Bent functions, difference sets and strongly regular graphs

Wilfried Meidl

Sabancı University

December 1, 2013

- Bent Functions, Definition, Properties
- Bent Functions and
  - Difference Sets
  - Strongly Regular Graphs
- A Construction of Bent Functions
- Interpretation with Difference Sets
- Graph Interpretation

Walsh (Fourier) Transform

Definition

p: a prime

$f : V_n \longrightarrow \mathbb{F}_p$

For each $b \in V_n$,

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x) - <b,x>}, \quad \epsilon_p = e^{2\pi i/p}.$$

Remark

For $V_n = \mathbb{F}_p^n$, $< b, x >= b \cdot x$, for $V_n = \mathbb{F}_{p^n}$, $< b, x >= \mathrm{Tr_n}(bx)$.

Walsh (Fourier) Transform

Definition

p: a prime

$f : V_n \longrightarrow \mathbb{F}_p$

For each $b \in V_n$,

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x) - <b,x>}, \quad \epsilon_p = e^{2\pi i/p}.$$

Remark

For $V_n = \mathbb{F}_p^n$, $< b, x >= b \cdot x$, for $V_n = \mathbb{F}_{p^n}$, $< b, x >= \mathrm{Tr_n}(bx)$.

Definition

$|\widehat{f}(b)| = p^{n/2}$ for all $b \in V_n \Rightarrow f$ is a bent function.

Walsh (Fourier) Transform

Definition

p: a prime

$f : V_n \longrightarrow \mathbb{F}_p$

For each $b \in V_n$,

$$\widehat{f}(b) = \sum_{x \in V_n} \epsilon_p^{f(x) - <b,x>}, \quad \epsilon_p = e^{2\pi i/p}.$$

Remark

For $V_n = \mathbb{F}_p^n$, $< b, x >= b \cdot x$, for $V_n = \mathbb{F}_{p^n}$, $< b, x >= \mathrm{Tr_n}(bx)$.

Definition

$|\widehat{f}(b)| = p^{n/2}$ for all $b \in V_n \Rightarrow f$ is a bent function. Alternatively, $f : V_n \longrightarrow \mathbb{F}_p$ is bent if and only if the derivative of f in direction a

$$D_a f(x) = f(x + a) - f(x)$$

is balanced for all $a \in V_n$, $a \neq 0$.

Walsh coefficients $\widehat{f}(b)$

- For Boolean bent functions

$$\widehat{f}(b) = \pm 2^{n/2}.$$

- (Kumar-Scholz-Welch 1985) For p-ary bent functions,

$$\widehat{f}(b) = \begin{cases} \pm p^{n/2}\epsilon_p^{f^*(b)} & : \quad n \text{ even or } n \text{ odd and } p \equiv 1 \bmod 4 \\ \pm i p^{n/2}\epsilon_p^{f^*(b)} & : \quad n \text{ odd and } p \equiv 3 \bmod 4, \end{cases}$$

for a function $f^* : V_n \to \mathbb{F}_p$, the so called *dual* function of f.

Regularity of Bent Functions

Let $f : V_n \to \mathbb{F}_p$ be a bent function. Then

$$\widehat{f}(b) = \zeta \; p^{n/2} \epsilon_p^{f^*(b)}, \text{ for all } b \in V_n.$$

ζ can only be ± 1 or $\pm i$.

- f is called regular if for all $b \in V_n, \zeta = 1$.
- f is called weakly regular if, for all $b \in V_n$, ζ is fixed.
- If ζ changes with b then f is called not weakly regular.

Plateaued Functions, Partially Bent Functions

Definition

$f : V_n \to \mathbb{F}_p$ is called s-plateaued if, for all $b \in V_n$, $|\widehat{f}(b)| = p^{\frac{n+s}{2}}$ or 0.

Plateaued Functions, Partially Bent Functions

Definition

$f : V_n \to \mathbb{F}_p$ is called s-plateaued if, for all $b \in V_n$, $|\widehat{f}(b)| = p^{\frac{n+s}{2}}$ or 0.

$f : V_n \to \mathbb{F}_p$ is called partially bent if, for all $a \in V_n$, $D_a f(x)$ is balanced or constant.

Plateaued Functions, Partially Bent Functions

Definition

$f : V_n \to \mathbb{F}_p$ is called s-plateaued if, for all $b \in V_n$, $|\widehat{f}(b)| = p^{\frac{n+s}{2}}$ or 0.

$f : V_n \to \mathbb{F}_p$ is called partially bent if, for all $a \in V_n$, $D_a f(x)$ is balanced or constant.

Fact:

The set of elements $a \in V_n$ for which $D_a f(x)$ is constant is a subspace of V_n, the linear space Λ of f.

Partially bent functions are s-plateaued, s is the dimension of Λ. We call f then s-partially bent.

Boolean Bent Functions and Difference Sets

Recall:
Let G be a finite (abelian) group of order ν. A subset D of G of cardinality k is called a (ν, k, λ)-difference set in G if every element $g \in G$, different from the identity, can be written as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly λ different ways.

Hadamard difference set in elementary abelian 2-group:
$(\nu, k, \lambda) = (2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$.

Theorem
A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a bent function if and only if $D = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ is a Hadamard difference set in $\mathbb{F}_2^n$.

Bent Functions and Relative Difference Sets

Let G be a group of order mn and let N be a subgroup of order n. A k-subset R of G is called an (m, n, k, λ)-relative difference set in G relative to N if every element $g \in G \setminus N$ can be represented in exactly λ ways in the form $r_1 - r_2$, $r_1, r_2 \in R$, and no non-identity element in N has such a representation.

Theorem

For a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ let $R = \{(x, f(x)) \mid x \in \mathbb{F}_p^n\} \subset \mathbb{F}_p^n \times \mathbb{F}_p$. The set R is a (p^n, p, p^n, p^{n-1})-relative difference set in $\mathbb{F}_p^n \times \mathbb{F}_p$ (relative to $\mathbb{F}_p$) if and only if f is a bent function.

Bent functions and strongly regular graphs

For a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, p odd, let

$$\begin{aligned} D_0 &= \{x \in \mathbb{F}_p^n \mid f(x) = 0\}, \\ D_S &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonzero square in } \mathbb{F}_p\}, \\ D_N &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonsquare } \mathbb{F}_p\}. \end{aligned}$$

Bent functions and strongly regular graphs

For a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, p odd, let

$$\begin{aligned} D_0 &= \{x \in \mathbb{F}_p^n \mid f(x) = 0\}, \\ D_S &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonzero square in } \mathbb{F}_p\}, \\ D_N &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonsquare } \mathbb{F}_p\}. \end{aligned}$$

Theorem

(Yin Tan et al. 2010/2011) For an odd prime p let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a weakly regular bent function in even dimension n, with $f(0) = 0$, for which there exists a constant k with $\gcd(k-1, p-1) = 1$ such that for all $t \in \mathbb{F}_p$

$$f(tx) = t^k f(x).$$

Then the Cayley graphs of the sets $D_0 \setminus \{0\}$, D_S, D_N are strongly regular graphs.

Bent functions and strongly regular graphs

For a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, p odd, let

$$
\begin{aligned}
D_0 &= \{x \in \mathbb{F}_p^n \mid f(x) = 0\}, \\
D_S &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonzero square in } \mathbb{F}_p\}, \\
D_N &= \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonsquare } \mathbb{F}_p\}.
\end{aligned}
$$

Theorem

(Yin Tan et al. 2010/2011) For an odd prime p let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a weakly regular bent function in even dimension n, with $f(0) = 0$, for which there exists a constant k with $\gcd(k-1, p-1) = 1$ such that for all $t \in \mathbb{F}_p$

$$f(tx) = t^k f(x).$$

Then the Cayley graphs of the sets $D_0 \setminus \{0\}$, D_S, D_N are strongly regular graphs.

Vertices: Elements of $\mathbb{F}_p^n$. The vertices x, y are adjacent if $f(x-y) \in D_0 \setminus \{0\}$ ($f(x-y) \in D_S$, $f(x-y) \in D_N$).

A construction of bent functions

Theorem (Çeşmelioğlu, McGuire, M. 2012)

For each $y = (y_1, y_2, \ldots, y_s) \in \mathbb{F}_p^s$, *let* $f_y(x) : \mathbb{F}_p^m \to \mathbb{F}_p$ *be an s-plateaued function. If* $supp(\widehat{f_y}) \cap supp(\widehat{f_{\bar{y}}}) = \emptyset$ *for* $y, \bar{y} \in \mathbb{F}_p^s, y \neq \bar{y}$, *then the function* $F(x, y_1, y_2, \ldots, y_s)$ *from* $\mathbb{F}_p^{m+s}$ *to* $\mathbb{F}_p$ *defined by*

$$F(x, y_1, y_2, \ldots, y_s) = f_{y_1, y_2, \ldots, y_s}(x)$$

is bent.

A construction of bent functions

Theorem (Çeşmelioğlu, McGuire, M. 2012)

For each $y = (y_1, y_2, \dots, y_s) \in \mathbb{F}_p^s$, *let* $f_y(x) : \mathbb{F}_p^m \to \mathbb{F}_p$ *be an s-plateaued function. If* $supp(\widehat{f_y}) \cap supp(\widehat{f_{\bar{y}}}) = \emptyset$ *for* $y, \bar{y} \in \mathbb{F}_p^s, y \neq \bar{y}$, *then the function* $F(x, y_1, y_2, \dots, y_s)$ *from* $\mathbb{F}_p^{m+s}$ *to* $\mathbb{F}_p$ *defined by*

$$F(x, y_1, y_2, \dots, y_s) = f_{y_1, y_2, \dots, y_s}(x)$$

is bent.

For $p = 2$, $s = 1$ (Leander, McGuire 2009; Charpin et. al. 2005)

$$F(x, y) = yf_1(x) + (y + 1)f_0(x),$$

i.e.

$$F(x, y) = \begin{cases} f_0(x) & : \quad y = 0, \\ f_1(x) & : \quad y = 1. \end{cases}$$

Proof

For $a \in \mathbb{F}_p^m$, $b \in \mathbb{F}_p^s$, and putting $y = (y_1, \ldots, y_s)$, the Walsh transform $\widehat{F}$ of F at (a, b) is

$$\begin{aligned}\widehat{F}(a,b) &= \sum_{x \in \mathbb{F}_p^m, y \in \mathbb{F}_p^s} \epsilon_p^{F(x,y) - a \cdot x - b \cdot y} = \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-b \cdot y} \sum_{x \in \mathbb{F}_p^m} \epsilon_p^{F(x,y) - a \cdot x} \\ &= \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-b \cdot y} \sum_{x \in \mathbb{F}_p^m} \epsilon_p^{f_y(x) - a \cdot x} = \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-b \cdot y} \widehat{f_y}(a).\end{aligned}$$

As each $a \in \mathbb{F}_p^m$ belongs to the support of exactly one $\widehat{f_y}$, $y \in \mathbb{F}_p^s$, for this y we have $\left|\widehat{F}(a,b)\right| = |\epsilon_p^{-b \cdot y} \widehat{f_y}(a)| = p^{\frac{m+s}{2}}$. □

Special case

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function.
Then f seen as a function from $\mathbb{F}_p^n \times \mathbb{F}_p^s$ to $\mathbb{F}_p$, is s-partially bent with linear space $\mathbb{F}_p^s$.

Special case

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function.
Then f seen as a function from $\mathbb{F}_p^n \times \mathbb{F}_p^s$ to $\mathbb{F}_p$, is s-partially bent with linear space $\mathbb{F}_p^s$.

If $\{f_y \ : \ y \in \mathbb{F}_p^s\}$ is a set of bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ then the set of functions in $m = n + s$ variables $\{f_y(x) + x_{n+1}y_1 + \cdots + x_{n+s}y_s \ : \ y \in \mathbb{F}_p^s\}$ is a set of p^s s-partially bent functions with Walsh transforms with pairwise disjoint supports.

Special case

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function.
Then f seen as a function from $\mathbb{F}_p^n \times \mathbb{F}_p^s$ to $\mathbb{F}_p$, is s-partially bent with linear space $\mathbb{F}_p^s$.

If $\{f_y \ : \ y \in \mathbb{F}_p^s\}$ is a set of bent functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ then the set of functions in $m = n + s$ variables
$\{f_y(x) + x_{n+1}y_1 + \cdots + x_{n+s}y_s \ : \ y \in \mathbb{F}_p^s\}$ is a set of p^s s-partially bent functions with Walsh transforms with pairwise disjoint supports.

With $\underline{x} = (x_1, \ldots, x_n)$, $\bar{x} = (x_{n+1}, \ldots, x_{n+s})$, the function

$$F(\underline{x}, \bar{x}, y) = f_y(\underline{x}) + x_{n+1}y_1 + \cdots + x_{n+s}y_s := g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})$$

is an example for the construction of a bent function.

Applications

- Construction of infinite classes of not weakly regular bent functions (Çeşmelioğlu, McGuire, M., JCTA. 2012)

Applications

- Construction of infinite classes of not weakly regular bent functions (Çeşmelioğlu, McGuire, M., JCTA. 2012)
- Bent functions (ternary) of maximal algebraic degree (Çeşmelioğlu, M., IEEE Trans. Inform. Theory 2012, DCC 2013)

Applications

- Construction of infinite classes of not weakly regular bent functions (Çeşmelioğlu, McGuire, M., JCTA. 2012)
- Bent functions (ternary) of maximal algebraic degree (Çeşmelioğlu, M., IEEE Trans. Inform. Theory 2012, DCC 2013)
- Construction of bent functions of high algebraic degree and its dual simultaneously, self-dual bent functions (Çeşmelioğlu, Pott, M., Adv. Math. Comm. 2013)

Difference set interpretation

Bent function $F : \mathbb{F}_p^{n+2s} \to \mathbb{F}_p$:
$F(\underline{x}, \bar{x}, y_1, \ldots, y_s) = g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})$.

$$R = \{(\underline{x}, \bar{x}, y_1, \ldots, y_s, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s, y_i \in \mathbb{F}_p\}.$$

$(p^{n+2s}, p, p^{n+2s}, p^{n+2s-1})$-relative difference set in $\mathbb{F}_p^{n+2s} \times \mathbb{F}_p$.

Difference set interpretation

Bent function $F : \mathbb{F}_p^{n+2s} \to \mathbb{F}_p$:
$F(\underline{x}, \bar{x}, y_1, \ldots, y_s) = g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})$.

$$R = \{(\underline{x}, \bar{x}, y_1, \ldots, y_s, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s, y_i \in \mathbb{F}_p\}.$$

$(p^{n+2s}, p, p^{n+2s}, p^{n+2s-1})$-relative difference set in $\mathbb{F}_p^{n+2s} \times \mathbb{F}_p$.

Analog sets for the s-partially bent functions $g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})$:

$$R_{(y_1,\ldots,y_s)} = \{(\underline{x}, \bar{x}, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s\},$$

subset of $\mathbb{F}_p^n \times \mathbb{F}_p^s \times \mathbb{F}_p \simeq \mathbb{F}_p^{n+s+1}$.

Difference set interpretation

$$R = \{(\underline{x}, \bar{x}, y_1, \ldots, y_s, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s, y_i \in \mathbb{F}_p\}$$

$$R_{(y_1,\ldots,y_s)} = \{(\underline{x}, \bar{x}, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s\}$$

Obtaining the relative difference set R from the sets $R_{(y_1,\ldots,y_s)}$:

$$R = \bigcup_{(y_1,\ldots,y_s)\in\mathbb{F}_p^s} (y_1, \ldots, y_s) + R_{(y_1,\ldots,y_s)}.$$

Note, $(y_1, \ldots, y_s) = (0, \ldots, 0, y_1, \ldots, y_s, 0)$ are coset representatives of $\mathbb{F}_p^{n+s+1}$ in $\mathbb{F}_p^{n+2s+1}$.

Difference set interpretation

$$R = \{(\underline{x}, \bar{x}, y_1, \ldots, y_s, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s, y_i \in \mathbb{F}_p\}$$

$$R_{(y_1,\ldots,y_s)} = \{(\underline{x}, \bar{x}, g_{(y_1,\ldots,y_s)}(\underline{x}, \bar{x})) \ : \ \underline{x} \in \mathbb{F}_p^n, \bar{x} \in \mathbb{F}_p^s\}$$

Obtaining the relative difference set R from the sets $R_{(y_1,\ldots,y_s)}$:

$$R = \bigcup_{(y_1,\ldots,y_s)\in\mathbb{F}_p^s} (y_1, \ldots, y_s) + R_{(y_1,\ldots,y_s)}.$$

Note, $(y_1, \ldots, y_s) = (0, \ldots, 0, y_1, \ldots, y_s, 0)$ are coset representatives of $\mathbb{F}_p^{n+s+1}$ in $\mathbb{F}_p^{n+2s+1}$.

One can take any set of coset representatives $\{a_y \mid y \in \mathbb{F}_p^s\}$ of $\mathbb{F}_p^n \times \mathbb{F}_p^{s+1}$ in $\mathbb{F}_p^n \times \mathbb{F}_p^{2s+1}$ and form

$$R = \bigcup_{y\in\mathbb{F}_p^s} a_y + R_y.$$

Comparison with Davis, Jedwab 1997

$R_{(y_1,\ldots,y_s)} \longleftrightarrow$ building block in $G = \mathbb{F}_p^{n+s+1}$:
"A subset R of a group G is called a building block in G if the magnitude of all nonprincipal character sums over R is either 0 or m."

Comparison with Davis, Jedwab 1997

$R_{(y_1,\ldots,y_s)} \longleftrightarrow$ building block in $G = \mathbb{F}_p^{n+s+1}$:
"A subset R of a group G is called a building block in G if the magnitude of all nonprincipal character sums over R is either 0 or m."
The collection of the sets $R_{(y_1,\ldots,y_s)}$ forms an $(a,m,t) = (p^{n+s}, p^{(n+2s)/2}, p^s)$ building set in $G = \mathbb{F}_p^{n+s+1}$ relative to the subgroup $U = \{0\} \times \{0\} \times \cdots \times \{0\} \times \mathbb{F}_p$ of $\mathbb{F}_p^{n+s+1}$:
"An (a,m,t) building set in G relative to U is a collection of t building blocks with magnitude m in G, each containing a elements, such that for every nonprincipal character χ of G, the following holds:

1. *Exactly one of the building blocks has nonzero character sum if χ is nonprincipal on U.*
2. *If χ is principal on U, then character sums for all building blocks are equal to zero."*

Strongly Regular Graph Interpretation

Strongly Regular Graph Interpretation

Theorem (Çeşmelioğlu, M.)

Let $g_0, g_1 : \mathbb{F}_p^n \to \mathbb{F}_p$ *be two (distinct) bent functions in even dimension* n, $g_0(0) = g_1(0) = 0$ *such that*

- *both* g_0, g_1 *are regular, or both* g_0, g_1 *are weakly regular but not regular,*
- $g_i(tx) = t^k g_i(x)$ *for all* $t \in \mathbb{F}_p$ *and an integer* k *with* $\gcd(k-1, p-1) = 1$, $i = 0, 1$.

Then the function $F : \mathbb{F}_p^{n+2} \to \mathbb{F}_p$

$$F(x, y, z) = (g_1(x) - g_0(x))z^{p-1} + uyz^{k-1} + g_0(x),$$

for a non-zero element $u \in \mathbb{F}_p$ *is a weakly regular bent function satisfying* $F(t(x, y, z)) = t^k F(x, y, z)$ *for all* $t \in \mathbb{F}_p$.

Strongly Regular Graph Interpretation

Theorem (Çeşmelioğlu, M.)

Let $g_0, g_1 : \mathbb{F}_p^n \to \mathbb{F}_p$ *be two (distinct) bent functions in even dimension* n, $g_0(0) = g_1(0) = 0$ *such that*

- *both* g_0, g_1 *are regular, or both* g_0, g_1 *are weakly regular but not regular,*
- $g_i(tx) = t^k g_i(x)$ *for all* $t \in \mathbb{F}_p$ *and an integer* k *with* $\gcd(k-1, p-1) = 1$, $i = 0, 1$.

Then the function $F : \mathbb{F}_p^{n+2} \to \mathbb{F}_p$

$$F(x, y, z) = (g_1(x) - g_0(x))z^{p-1} + uyz^{k-1} + g_0(x),$$

for a non-zero element $u \in \mathbb{F}_p$ *is a weakly regular bent function satisfying* $F(t(x, y, z)) = t^k F(x, y, z)$ *for all* $t \in \mathbb{F}_p$.

$$F(x, y, a) = \begin{cases} g_0(x, y) = g_0(x) & : \quad a = 0, \\ g_1(x) + ua^{k-1}y & : \quad a \neq 0 \end{cases},$$

is a 1-partially bent function in $n + 1$ variables for every $a \in \mathbb{F}_p$.

Strongly Regular Graph Interpretation

Strongly regular graph for
$F(x, y, z) = (g_1(x) - g_0(x))z^{p-1} + uyz^{k-1} + g_0(x)$:

Set of vertices: $\mathbb{F}_p^{n+2} = \mathbb{F}_p^n \times \mathbb{F}_p \times \mathbb{F}_p$.

The vertices (x, y, z), (x_1, y_1, z_1) are adjacent if and only if $F(x - x_1, y - y_1, z - z_1)$ is a nonzero square (nonsquare, equal zero).

Strongly Regular Graph Interpretation

Strongly regular graph for
$F(x, y, z) = (g_1(x) - g_0(x))z^{p-1} + uyz^{k-1} + g_0(x)$:

Set of vertices: $\mathbb{F}_p^{n+2} = \mathbb{F}_p^n \times \mathbb{F}_p \times \mathbb{F}_p$.

The vertices (x, y, z), (x_1, y_1, z_1) are adjacent if and only if $F(x - x_1, y - y_1, z - z_1)$ is a nonzero square (nonsquare, equal zero).

Observation: Since $F(x - x_1, y - y_1, z - z_1) =$

$$\begin{cases} g_0(x - x_1) & : \quad z_1 = z, \\ g_1(x - x_1) + u(y - y_1)(z - z_1)^{k-1} & : \quad z_1 \neq z \end{cases},$$

Strongly Regular Graph Interpretation

Strongly regular graph for
$F(x,y,z) = (g_1(x) - g_0(x))z^{p-1} + uyz^{k-1} + g_0(x)$:

Set of vertices: $\mathbb{F}_p^{n+2} = \mathbb{F}_p^n \times \mathbb{F}_p \times \mathbb{F}_p$.

The vertices (x,y,z), (x_1,y_1,z_1) are adjacent if and only if $F(x-x_1, y-y_1, z-z_1)$ is a nonzero square (nonsquare, equal zero).

Observation: Since $F(x-x_1, y-y_1, z-z_1) =$

$$\begin{cases} g_0(x-x_1) & : \quad z_1 = z, \\ g_1(x-x_1) + u(y-y_1)(z-z_1)^{k-1} & : \quad z_1 \neq z \end{cases},$$

- (x,y,z), (x_1,y_1,z) are adjacent if and only if $g_0(x-x_1)$ is a nonzero square (nonsquare, equal zero), i.e. x and x_1 are adjacent in the strongly regular graph of g_0,

Strongly Regular Graph Interpretation

Strongly regular graph for
$F(x, y, z) = (g_1(x) - g_0(x))z^{p-1} + uyz^{k-1} + g_0(x)$:

Set of vertices: $\mathbb{F}_p^{n+2} = \mathbb{F}_p^n \times \mathbb{F}_p \times \mathbb{F}_p$.

The vertices (x, y, z), (x_1, y_1, z_1) are adjacent if and only if $F(x - x_1, y - y_1, z - z_1)$ is a nonzero square (nonsquare, equal zero).

Observation: Since $F(x - x_1, y - y_1, z - z_1) =$

$$\begin{cases} g_0(x - x_1) & : \quad z_1 = z, \\ g_1(x - x_1) + u(y - y_1)(z - z_1)^{k-1} & : \quad z_1 \neq z \end{cases},$$

- (x, y, z), (x_1, y_1, z) are adjacent if and only if $g_0(x - x_1)$ is a nonzero square (nonsquare, equal zero), i.e. x and x_1 are adjacent in the strongly regular graph of g_0,
- (x, y, z), (x_1, y_1, z_1), $z_1 \neq z$, are adjacent if and only if $g_1(x - x_1) + u(y - y_1)(z - z_1)^{k-1}$ is a nonzero square (nonsquare, equal zero).

Questions

- Find initial functions.
  Known examples: Quadratic functions,
  $f(x) = \mathrm{Tr_n}(x^{p^{3r}+p^{2r}-p^r+1} + x^2)$, $n = 4r$.
  For $p = 3$,
  $f(x) = \mathrm{Tr_n}(\alpha x^{(3^r+1)/2})$, $\gcd(r, 2n) = 1$, and
  $f(x) = \mathrm{Tr_n}(\alpha x^{t(3^r-1)})$, $f(x) = \mathrm{Tr_n}(\alpha x^{(3^r-1)/4+3^r+1})$,
  conditions on r, n, α.
  All for $k = 2$.
- Find functions for other k.
  Example: $f(x, y) = x_1 y_1^{k-1} + x_2 y_2^{k-1} + \cdots + x_m y_m^{k-1}$
  (homogeneous).
- Find homogeneous bent functions.