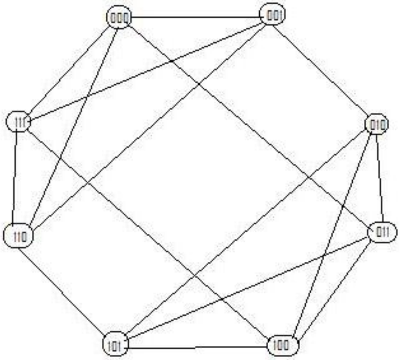
Other direction, construct gbent f and decompose into bent functions, e.g. $q = 2^r$!

Recalling Cayley graph

- *Cayley graph* of $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\Gamma_f = (\mathbb{F}_2^n, E_f)$, $E_f = \{(\mathbf{w}, \mathbf{u}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \ : \ f(\mathbf{w} \oplus \mathbf{u}) = 1\}$.
- Adjacency matrix $A_f = \{a_{i,j}\}$, $a_{i,j} = f(\mathbf{b}(i) \oplus \mathbf{b}(j))$;
- Γ_f is a *regular graph of degree* $wt(f) = |\Omega_f|$
- *Spectrum* of Γ_f is the set of eigenvalues of A_f (Γ_f).

Cayley graph example: $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_3$

Truth Table: 01010011



Recalling SRG Cayley graph

- An r-regular graph Γ with parameters (v, r, d, e) is a *strongly regular graph* (srg) iff $\exists\ e, d > 0$ s.t.

$$\#adj(\mathbf{u}, \mathbf{v}) = e \quad \#nonadj(\mathbf{u}, \mathbf{v}) = d, \quad \forall \mathbf{u}, \mathbf{v}$$

- The parameters satisfy $r(r - d - 1) = e(v - r - 1)$.

P.J. Cameron: "*Strongly regular graphs lie on the cusp between highly structured and unstructured. For example, there is a unique srg with parameters* $(36, 10, 4, 2)$, *but there are* 32548 *non-isomorphic SRG with parameters* $(36, 15, 6, 6)$. *In the light of this, it will be difficult to develop a theory of random strongly regular graphs!*"

One more tool - Walsh-Hadamard transform

- A bit confusing Walsh, Walsh-Hadamard, (normalized) Fourier ...
- Anyway, Walsh-Hadamard transform is similar to WT,

$$\hat{W}_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\alpha \cdot x},$$

thus instead of $(-1)^{f(x)}$ we use $f(x)$.

- We simply get direct connection to graph eigenvalues !
- Easy to show that $W_f(\alpha) = -2\hat{W}_f(\alpha) + 2^n\delta(\alpha)$, where $\delta(0) = 1$ and zero otherwise.

One more tool - Walsh-Hadamard transform

- A bit confusing Walsh, Walsh-Hadamard, (normalized) Fourier ...
- Anyway, Walsh-Hadamard transform is similar to WT,

$$\hat{W}_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\alpha \cdot x},$$

  thus instead of $(-1)^{f(x)}$ we use $f(x)$.
- We simply get direct connection to graph eigenvalues !
- Easy to show that $W_f(\alpha) = -2\hat{W}_f(\alpha) + 2^n\delta(\alpha)$, where $\delta(0) = 1$ and zero otherwise.

WH transform - some easy observations

- Walsh spectra of bent functions is $W_f(\alpha) \in \{-2^{n/2}, +2^{n/2}\}$
- Since

$$W_f(0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = \pm 2^{n/2}$$

then

$$wt(f) = 2^{n-1} - 2^{n/2-1} \quad \text{or} \quad wt(f) = 2^{n-1} + 2^{n/2-1}.$$

- On the other hand, using WH transform the spectra of bent functions is either

$$\{2^{n-1} - 2^{n/2-1}, -2^{n/2-1}, 2^{n/2-1}\}$$

or

$$\{2^{n-1} - 2^{n/2-1}, -2^{n/2-1}, 2^{n/2-1}\}$$

WH transform - some easy observations

- Walsh spectra of bent functions is $W_f(\alpha) \in \{-2^{n/2}, +2^{n/2}\}$
- Since
$$W_f(0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = \pm 2^{n/2}$$
then
$$wt(f) = 2^{n-1} - 2^{n/2-1} \text{ or } wt(f) = 2^{n-1} + 2^{n/2-1}.$$
- On the other hand, using WH transform the spectra of bent functions is either
$$\{2^{n-1} - 2^{n/2-1}, -2^{n/2-1}, 2^{n/2-1}\}$$
or
$$\{2^{n-1} - 2^{n/2-1}, -2^{n/2-1}, 2^{n/2-1}\}$$

Cayley graph - connections

Theorem (Bernasconi–Codenotti '99)

The following are equivalent for $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

(i) *The eigenvalues of* Γ_f, $\lambda_i = \hat{W}_f(\mathbf{b}(i))$, $\forall i$.

(ii) *multiplicity*$(\hat{W}_b(\mathbf{b}(0))) = 2^{n-dim\langle\Omega_f\rangle}$, *where* $dim\langle\Omega_f\rangle$ *is the dimension of* $\langle\Omega_f\rangle$ *as a subspace of* $\mathbb{F}_2^n$ *over* $\mathbb{F}_2$.

(iii) *(Under* Γ_f *connected)* f *has a spectral coefficient equal to* $-wt(f)$ *iff its Walsh spectrum is symmetric w.r.t* 0.

(iv) *The* $\#$ *nonzero spectral coefficients equals* $rk(A_f)$, *and* $2^{d_2} \leq rk(A_f) \leq \sum_{i=1}^{d} \binom{n}{i}$ *(*d_2*, respectively,* d *is the degree of* f *over* $\mathbb{F}_2$*, respectively* $\mathbb{R}$*).*

Cayley graph - connections

Theorem (Bernasconi–Codenotti '99)

The following are equivalent for $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

(i) *The eigenvalues of Γ_f, $\lambda_i = \hat{W}_f(\mathbf{b}(i))$, $\forall i$.*

(ii) *multiplicity$(\hat{W}_b(\mathbf{b}(0))) = 2^{n-dim\langle\Omega_f\rangle}$, where $dim\langle\Omega_f\rangle$ is the dimension of $\langle\Omega_f\rangle$ as a subspace of $\mathbb{F}_2^n$ over $\mathbb{F}_2$.*

(iii) *(Under Γ_f connected) f has a spectral coefficient equal to $-wt(f)$ iff its Walsh spectrum is symmetric w.r.t 0.*

(iv) *The # nonzero spectral coefficients equals $rk(A_f)$, and $2^{d_2} \leq rk(A_f) \leq \sum_{i=1}^{d} \binom{n}{i}$ (d_2, respectively, d is the degree of f over $\mathbb{F}_2$, respectively $\mathbb{R}$).*

Cayley graph - connections

Theorem (Bernasconi–Codenotti '99)

The following are equivalent for $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

(*i*) *The eigenvalues of* Γ_f, $\lambda_i = \hat{W}_f(\mathbf{b}(i))$, $\forall i$.

(*ii*) *multiplicity*$(\hat{W}_b(\mathbf{b}(0))) = 2^{n-dim\langle\Omega_f\rangle}$, *where* $dim\langle\Omega_f\rangle$ *is the dimension of* $\langle\Omega_f\rangle$ *as a subspace of* $\mathbb{F}_2^n$ *over* $\mathbb{F}_2$.

(*iii*) *(Under* Γ_f *connected)* f *has a spectral coefficient equal to* $-wt(f)$ *iff its Walsh spectrum is symmetric w.r.t* 0.

(*iv*) *The* $\#$ *nonzero spectral coefficients equals* $rk(A_f)$, *and* $2^{d_2} \leq rk(A_f) \leq \sum_{i=1}^{d} \binom{n}{i}$ *(*d_2*, respectively,* d *is the degree of* f *over* $\mathbb{F}_2$*, respectively* $\mathbb{R}$*).*

Cayley graph - connections

Theorem (Bernasconi–Codenotti '99)

The following are equivalent for $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

(i) *The eigenvalues of* Γ_f, $\lambda_i = \hat{W}_f(\mathbf{b}(i))$, $\forall i$.

(ii) $multiplicity(\hat{W}_b(\mathbf{b}(0))) = 2^{n-dim\langle\Omega_f\rangle}$, *where* $dim\langle\Omega_f\rangle$ *is the dimension of* $\langle\Omega_f\rangle$ *as a subspace of* $\mathbb{F}_2^n$ *over* $\mathbb{F}_2$.

(iii) *(Under* Γ_f *connected)* f *has a spectral coefficient equal to* $-wt(f)$ *iff its Walsh spectrum is symmetric w.r.t* 0.

(iv) *The* $\#$ *nonzero spectral coefficients equals* $rk(A_f)$, *and* $2^{d_2} \le rk(A_f) \le \sum_{i=1}^{d} \binom{n}{i}$ *(*d_2*, respectively,* d *is the degree of* f *over* $\mathbb{F}_2$*, respectively* $\mathbb{R}$*).*

Cayley graph - connections II

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 $\lambda_i = \hat{W}_f(\mathbf{b}_i)$, 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 $\mathbb{F}_2^n$ [CVETK72]. Moreover, the i-th eigenvalue of A_f (adjacency matrix), corresponding to the eigenvector $Q_{\mathbf{b}_i}$ is

$$\lambda_i = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{b}_i \cdot x} f(x) = \hat{W}_f(\mathbf{b}_i).$$

$\square$

Few spectral coefficients

Cvetkovic & Doob (various years)

- Γ_f has three distinct eigenv. $0, \pm\lambda$ if and only if Γ_f is complete bipartite between Ω_f and $\mathbb{F}_2^n \backslash \Omega_f$ (**plateaued !!**).

- Γ_f has three distinct eigenv. $\lambda_0 = |\Omega_f| > \lambda_1 = 0 > \lambda_2 \neq -\lambda_0$ if and only if $\bar{\Gamma}_f$ is the direct sum of $-\frac{r}{\lambda_2} + 1$ complete graphs of order $-\lambda_2$. (skewed case)

- If Γ_f has three distinct (nonzero) eigenvalues (bent case): $\lambda_0 = |\Omega_f| = wt(f), \lambda_2 = -\lambda_1 = \sqrt{|\Omega_f| - e}$, of multiplicities $m_0 = 1, m_1 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)-|\Omega_f|}{2\sqrt{|\Omega_f|-e}}, m_2 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)+|\Omega_f|}{2\sqrt{|\Omega_f|-e}}$.

Few spectral coefficients

Cvetkovic & Doob (various years)

- Γ_f has three distinct eigenv. $0, \pm\lambda$ if and only if Γ_f is complete bipartite between Ω_f and $\mathbb{F}_2^n \backslash \Omega_f$ (**plateaued !!**).

- Γ_f has three distinct eigenv. $\lambda_0 = |\Omega_f| > \lambda_1 = 0 > \lambda_2 \neq -\lambda_0$ if and only if $\bar{\Gamma}_f$ is the direct sum of $-\frac{r}{\lambda_2} + 1$ complete graphs of order $-\lambda_2$. (skewed case)

- If Γ_f has three distinct (nonzero) eigenvalues (bent case): $\lambda_0 = |\Omega_f| = wt(f), \lambda_2 = -\lambda_1 = \sqrt{|\Omega_f| - e}$, of multiplicities $m_0 = 1, m_1 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)-|\Omega_f|}{2\sqrt{|\Omega_f|-e}}, \ m_2 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)+|\Omega_f|}{2\sqrt{|\Omega_f|-e}}$.

Few spectral coefficients

Cvetkovic & Doob (various years)

- Γ_f has three distinct eigenv. $0, \pm\lambda$ if and only if Γ_f is complete bipartite between Ω_f and $\mathbb{F}_2^n \backslash \Omega_f$ (**plateaued !!**).

- Γ_f has three distinct eigenv. $\lambda_0 = |\Omega_f| > \lambda_1 = 0 > \lambda_2 \neq -\lambda_0$ if and only if $\bar{\Gamma}_f$ is the direct sum of $-\frac{r}{\lambda_2} + 1$ complete graphs of order $-\lambda_2$. (skewed case)

- If Γ_f has three distinct (nonzero) eigenvalues (bent case): $\lambda_0 = |\Omega_f| = wt(f), \lambda_2 = -\lambda_1 = \sqrt{|\Omega_f| - e}$, of multiplicities $m_0 = 1, m_1 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)-|\Omega_f|}{2\sqrt{|\Omega_f|-e}}$, $m_2 = \frac{\sqrt{|\Omega_f|-e}\,(2^n-1)+|\Omega_f|}{2\sqrt{|\Omega_f|-e}}$.

- Bernasconi and Codenotti started an investigation in '99 by displaying the Cayley graphs associated to each equivalence class representative of Boolean functions in 4 variables; obviously, there are $2^{2^4} = 65,536$ different Boolean functions in 4 variables, and the number of equivalence classes in four variables under affine transformations is only 8 (eight).

- We display the truth table and the WH spectrum of a representative of each class in Table 2.

- Bernasconi and Codenotti started an investigation in '99 by displaying the Cayley graphs associated to each equivalence class representative of Boolean functions in 4 variables; obviously, there are $2^{2^4} = 65,536$ different Boolean functions in 4 variables, and the number of equivalence classes in four variables under affine transformations is only 8 (eight).

- We display the truth table and the WH spectrum of a representative of each class in Table 2.

4-variable equivalence classes

Table : Truth table and WH spectrum of equivalence class representatives for Boolean functions in 4 variables under affine transformations

No.	Boolean Representative	WH Spectrum															
1	0000000000000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	00000000 00000001	1	-1	-1	1	-1	1	1	-1	-1	1	1	-1	1	-1	-1	1
3	0000000000000011	2	0	-2	0	-2	0	2	0	-2	0	2	0	2	0	-2	0
4	0000000000000111	3	-1	-1	-1	-3	1	1	1	-3	1	1	1	3	-1	-1	-1
5	0000000000001111	4	0	0	0	-4	0	0	0	-4	0	0	0	4	0	0	0
6	0000000000010111	4	-2	-2	0	-2	0	0	2	-4	2	2	0	2	0	0	-2
7	0000000100010111	5	-3	-3	1	-3	1	1	1	-3	1	1	1	1	1	1	-3
8	0000001101011001	6	-2	-2	2	-2	-2	2	-2	-2	2	-2	-2	-2	2	2	2

Question : How many nonisomorphic Cayley graphs there are over $\mathbb{F}_2^4$?

Got the answer a few months ago but I forgot it :)

First equivalence class

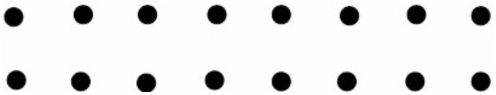


Figure : Cayley graph associated to the first representative of Table 2

- The Cayley graph associated to the representative of the first equivalence class has only one eigenvalue, and is a totally disconnected graph

Second equivalence class

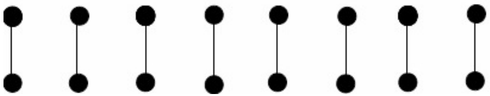


Figure : Cayley graph associated to the second representative of Table 2

- The Cayley graph associated to the representative of the second equivalence class has two distinct spectral coefficients and its associated graph is a pairing, that is, a set of edges without common vertices.

Third equivalence class

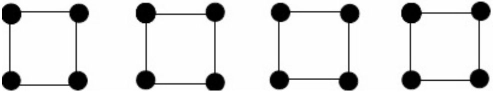


Figure : Cayley graph associated to the third representative of Table 2

- The Cayley graph associated to the representative of the third equivalence class has four connected components and three distinct eigenvalues, one equal to 0 and two symmetric with respect to 0. That implies that each connected component is a complete bipartite graph.

Fourth equivalence class

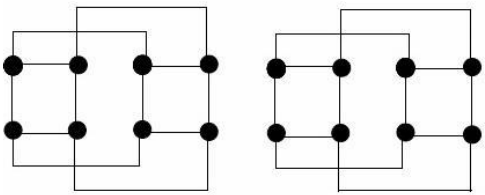


Figure : Cayley graph associated to the fourth representative of Table 2

- The Cayley graph associated to the representative of the fourth equivalence class has two connected components, each corresponding to a three-dimensional cube.

Fifth equivalence class

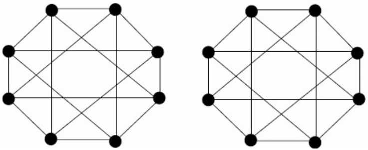


Figure : Cayley graph associated to the fifth representative of Table 2

- The Cayley graph associated to the representative of the fifth equivalence class has two connected components and three distinct eigenvalues as for the third equivalence class, and so, each connected component is a complete bipartite graph.

Fifth equivalence class

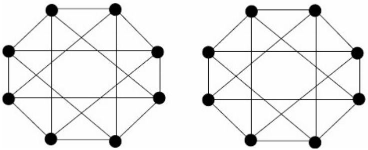


Figure : Cayley graph associated to the fifth representative of Table 2

- The Cayley graph associated to the representative of the fifth equivalence class has two connected components and three distinct eigenvalues as for the third equivalence class, and so, each connected component is a complete bipartite graph.
- Should correspond to semi-bent functions with WH spectra $\{0, 2^{n/2+1}, -2^{n/2+1}\}$!
- Interesting - since 4 suitable semi-bent functions on $\mathbb{F}_2^n$ give a bent function on $\mathbb{F}_2^{n+2}$ ... Need a smart extrapolation of graphs to get SRG Cayley graph.

Sixth equivalence class

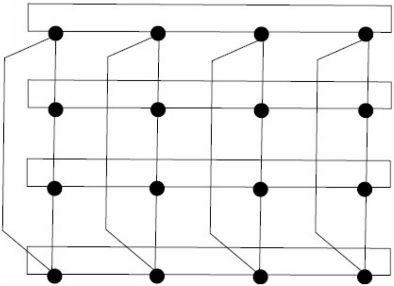


Figure : Cayley graph associated to the sixth representative of Table 2

- The Cayley graph associated to the representative of the sixth equivalence class is a connected graph, with five distinct eigenvalues.

Seventh equivalence class

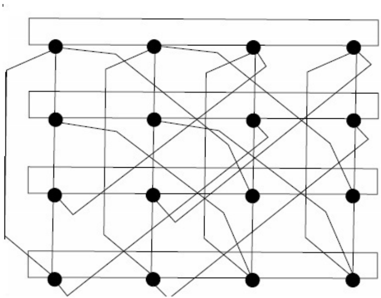


Figure : Cayley graph associated to the seventh representative of Table 2

- The Cayley graph associated to the representative of the seventh equivalence class has only three distinct eigenvalues and, therefore, is strongly regular.

Eighth equivalence class

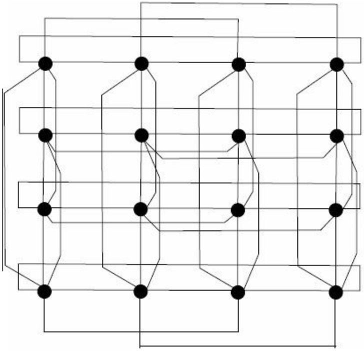


Figure : Cayley graph associated to the eighth representative of Table 2

- The Cayley graph associated to the representative (which is a bent function) of the eighth equivalence class is strongly regular, with parameters $e = d = 2$.

Bent Cayley graph characterization

Theorem (Bernasconi-Codenotti '99 & Bernasconi-Codenotti-VanderKam '01)

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (n even) is bent iff Γ_f is a srg with $e = d$.

Moreover, $A^2 = \left(2^{n-1} \pm 2^{n/2-1} - e\right) I + eJ.$

- **Question:** How can/do we use it to find bent (or nonbent) f's?

Bent Cayley graph characterization

Theorem (Bernasconi-Codenotti '99 & Bernasconi-Codenotti-VanderKam '01)

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ (n even) is bent iff Γ_f is a srg with $e = d$.

Moreover, $A^2 = \left(2^{n-1} \pm 2^{n/2-1} - e\right) I + eJ.$

- **Question:** How can/do we use it to find bent (or nonbent) f's?

bipartite $\longleftrightarrow$ no odd length cycles $\longleftrightarrow$ sym. spectrum

Theorem (Bernasconi & Codenotti, '00)

Assume $f(\mathbf{0}) = 0$ & Γ_f connected. Then Γ_f is bipartite if and only if $\mathbb{F}_2^n - \Omega_f$ contains a subspace of dimension $n-1$.

Theorem (P.S. '07)

If f is bent, then Γ_f is not bipartite. In fact, if Γ_f is triangle-free (no paths of the form $xyzx$, where the vertices x, y, z are distinct), then f is not bent.

- Converse not true:

$$f(\mathbf{x}) = x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6 \oplus x_5x_6x_1 \oplus x_6x_1x_2$$

Γ_f has plenty of triangles, but f is not bent.

bipartite $\longleftrightarrow$ no odd length cycles $\longleftrightarrow$ sym. spectrum

Theorem (Bernasconi & Codenotti, '00)

Assume $f(\mathbf{0}) = 0$ & Γ_f connected. Then Γ_f is bipartite if and only if $\mathbb{F}_2^n - \Omega_f$ contains a subspace of dimension $n-1$.

Theorem (P.S. '07)

If f is bent, then Γ_f is not bipartite. In fact, if Γ_f is triangle-free (no paths of the form $xyzx$, where the vertices x, y, z are distinct), then f is not bent.

- Converse not true:

$$f(\mathbf{x}) = x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6 \oplus x_5x_6x_1 \oplus x_6x_1x_2$$

Γ_f has plenty of triangles, but f is not bent.

bipartite $\longleftrightarrow$ no odd length cycles $\longleftrightarrow$ sym. spectrum

Theorem (Bernasconi & Codenotti, '00)

Assume $f(\mathbf{0}) = 0$ & Γ_f connected. Then Γ_f is bipartite if and only if $\mathbb{F}_2^n - \Omega_f$ contains a subspace of dimension $n-1$.

Theorem (P.S. '07)

If f is bent, then Γ_f is not bipartite. In fact, if Γ_f is triangle-free (no paths of the form $xyzx$, where the vertices x, y, z are distinct), then f is not bent.

- Converse not true:

$$f(\mathbf{x}) = x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6 \oplus x_5x_6x_1 \oplus x_6x_1x_2$$

Γ_f has plenty of triangles, but f is not bent.

Nagy graphs and homogeneous bent functions

Some results on homogeneous bent B.f.

- On $\mathbb{F}_2^6$, there are 2^{20} homogeneous B.f. of degree 3 (meaning all terms in ANF of degree 3)
- Among these, there are 30 homogeneous **bent** B.f. with a representative:

  $x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6$

  which is equivalent to

  Rothaus: $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$
- Qu-Seberry-Pieprzyk (2000): *There are* $> 30^n\binom{6n}{6}$ *homogeneous bent B.f. on* $\mathbb{F}_2^{6n}$.

Some results on homogeneous bent B.f.

- On $\mathbb{F}_2^6$, there are 2^{20} homogeneous B.f. of degree 3 (meaning all terms in ANF of degree 3)

- Among these, there are 30 homogeneous **bent** B.f. with a representative:

  $x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6$
  which is equivalent to

  Rothaus: $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$
- Qu-Seberry-Pieprzyk (2000): *There are* $> 30^n\binom{6n}{6}$

  homogeneous bent B.f. on $\mathbb{F}_2^{6n}$.

Nonexistence results

Theorem (Xia-Seberry-Pieprzyk-Charnes (2004))

Maximum degree n is never attained by homogeneous bent functions on $\mathbb{F}_2^{2n}$.

Theorem (Meng-Zhang-Yang-Cui (2007))

For any k, there is N (least integer satisfying $2^{N-1} > \sum_{i=0}^{k+1} \binom{N+1}{i}$) such that there are no homogeneous bent B.f. of degree $\geq n-k$ on $\mathbb{F}_2^{2n}$, $n \geq N$.

- Let $k = 0$. Then $N = 4$ is the least integer with $2^{N-1} > \binom{N+1}{0} + \binom{N+1}{1}$. Xia et al.'s result follows immediately.

Nonexistence results

Theorem (Xia-Seberry-Pieprzyk-Charnes (2004))

Maximum degree n is never attained by homogeneous bent functions on $\mathbb{F}_2^{2n}$.

Theorem (Meng-Zhang-Yang-Cui (2007))

For any k, there is N (least integer satisfying $2^{N-1} > \sum_{i=0}^{k+1} \binom{N+1}{i}$) such that there are no homogeneous bent B.f. of degree $\geq n-k$ on $\mathbb{F}_2^{2n}$, $n \geq N$.

- Let $k = 0$. Then $N = 4$ is the least integer with $2^{N-1} > \binom{N+1}{0} + \binom{N+1}{1}$. Xia et al.'s result follows immediately.

Nonexistence results

Theorem (Xia-Seberry-Pieprzyk-Charnes (2004))

Maximum degree n is never attained by homogeneous bent functions on $\mathbb{F}_2^{2n}$.

Theorem (Meng-Zhang-Yang-Cui (2007))

For any k, there is N (least integer satisfying $2^{N-1} > \sum_{i=0}^{k+1} \binom{N+1}{i}$) such that there are no homogeneous bent B.f. of degree $\geq n-k$ on $\mathbb{F}_2^{2n}$, $n \geq N$.

- Let $k = 0$. Then $N = 4$ is the least integer with $2^{N-1} > \binom{N+1}{0} + \binom{N+1}{1}$. Xia et al.'s result follows immediately.

Existence conjectures

Conjecture (Meng-Zhang-Yang-Cui (2007))

For any $k > 1$, there exists N s.t. for any $n > N$, there exist homogeneous bent functions of degree k on $\mathbb{F}_2^{2n}$.

- Perhaps we can answer the following "easier" question:

Research Question (P.S. 2007)

For any k, find a homogeneous bent function of degree k, in some dimension.

Existence conjectures

Conjecture (Meng-Zhang-Yang-Cui (2007))

For any $k > 1$, there exists N s.t. for any $n > N$, there exist homogeneous bent functions of degree k on $\mathbb{F}_2^{2n}$.

- Perhaps we can answer the following "easier" question:

Research Question (P.S. 2007)

For any k, find a homogeneous bent function of degree k, in some dimension.

Further Restrictions: invariance under a group of transformations

The bent functions found by Qu et al.'s arise as invariants under the action of the symmetric group on four letters; using invariant theory they construct cubic homogeneous bent functions in 8, 10, and 12 variables.

Definition (Nagy Graph)

Let $\Gamma_{(n,k)}$ be the graph whose vertices correspond to the $\binom{n}{k}$ unordered subsets of size k of a set $\{1, \ldots, n\}$. Two vertices of $\Gamma_{(n,k)}$ are joined by an edge whenever the corresponding k-sets intersect in a subset of size one.

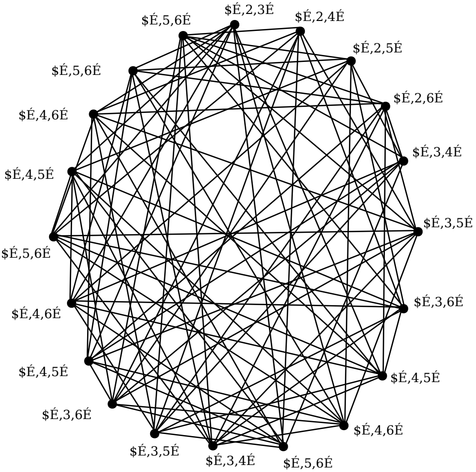
Further Restrictions: invariance under a group of transformations

The bent functions found by Qu et al.'s arise as invariants under the action of the symmetric group on four letters; using invariant theory they construct cubic homogeneous bent functions in 8, 10, and 12 variables.

Definition (Nagy Graph)

Let $\Gamma_{(n,k)}$ be the graph whose vertices correspond to the $\binom{n}{k}$ unordered subsets of size k of a set $\{1, \ldots, n\}$. Two vertices of $\Gamma_{(n,k)}$ are joined by an edge whenever the corresponding k-sets intersect in a subset of size one.

Nagy graph $\Gamma_{(6,3)}$



Cliques in the Nagy graph $\Gamma_{(6,3)}$

- A *clique* in an undirected graph is a complete subgraph (subset of vertices s.t. any two vertices are connected)
- *Maximal clique*: not strictly contained in a bigger one;
- *Maximum clique*: largest complete subgraph;
- *Clique number*: the order of the maximum clique in a graph; denoted by $\omega(G)$.
- Finding whether there is a clique of a given size in a graph (*the clique problem*) is NP-complete.

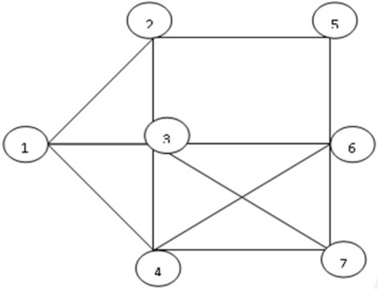
Cliques in the Nagy graph $\Gamma_{(6,3)}$

- A *clique* in an undirected graph is a complete subgraph (subset of vertices s.t. any two vertices are connected)
- *Maximal clique*: not strictly contained in a bigger one;
- *Maximum clique*: largest complete subgraph;
- *Clique number*: the order of the maximum clique in a graph; denoted by $\omega(G)$.
- Finding whether there is a clique of a given size in a graph (*the clique problem*) is NP-complete.

Cliques in the Nagy graph $\Gamma_{(6,3)}$

- A *clique* in an undirected graph is a complete subgraph (subset of vertices s.t. any two vertices are connected)
- *Maximal clique*: not strictly contained in a bigger one;
- *Maximum clique*: largest complete subgraph;
- *Clique number*: the order of the maximum clique in a graph; denoted by $\omega(G)$.
- Finding whether there is a clique of a given size in a graph (*the clique problem*) is NP-complete.

Maximum vs. maximal clique example



Cliques of K_3: {1, 2, 3}, {1, 3, 4},
{3. 4, 6}, {3, 4, 7},
{3, 6, 7}, {4, 6, 7}
Clique of K_4: {3, 4, 6, 7}

Maximal cliques: {1, 2, 3},
{1, 3, 4},
{3, 4, 6, 7}

Maximum clique with : $\omega(G) = 4$:
{3, 4, 6, 7}

A graph *G* and its nontrivial cliques, maximal cliques and maximum clique.

Cliques and Homogeneous Bent Functions

Theorem (Charnes-Rötteler-Beth (2002))

The thirty homogeneous bent functions in six variables listed by Qu et al. are in one to one correspondence with the complements of the 30 *(maximum) cliques of* $\Gamma_{(6,3)}$.

Proposed questions!

- It is unknown whether there are quartic/quintic/etc. homogeneous bent functions.
- I propose to look at the complements of the maximal cliques of the Nagy graph $\Gamma_{(10,4)}, \Gamma_{(12,4)}$. Do the same for $\Gamma_{(12,5)}, \Gamma_{(14,5)}$.
- Can one find efficiently a (all) clique(s) in $\Gamma_{(2n,k)}$, $k < n$?
- Not a trivial matter, I suspect: for instance, $\Gamma_{(10,4)}$ has 210 vertices; $\Gamma_{(12,5)}$ has 792 vertices;
- Modify Nagy graphs by constructing edges between tuples overlapping in two (or more indices) and investigate these issues.

Proposed questions!

- It is unknown whether there are quartic/quintic/etc. homogeneous bent functions.
- I propose to look at the complements of the maximal cliques of the Nagy graph $\Gamma_{(10,4)}, \Gamma_{(12,4)}$. Do the same for $\Gamma_{(12,5)}, \Gamma_{(14,5)}$.
- Can one find efficiently a (all) clique(s) in $\Gamma_{(2n,k)}$, $k < n$?
- Not a trivial matter, I suspect: for instance, $\Gamma_{(10,4)}$ has 210 vertices; $\Gamma_{(12,5)}$ has 792 vertices;
- Modify Nagy graphs by constructing edges between tuples overlapping in two (or more indices) and investigate these issues.

Proposed questions!

- It is unknown whether there are quartic/quintic/etc. homogeneous bent functions.
- I propose to look at the complements of the maximal cliques of the Nagy graph $\Gamma_{(10,4)}, \Gamma_{(12,4)}$. Do the same for $\Gamma_{(12,5)}, \Gamma_{(14,5)}$.
- Can one find efficiently a (all) clique(s) in $\Gamma_{(2n,k)}$, $k < n$?
- Not a trivial matter, I suspect: for instance, $\Gamma_{(10,4)}$ has 210 vertices; $\Gamma_{(12,5)}$ has 792 vertices;
- Modify Nagy graphs by constructing edges between tuples overlapping in two (or more indices) and investigate these issues.

Proposed questions!

- It is unknown whether there are quartic/quintic/etc. homogeneous bent functions.
- I propose to look at the complements of the maximal cliques of the Nagy graph $\Gamma_{(10,4)}, \Gamma_{(12,4)}$. Do the same for $\Gamma_{(12,5)}, \Gamma_{(14,5)}$.
- Can one find efficiently a (all) clique(s) in $\Gamma_{(2n,k)}$, $k < n$?
- Not a trivial matter, I suspect: for instance, $\Gamma_{(10,4)}$ has 210 vertices; $\Gamma_{(12,5)}$ has 792 vertices;
- Modify Nagy graphs by constructing edges between tuples overlapping in two (or more indices) and investigate these issues.

Proposed questions!

- It is unknown whether there are quartic/quintic/etc. homogeneous bent functions.
- I propose to look at the complements of the maximal cliques of the Nagy graph $\Gamma_{(10,4)}, \Gamma_{(12,4)}$. Do the same for $\Gamma_{(12,5)}, \Gamma_{(14,5)}$.
- Can one find efficiently a (all) clique(s) in $\Gamma_{(2n,k)}$, $k < n$?
- Not a trivial matter, I suspect: for instance, $\Gamma_{(10,4)}$ has 210 vertices; $\Gamma_{(12,5)}$ has 792 vertices;
- Modify Nagy graphs by constructing edges between tuples overlapping in two (or more indices) and investigate these issues.

References I

C. Bey, G. M. Kyureghyan, *On Boolean functions with the sum of every two of them being bent*, Des. Codes Cryptogr. 49 (2008), 341–346.

C. Carlet, *Two new classes of bent functions*, Adv. in Crypt. – Eurocrypt'93, LNCS 765 (1994), Springer–Verlag, 77–101.

C. Carlet, Boolean functions for cryptography and error correcting codes. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

C. Carlet, Vectorial Boolean functions for cryptography. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

C. Carlet, *Generalized partial spreads*, IEEE Trans. Inform. Theory 41((1995), 1482–1487.

C. Carlet, P. Guillot *A characterization of binary bent functions*, J. Combin. Theory (A) 76(2) (1996), 328–335.

C. Carlet, P. Guillot, *An alternate characterization of the bentness of binary functions, with uniqueness*, Des. Codes Cryptography 14(2) (1998), 133–140.

T. W. Cusick, P. Stănică, Cryptographic Boolean functions and Applications, Elsevier–Academic Press, 2009.

L. E. Danielsen, T. A. Gulliver and M. G. Parker, *Aperiodic Propagation Criteria for Boolean Functions*, Inform. Comput. 204:5 (2006), 741–770.

References II

J. F. Dillon, *Elementary Hadamard difference sets*, Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, 1975, 237–249.

H. Dobbertin, *Construction of bent functions and balanced Boolean functions with high nonlinearity*, In Fast Software Encryption (Workshop on Cryptographic Algorithms), Leuven 1994 (1995), LNCS 1008, Springer-Verlag, 61–74.

H. Dobbertin, G. Leander, *Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions*, Des. Codes Cryptography 49 (2008), 3–22.

P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory (A) 40 (1985), 90–107.

T.Y. Lam, K.H. Leung, *On vanishing sums of roots of unity*, J. Algebra 224 (2000), no. 1, 91–109.

R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1983.

F. J. MacWilliams, N. J. A. Sloane, The theory of error–correcting codes, North-Holland, Amsterdam, 1977.

M. G. Parker, A. Pott, *On Boolean functions which are bent and negabent*. In: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (eds.), SSC 2007, LNCS 4893 (2007), Springer, Heidelberg, 9–23.

M. G. Parker, A. Pott, personal communications.

C. Riera, M. G. Parker, *One and two-variable interlace polynomials: A spectral interpretation*, Proc. of WCC 2005, LNCS 3969 (2006), Springer, Heidelberg, 397–411.

References III

C. Riera, M. G. Parker, *Generalized bent criteria for Boolean functions*, IEEE Trans. Inform. Theory 52:9 (2006), 4142–4159.

O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory Series A 20 (1976), 300–305.

P. Sarkar, S. Maitra, *Cross–Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes*, Theory Comput. Systems 35 (2002), 39–57.

S. Sarkar, *On the symmetric negabent Boolean functions*, Indocrypt 2009, LNCS 5922 (2009), 136–143.

P. Savicky, *On the bent Boolean functions that are symmetric*, European J. Comb. 15 (1994), 407–410.

K. U. Schmidt, M. G. Parker, A. Pott, *Negabent functions in the Maiorana–McFarland class*. In: S.W. Golomb, M.G. Parker, A. Pott, A. Winterhof (eds.), SETA 2008, LNCS 5203 (2008), Springer, Heidelberg, 390–402.

Kai-Uwe Schmidt, *Quaternary Constant-Amplitude Codes for Multicode CDMA*, IEEE Transactions on Information Theory Volume 55 Issue 4, 2009, 1824–1832.

K-U. Schmidt, *Quaternary Constant-Amplitude Codes for Multicode CDMA*, IEEE International Symposium on Information Theory, ISIT'2007 (Nice, France, June 24–29, 2007), 2781–2785; available at http://arxiv.org/abs/cs.IT/0611162.

P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, http://eprint.iacr.org/2009/544.pdf; see also, Prikl. Diskr. Mat. 1 (2009), 16–18.

References IV

P. Stanica, S. Gangopadhyay, A. Chaturvedi, A. Kar Gangopadhyay, S. Maitra, *Nega-Hadamard transform, bent and negabent functions*, Sequences and Their Applications – SETA 2010 (C. Carlet and A. Pott, eds.), LNCS 6338 (2010), 359–372.

P. Stanica, S. Gangopadhyay, B. K. Singh, *Some Results Concerning Generalized Bent Functions*, http://eprint.iacr.org/2011/290.pdf.

P. Stanica, T. Martinsen, *Octal Bent Generalized Boolean Functions*, http://eprint.iacr.org/2011/089.pdf.

P. Stanica, T. Martinsen, S. Gangopadhyay, B. K. Singh, *Bent and Generalized Bent Boolean Functions*, manuscript, 2011.

Y. Zhao, H. Li, *On bent functions with some symmetric properties*, Discrete Appl. Math. 154 (2006), 2537–2543.