Combinatorics of $p$-ary Bent Functions

MIDN 1/C Steven Walsh

United States Naval Academy

25 April 2014
Objectives

- Introduction/Motivation
- Definitions
- Important Theorems
- Main Results: Connecting Bent Functions to Combinatorical Structures
- Conclusion
Introduction/Motivation

- Linear feedback shift register: a shift register in which inputs are linear functions of their previous states.
- Can be used to generate pseudo-random sequences that can be used as keystreams in a stream cipher system.
- Example: Fibonacci sequence (mod 2), defined by initial state \( s_0 = 0, s_1 = 1 \) and recursive function \( s_n = s_{n-1} + s_{n-2} \) \((0,1,1,2,3,5,8,13,21...) \rightarrow (0,1,0,1,1,0,1,1...)\)
- LFSRs can be broken using the Berlekamp-Massey algorithm.
Berlekamp-Massey algorithm

- For a binary LFSR with key length \( n \) and maximal length period \( 2^n - 1 \), only \( 2n \) consecutive terms of the sequence are required to determine the coefficients of the LFSR
- Example: Fibonacci sequence mod 2, key length is 2 and period is 3, so 4 digits are required to decode the LFSR

Example: choose a 4-bit subsequence (say, \((0,1,1,0)\)) and use the equation \( s_n = c_1 s_{n-1} + c_2 s_{n-2} \) to solve for \( c_1 \) and \( c_2 \) and thus, determine the key \((c_1, c_2)\):

\[
\begin{align*}
1 &= c_1(1) + c_2(0) \Rightarrow c_1 = 1 \\
0 &= c_1(1) + c_2(1) = 1(1) + c_2(1) \Rightarrow c_2 = 1
\end{align*}
\]
Implementing more secure cipher stream systems

LFSRs are very susceptible to decryption through various techniques, including Berlekamp-Massey algorithm and brute force attacks.

To construct more secure keystreams, utilize bent, or perfectly non-linear, functions:

- non-linearity will generate more random sequences
- resistant to linear cryptanalysis
Definitions and Examples
Walsh-Hadamard transform

For $f : GF(p)^n \to GF(p)$, the Walsh-Hadamard transform of $f$ is a complex-valued function on $GF(p)^n$ defined by:

$$W_f(u) = \sum_{x \in GF(p)^n} \zeta^{f(x) - \langle u, x \rangle}$$

where $\zeta = e^{2\pi i / p}$ (the $p$th root of unity).

$f : GF(p)^n \to GF(p)$ is bent if

$$|W_f(u)| = p^{n/2}$$

for all $u \in GF(p)^n$. 
Partial difference sets

- Let $G$ be a finite abelian group of order $v$
- Let $D$ be a subset of $G$ with cardinality $k$

$D$ is a $(v, k, \lambda)$-difference set if the multiset $\{d_1d_2^{-1} \mid d_1, d_2 \in D\}$ contains every non-identity element of $G$ exactly $\lambda$ times

$D$ is a $(v, k, \lambda, \mu)$-partial difference set (PDS) if the multiset $\{d_1d_2^{-1} \mid d_1, d_2 \in D\}$ contains every non-identity element of $D$ exactly $\lambda$ times and every non-identity element of $G \setminus D$ exactly $\mu$ times
Cayley graphs

Constructing a Cayley graph:

- Let $G$ be a group, let $D \subset G$ such that $1 \notin D$
- Let the vertices of the graph be elements of $G$
- Two vertices $g_1$ and $g_2$ are connected by a directed edge from $g_1$ to $g_2$ if $g_2 = dg_1$ for some $d \in D$

For a $(v, k, \lambda, \mu)$-PDS $D$, the Cayley graph $X(G, D)$ is a srg-$(v, k, \lambda, \mu)$ if:

- $X(G, D)$ has $v$ vertices such that each vertex is connected to $k$ other vertices
- Distinct vertices $g_1$ and $g_2$ share edges with either $\lambda$ or $\mu$ common vertices
Bent function correspondences

Two known ways to determine whether a function is bent (for $p = 2$)

- **Dillon correspondence**: $f : \text{GP}(2)^n \rightarrow \text{GF}(2)$ is bent if and only if the level curve
  \[ f^{-1}(1) = \{ v \in \text{GF}(2)^n | f(v) = 1 \} \]
  yields a difference set in $\text{GF}(2)^n$ with parameters
  $(v, k, \lambda) = (4m^2, 2m^2 \pm m, m^2 \pm m)$ for some integer $m$

- **Bernasconi correspondence**: $f : \text{GF}(2)^n \rightarrow \text{GF}(2)$ is bent if and only if the Cayley graph of $f$ is a srg-$\text{sg}(2^n, k, \lambda, \mu)$, where
  $\lambda = \mu$ and $k = |\{ v \in \text{GF}(2)^n | f(v) \neq 0 \}|$
Weighted partial difference sets

Let $G$ be a finite abelian multiplicative group of order $v$ and let $D$ be a subset of $G$ of cardinality $k$. Decompose $D$ into a union of disjoint subsets

$$D = D_1 \cup D_2 \cup \cdots \cup D_d$$

and assume $1 \notin D$. Let $|D_i| = k_i$. 
Weighted partial difference sets

$D$ is a weighted partial difference set (PDS) if the following properties hold:

- The multiset

$$D_iD_j^{-1} = \{d_1d_2^{-1} \mid d_1 \in D_i, d_2 \in D_j\}$$

represents every non-identity element of $D_l$ exactly $\lambda_{i,j,l}$ times and every non-identity element of $G \setminus D$ exactly $\mu_{i,j}$ times ($1 \leq i, j, l \leq d$)

- For each $i \in \{1, 2, \ldots, d\}$, $\exists j \in \{1, 2, \ldots, d\}$ such that $D_i^{-1} = D_j$ (if $D_i^{-1} = D_i$ for all $i$, then the weighted PDS is symmetric)
Weighted Cayley Graphs

Construction of a weighted Cayley graph $X_w(G, D)$ is similar to that of a standard Cayley graph:

- Let $G$ be a group, $D$ a subset of $G$
- Decompose $D$ into a union of subsets $D_1 \cup D_2 \cup \cdots \cup D_d$
- The vertices of the graph are the elements of $G$
- Two vertices $g_1$ and $g_2$ are connected by an edge of weight $k$ if $g_1 = dg_2$ for some $d \in D_k$
PDS Example

$G = GF(3)[x]/(x^2 + 1) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\} (GF(9), +)$

$D = \{1, 2, x, 2x\}$

$\{d_1 d_2^{-1} | d_1, d_2 \in D\} = \{0, 2, 1 + 2x, 1 + x, 0, 1, 2x + 2, x + 2, 0, x + 2, x + 1, 2x, 0, 2x + 2, 2x + 1, x\}$

So $D$ is a $(9,4,1,2)$ partial difference set.
Weighted PDS Example

- $G = GF(3)[x]/(x^2 + 1) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$ (additive group)

- $D_1 = \{1, 2\}, D_2 = \{x, 2x\}$

- $\{d_1 d_2^{-1} \mid d_1, d_2 \in D_1\} = \{0, 2, 0, 1\}$
- $\{d_1 d_2^{-1} \mid d_1 \in D_1, d_2 \in D_2\} = \{2x + 1, x + 1, x + 2, 2x + 2\}$
- $\{d_1 d_2^{-1} \mid d_1, d_2 \in D_2\} = \{0, 2x, 0, x\}$

- $\lambda_{1,1,1} = 1, \lambda_{1,1,2} = 0, \mu_{1,1} = 0$
- $\lambda_{1,2,1} = 0, \lambda_{1,2,2} = 0, \mu_{1,2} = 1$
- $\lambda_{2,2,1} = 0, \lambda_{2,2,2} = 1, \mu_{2,2} = 0$
Corresponding Cayley Graph
Using Level Curves as Weighted Partial Difference Sets

Let $f : GF(p)^n \to GF(p)$ be a function. One possible way to generate a weighted partial difference set is as follows:

- $G = GF(p)^n$
- $D_0 = \{0\}$
- $D_i = f^{-1}(i)$ for $i = 1, 2, ..., p - 1$
- $D_p = f^{-1}(0) - \{0\}$
Association schemes

- $S$ is a finite set
- $R_0, R_1, \ldots, R_d$ binary relations on $S$
- $R_0 = \{(x, x) \in S \times S | x \in S\}$
- $R_i^* = \{(x, y) \in S \times S | (y, x) \in R_i\}$

Then $(S, R_0, R_1, \ldots, R_d)$ is a $d$-class association scheme if:
- $S \times S = R_0 \cup R_1 \cup \cdots \cup R_d$, with $R_i \cap R_j = \emptyset$ for all $i \neq j$.
- For each $i$, $\exists j$ such that $R_i^* = R_j$
- For all $i, j$ and all $(x, y) \in S \times S$, define

$$p_{ij}(x, y) = |\{z \in S | (x, z) \in R_i, (z, y) \in R_j\}|.$$

For all $k$ and for all $(x, y) \in R_k$, $p_{ij}(x, y)$ is a constant, denoted $p_{ij}^k$. 

Let $G$ be a group with a weighted partial difference set

$D = D_1 \cup D_2 \cup \cdots \cup D_d$

Construct an association scheme as follows:

- $S = G$
- $R_0 = \{(g, g) \in G \times G \mid g \in G\}$
- $R_i = \{(g, h) \in G \times G \mid gh^{-1} \in D_i, g \neq h\}$ (for $i = 1, 2, \ldots, d$)
- $R_{d+1} = \{(g, h) \in G \times G \mid gh^{-1} \notin D, g \neq h\}$
Schur rings

- $G$ a finite abelian group
- $C_0, C_1, \ldots, C_d$ finite subsets of $G$
- identify each $C_i$ as a formal sum of its elements in $\mathbb{C}[G]$

The subalgebra of $\mathbb{C}[G]$ generated by $C_0, C_1, \ldots, C_d$ is a Schur ring if:

- $C_0 = \{1\}$, the singleton containing the identity
- $G = C_0 \cup C_1 \cup \cdots \cup C_d$, with $C_i \cap C_j = \emptyset$ for all $i \neq j$
- for each $i$, $\exists j$ such that $C_i^{-1} = C_j$
- for all $i, j$,

$$C_i \cdot C_j = \sum_{k=0}^{d} p_{ij}^k C_k,$$

for some integers $p_{ij}^k$
Schur ring example

Let $G = \{\zeta^k \mid k \in \mathbb{Z}, 0 \leq k \leq 5\}$, where $\zeta = e^{2\pi i/6}$

\[
D_0 = \{\zeta^0\} = \{1\}, \quad D_1 = \{\zeta^2, \zeta^4\}, \quad D_2 = \{\zeta, \zeta^3, \zeta^5\}
\]

\[
D_1 \cdot D_2 = (\zeta^2 + \zeta^4) \cdot (\zeta + \zeta^3 + \zeta^5)
\]
\[
= \zeta^3 + \zeta^5 + \zeta^7 + \zeta^5 + \zeta^7 + \zeta^9
\]
\[
= 2\zeta + 2\zeta^3 + 2\zeta^5 = 2D_2
\]

By this same process,

\[
D_1 \cdot D_1 = 2D_0 + D_1
\]
\[
D_2 \cdot D_2 = 3D_0 + 3D_1
\]

Therefore, the intersection numbers for this Schur ring are:

\[
p^0_{11} = 2, \quad p^1_{11} = 1, \quad p^2_{11} = 0
\]

\[
p^0_{12} = 0, \quad p^1_{12} = 0, \quad p^2_{12} = 2
\]

\[
p^0_{22} = 3, \quad p^1_{22} = 3, \quad p^2_{22} = 0
\]
Adjacency matrices

- $S$ a finite set $\{s_1, s_2, \cdots, s_m\}$
- $R_0, R_1, \cdots, R_d$ defined as above

The adjacency matrix of $R_l$ is the $m \times m$ matrix $A_l$ whose $(i, j)$th entry is 1 if $(s_i, s_j) \in R_l$ or 0 otherwise. We say that a subring $A_1, \ldots, A_d$ of $\mathbb{C}[M_{m \times m}(\mathbb{Z})]$ is an adjacency ring or Bose-Mesner algebra if:

- for each $i \in \{0, \ldots, d\}$, $A_i$ is a $(0, 1)$-matrix,
- $\sum_{i=0}^d A_i = J$ (the all 1's matrix),
- for each $i \in \{0, \ldots, d\}$, $^tA_i = A_j$, for some $j \in \{0, \ldots, d\}$,
- there is a subset $J \subset \{0, \ldots, d\}$ such that $\sum_{j \in J} A_j = I$, and
- there is a set of non-negative integers $\{p_{ij}^k \mid i, j, k \in \{0, \ldots, d\}\}$ such that

$$A_i A_j = \sum_{k=0}^d p_{ij}^k A_k,$$

for all such $i, j$. 
Constructing Adjacency Matrices

Constructing an adjacency matrix $A_k$ from a weighted partial difference set

- Let $G$ be a group of order $v$, $D = D_1 \cup \cdots \cup D_d$ a weighted PDS
- $A_k$ is a $v \times v$ matrix
- $(i,j)$th entry = 1 if $\vec{i} - \vec{j} \in D_k$, 0 otherwise

Constructing an adjacency matrix $A_k$ from a weighted Cayley graph $X_w(G, D)$:

- $A_k$ is a $v \times v$ matrix, where $v = |G|$
- $(i,j)$th entry = 1 if vertices $g_i$ and $g_j$ are connected by an edge of weight $k$
Adjacency Matrices for $GF(9)$ Example

\[ A_1 = \begin{pmatrix}
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\end{pmatrix} \]

\[ A_2 = \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
\end{pmatrix} \]
Important Theorems
Intersection number-matrix theorem

$G$ a finite abelian group, $D_0, \cdots, D_d \subseteq G$ such that $D_i \cap D_j = \emptyset$ if $i \neq j$, and

- $G$ is the disjoint union of $D_0 \cup \cdots \cup D_d$
- for each $i$ there is a $j$ such that $D_i^{-1} = D_j$, and
- $D_i \cdot D_j = \sum_{k=0}^{l} p_{ij}^k D_k$ for some positive integer $p_{ij}^k$.

Then the matrices $P_k = (p_{ij}^k)_{0 \leq i, j \leq d}$ satisfy the following properties:

- $P_0$ is a diagonal matrix with entries $|D_0|, \cdots, |D_d|$
- For each $k$, the $j$th column of $P_k$ has sum $|D_j|$ ($j = 0, \cdots, d$). Likewise, the $i$th row of $P_k$ has sum $|D_i|$ ($i = 0, \cdots, d$).
Intersection number-trace theorem

Let \( f : GF(p)^n \rightarrow GF(p) \) be a function, \( \Gamma \) be its Cayley graph. Assume \( \Gamma \) is a weighted strongly regular graph. Let \( A = (a_{k,l}) \) be the adjacency matrix of \( \Gamma \). Let \( A_i = (a^i_{k,l}) \) be the \((0,1)\)-matrix where

\[
a^i_{k,l} = \begin{cases} 
1 & \text{if } a_{k,l} = i \\
0 & \text{otherwise}
\end{cases}
\]

for each \( i = 1, 2, \ldots, p - 1 \). Let \( A_0 = I \). Let \( A_p \) be the \((0,1)\)-matrix such that \( A_0 + A_1 + \cdots + A_{p-1} + A_p = J \). The intersection numbers \( p_{ij}^k \) defined by

\[
A_iA_j = \sum_{k=0}^{p} p_{ij}^k A_k
\]

satisfy the formula

\[
p_{ij}^k = \left( \frac{1}{p^n|D_k|} \right) \ Tr(A_iA_jA_k)
\]

for all \( i, j, k = 1, 2, \ldots, p \).
Connections between intersection numbers

Let \( G = GF(p)^n \). Let \( D_0, \cdots, D_d \subseteq G \) such that \( D_i \cap D_j = \emptyset \) if \( i \neq j \), and

- \( G \) is the disjoint union \( D_0 \cup \cdots \cup D_d \),
- for each \( i \) there is a \( j \) such that \( D_i^{-1} = D_j \), and
- \( D_i \cdot D_j = \sum_{k=0}^{l} p_{ij}^k D_k \) for some positive integer \( p_{ij}^k \).

Then, for all \( i, j, k \), \( |D_k| p_{ij}^k = |D_i| p_{kj}^i \).
Main Results
First result: even bent functions $f : GF(3)^2 \rightarrow GF(3)$

If $f$ is an even, bent function such that $f(0) = 0$ and the level curves $f^{-1}(i)$ yield a weighted PDS then one of the following occurs:

We have $|D_1| = |D_2| = 2$, and the intersection numbers $p_{ij}^k$ are given as follows:

$$
\begin{array}{c|cccc}
  & 0 & 1 & 2 & 3 \\
\hline
p_{ij}^0 & 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 1 & 0 & 2 & 0 & 0 \\
 2 & 0 & 0 & 2 & 0 \\
 3 & 0 & 0 & 0 & 4 \\
\end{array}
\begin{array}{c|cccc}
  & 0 & 1 & 2 & 3 \\
\hline
p_{ij}^1 & 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 \\
 1 & 1 & 1 & 0 & 0 \\
 2 & 0 & 0 & 0 & 2 \\
 3 & 0 & 0 & 2 & 2 \\
\end{array}
\begin{array}{c|cccc}
  & 0 & 1 & 2 & 3 \\
\hline
p_{ij}^2 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1 & 0 \\
 1 & 0 & 0 & 0 & 2 \\
 2 & 1 & 0 & 1 & 0 \\
 3 & 0 & 2 & 0 & 2 \\
\end{array}
\begin{array}{c|cccc}
  & 0 & 1 & 2 & 3 \\
\hline
p_{ij}^3 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 1 & 1 \\
 1 & 0 & 0 & 1 & 1 \\
 2 & 0 & 1 & 0 & 1 \\
 3 & 1 & 1 & 1 & 1 \\
\end{array}
We have $|D_1| = |D_2| = 4$, $D_3 = \emptyset$, and the intersection numbers $p_{ij}^k$ are given as follows:

\[
\begin{array}{c|ccc}
  p_{ij}^0 & 0 & 1 & 2 \\
  \hline
  0 & 1 & 0 & 0 \\
  1 & 0 & 4 & 0 \\
  2 & 0 & 0 & 4 \\
\end{array}
\quad
\begin{array}{c|ccc}
  p_{ij}^1 & 0 & 1 & 2 \\
  \hline
  0 & 0 & 1 & 0 \\
  1 & 1 & 1 & 2 \\
  2 & 0 & 2 & 2 \\
\end{array}
\quad
\begin{array}{c|ccc}
  p_{ij}^2 & 0 & 1 & 2 \\
  \hline
  0 & 0 & 0 & 1 \\
  1 & 0 & 2 & 2 \\
  2 & 1 & 2 & 1 \\
\end{array}
\quad
\text{no } p_{ij}^3
\]

Since $D_3 = \emptyset$, there are no $i, j$ such that $D_iD_j$ will produce elements of $D_3$. 
## Chart of even bent functions

<table>
<thead>
<tr>
<th>$GF(3)^2$</th>
<th>$(0, 0)$</th>
<th>$(1, 0)$</th>
<th>$(2, 0)$</th>
<th>$(0, 1)$</th>
<th>$(1, 1)$</th>
<th>$(2, 1)$</th>
<th>$(0, 2)$</th>
<th>$(1, 2)$</th>
<th>$(2, 2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b_1$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$b_2$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$b_3$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$b_4$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$b_5$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$b_6$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$b_7$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$b_8$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$b_9$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$b_{10}$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$b_{11}$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$b_{12}$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$b_{13}$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$b_{14}$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$b_{15}$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$b_{16}$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$b_{17}$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$b_{18}$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Second result: even bent functions $f : GF(3)^3 \rightarrow GF(3)$

If $f$ is an even, bent function such that $f(0) = 0$ and the level curves $f^{-1}(i)$ yield a weighted PDS then one of the following occurs:

We have $|D_1| = 6$, $|D_2| = 12$, and the intersection numbers $p_{ij}^k$ are given as follows:

<table>
<thead>
<tr>
<th>$p_{ij}^0$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p_{ij}^1$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p_{ij}^2$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p_{ij}^3$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
We have $|D_1| = 12$, $|D_2| = 6$, and the intersection numbers $p_{ij}^k$ are given as follows:

\[
\begin{array}{cccc}
p_{ij}^0 & 0 & 1 & 2 & 3 \\
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 12 & 0 & 0 \\
2 & 0 & 0 & 6 & 0 \\
3 & 0 & 0 & 0 & 8 \\
p_{ij}^1 & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 0 & 0 \\
1 & 1 & 5 & 2 & 4 \\
2 & 0 & 2 & 2 & 2 \\
3 & 0 & 4 & 2 & 2 \\
p_{ij}^2 & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 1 & 0 \\
1 & 0 & 4 & 4 & 4 \\
2 & 1 & 4 & 1 & 0 \\
3 & 0 & 4 & 0 & 4 \\
p_{ij}^3 & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 1 \\
1 & 0 & 6 & 3 & 3 \\
2 & 0 & 3 & 0 & 3 \\
3 & 1 & 3 & 3 & 1 
\end{array}
\]
Preserving structures under function composition

Suppose:

- $f : \mathbb{GF}(p)^n \rightarrow \mathbb{GF}(p)$ is an even function such that $f(0) = 0$
- $D_i = f^{-1}(i)$ for $i \in \mathbb{GF}(p)$
- $\phi : \mathbb{GF}(p)^n \rightarrow \mathbb{GF}(p)^n$ is a linear map that is invertible (i.e., $\det \phi \neq 0 \bmod p$)
- $g = f \circ \phi$

If the collection of sets $D_1, D_2, \cdots, D_{p-1}$ forms a weighted partial difference set for $\mathbb{GF}(p)^n$ then so does its image under the function $\phi$.

Additionally, the Schur ring associated to the weighted partial difference set of $f$ is isomorphic to the Schur ring associated to the weighted partial difference set of $g$. 
Group action

Let $G$ be a multiplicative group and let $X$ be a set. $G$ acts on $X$ (on the left) if there exists a map $\rho : G \times X \to X$ such that:

- $\rho(1_G, x) = x$ for all $x \in X$
- $\rho(g, \rho(h, x)) = \rho(gh, x)$ for all $g, h \in G, x \in X$

An orbit is any set of the form $\{\rho(g, x) | g \in G\}$; we call this the orbit of $x$. 
Proof of second result

Consider the set $\mathbb{E}$ of all functions $f : GF(3)^3 \rightarrow GF(3)$ such that

- $f$ is even
- $f(0) = 0$
- the degree of the algebraic normal form of $f$ is at most 4

There are $3^{12} = 531,441$ such functions

Let $\mathbb{B} \subseteq \mathbb{E}$ be the subset of bent functions

Let $G = GL(3, GF(3))$ be the set of linear automorphisms $\phi : GF(3)^3 \rightarrow GF(3)^3$. $f \in \mathbb{E}$ is equivalent to $g \in \mathbb{E}$ if and only if $f$ is sent to $g$ under some element of $G$. 
Proof (cont.)

signature of $f$: sequence of cardinalities of the level curves $f^{-1}(1)$ and $f^{-1}(2)$.

All of the functions in each equivalence class have the same signature.

- 35 unique signatures across all functions on $GF(3)^3$

Mathematica was used to find all equivalence classes of functions in $\mathbb{E}$; 281 total equivalence classes, but only 4 classes consist of bent functions.

Call these classes $B_1, B_2, B_3, B_4$; then $\mathbb{B} = B_1 \cup B_2 \cup B_3 \cup B_4$
Two equivalence classes had signature (6,12) and two classes had signature (12,6)

- $x_1^2 + x_2^2 + x_3^2$ represents $B_1$, a class of 234 functions of signature (6,12)
- $x_1x_3 + 2x_2^2 + 2x_1^2x_2^2$ represents $B_2$, a class of 936 functions of signature (6,12)
- $B_3 = -B_1$, $B_4 = -B_2$

We conclude through calculation that $B_1$ corresponds with the first condition of the theorem, while $B_3$ corresponds to the second condition. $B_2$ and $B_4$ do not yield weighted partial difference sets.
Conclusions/Further Research

- Main result is only a partial characterization
  - Certain constraints on the functions
  - Reverse claim?

- Characterization in $GF(5)^n$

- Developing non-linear cryptanalysis