On the relationship between irreducible cyclic codes, finite projective planes and non-weakly regular bent functions

Rumi Melih Pelen

Department of Mathematics,
Erzurum Technical University,
Erzurum, Turkey.

A conference in honor of Joachim Rosenthal’s 60th birthday
July 11-15, 2022
Zurich, Switzerland
Outline

1. Non-Weakly Regular Bent Functions
2. Strongly Regular Graphs and Cyclotomic schemes
3. Finite Projective Planes
4. Irreducible Cyclic Codes

On the relationship between irreducible cyclic codes, finite projective planes and non-weakly regular bent functions.
Non-Weakly Regular Bent Functions

Bent Functions

- \( p \): odd prime and \( \mathbb{F}_{p^n} \): finite fields of order \( p^n \).
- \( \mathbb{F}_{p^n} \) is an \( n \) dimensional vector space over \( \mathbb{F}_p \).
- Let \( f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p \). The Walsh transform of \( f \) at \( \alpha \in \mathbb{F}_p^n \) is defined as a complex valued function \( \hat{f} \) on \( \mathbb{F}_p^n \)

\[
\hat{f}(\alpha) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x) - \alpha \cdot x}
\]

where \( \epsilon_p = e^{\frac{2\pi i}{p}} \) and \( \alpha \cdot x \) denotes the usual dot product in \( \mathbb{F}_p^n \).

- The function \( f \) is called bent function if \( |\hat{f}(\alpha)| = p^{n/2} \) for all \( \alpha \in \mathbb{F}_p^n \).
• The Walsh coefficients of a bent function $f$ is characterized in [3] as follows

$$\hat{f}(\alpha) = \begin{cases} 
\pm p^{n/2} \epsilon_p f^*(\alpha) & \text{if } p^n \equiv 1 \text{ mod } 4, \\
\pm ip^{n/2} \epsilon_p f^*(\alpha) & \text{if } p^n \equiv 3 \text{ mod } 4,
\end{cases}$$

• The function $f^* : \mathbb{F}_p^n \to \mathbb{F}_p$ is called dual of $f$.

• A bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ with Walsh transform $\hat{f}(\alpha) = \xi_{\alpha} p^{n/2} \epsilon_p f^*(\alpha)$ is called **regular** if $\forall \alpha \in \mathbb{F}_p^n$, we have $\xi_{\alpha} = 1$, and is called **weakly regular** if $\forall \alpha \in \mathbb{F}_p^n$, we have $\xi_{\alpha} = \xi$ where $\xi \in \{\pm 1, \pm i\}$ is a constant (i.e. independent from $\alpha$), otherwise (i.e. $\xi_{\alpha}$ changes sign with respect to $\alpha$) it is called **non-weakly regular**.
• We define the type of a bent function $f$ as follows,

\[
\hat{f}(0) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p f(x) = \xi p^{\frac{n}{2}} \epsilon_p f^*(0)
\]

then $f$ is of **type(+)**.

\[
\hat{f}(0) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p f(x) = -\xi p^{\frac{n}{2}} \epsilon_p f^*(0)
\]

then $f$ is of **type(-)**. \(1\)

where $\xi \in \{1, i\}$ is a constant depending on $p$ and $n$.

• The partition of $\mathbb{F}_p^n$ with respect to sign of the Walsh coefficients of $f$ is given in [1] as follow

\[
B_+(f) := \{\beta : \beta \in \mathbb{F}_p^n \mid f(x) + \beta \cdot x \text{ is of type(+)})\}
\]

\[
B_-(f) := \{\beta : \beta \in \mathbb{F}_p^n \mid f(x) + \beta \cdot x \text{ is of type(−)})\}
\]

\(2\)

\(3\)
Strongly Regular Graphs

**Definition 1 (Partial Difference Sets)**

Let $G$ be a group of order $v$ and $D$ be a subset of $G$ with $k$ elements. Then $D$ is called a $(v, k, \lambda, \mu)$-partial difference set (PDS) in $G$ if the expressions $gh^{-1}$, for $g$ and $h$ in $D$ with $g \neq h$, represent each nonidentity element in $D$ exactly $\lambda$ times and represent each nonidentity element not in $D$ exactly $\mu$ times.

A PDS is called **regular** if $e \notin D$ and $D^{-1} = D$. 
Definition 2 (Strongly Regular Graphs)

A graph \(\Gamma\) with \(v\) vertices is said to be a \((v, k, \lambda, \mu)\)-strongly regular graph if

1. it is regular of valency \(k\), i.e., each vertex is joined to exactly \(k\) other vertices;
2. any two adjacent vertices are both joined to exactly \(\lambda\) other vertices and two nonadjacent vertices are both joined to exactly \(\mu\) other vertices.

Definition 3 (Cayley Graph)

\(G\) : a finite abelian group
\(D\) : an inverse-closed subset of \(G\) (\(0 \notin D\) and \(D = -D\))
\(E := \{(x, y)|x, y \in G, x - y \in D\}\)

\((G, E)\) is called a Cayley graph, denoted by \(\text{Cay}(G, D)\).
$D$ is called the connection set of $(G, E)$.

**Proposition 1 ([8])**

A Cayley graph $\Gamma$, generated by a subset $D$ of the regular automorphism group $G$, is a strongly regular graph if and only if $D$ is a **regular** PDS in $G$. 
Translation Schemes

**Definition 1 (Association scheme)**

Let $V$ be a finite set of vertices, and let \( \{R_0, R_1, \ldots, R_d\} \) be binary relations on $V$ with $R_0 := \{(x, x) : x \in V\}$. The configuration $(V; R_0, R_1, \ldots, R_d)$ is called an association scheme of class $d$ on $V$ if the following holds:

1. $V \times V = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$.
2. $R_i^t = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where $R_i^t := \{(x, y) : (y, x) \in R_i\}$. If $i' = i$, we call $R_i$ is symmetric.
3. For $i, j, k \in \{0, 1, \ldots, d\}$ and for any pair $(x, y) \in R_k$, the number $\#\{z \in V | (x, z) \in R_i, (z, y) \in R_j\}$ is a constant, which is denoted by $p_{ij}^k$. 
Remark 1

2-class symmetric association schemes are strongly regular graphs.

Definition 2 (Translation Scheme)

Let $\Gamma_i := (G, E_i)$, $1 \leq i \leq d$ be Cayley graphs on an abelian group $G$, and $D_i$ are connection sets of $(G, E_i)$ with $D_0 := \{0\}$. Then, $(G, \{D_i\}_{i=0}^d)$ is called a translation scheme if $(G, \{\Gamma_i\}_{i=0}^d)$ is an association scheme.

Given a $d$-class translation scheme $(X, \{R_i\}_{i=0}^d)$, we can take union of classes to form graphs with larger edge sets which is called a fusion.
Cyclotomic Schemes

**Definition 3 (Cyclotomic Scheme)**

Let $\mathbb{F}_q$ be the finite fields of order $q$, $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$, and $C_0$ be a subgroup of $\mathbb{F}_q^*$ s.t. $C_0 = -C_0$. The partition $\mathbb{F}_q^* \setminus C_0$ of $\mathbb{F}_q^*$ gives a translation scheme on $(\mathbb{F}_q, +)$, called a cyclotomic scheme.

Each coset (called a cyclotomic coset) of $\mathbb{F}_q^* \setminus C_0$ is expressed as

$$C_i^{(N,q)} = w^i \langle w^N \rangle, \quad 0 \leq i \leq N - 1,$$

where $N|q - 1$ is a positive integer and $w$ is a fixed primitive element of $\mathbb{F}_q^*$. The eigenvalues of the cyclotomic scheme given by $\Psi_1(C_i^{(N,q)})$, called Gauss periods, where $\Psi_1 : \mathbb{F}_q \to \mathbb{C}^*$ defined by $\Psi_1(x) = \epsilon_p^{\text{Tr}(x)}$ be the canonical additive character of $\mathbb{F}_q$. 

---

Non-Weakly Regular Bent Functions

Strongly Regular Graphs and Cyclotomic schemes

Finite Projective Planes

Irreducible Cyclic Codes
Some Previous Results on Strongly Regular Graphs

It is known that one of the tools to construct partial difference sets are bent functions. In [5], it is proven that pre-image sets of the ternary weakly regular even bent functions are partial difference sets.

Let $f : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ be a $p$-ary function, and $D_i := \{x : x \in \mathbb{F}_{p^m} | f(x) = i\}$. The following is due to [5]

**Theorem 1 (Y. Tan, A. Pott, and T. Feng)**

Let $f : \mathbb{F}_{3^{2m}} \rightarrow \mathbb{F}_3$ be ternary function satisfying $f(x) = f(-x)$, and $f(0) = 0$. Then $f$ is weakly regular bent if and only if $D_1$ and $D_2$ are both

$$(3^{2m}, 3^{2m-1} + \epsilon 3^{m-1}, 3^{2m-2}, 3^{2m-2} + \epsilon 3^{m-1}) - \text{PDSs},$$

where $\epsilon = \pm 1$. Moreover, $D_0 \setminus \{0\}$ is a

$$(3^{2m}, 3^{2m-1} - 1 - 2\epsilon 3^{m-1}, 3^{2m-2} - 2 - 2\epsilon 3^{m-1}, 3^{2m-2} - \epsilon 3^{m-1}) - \text{PDSs}.$$
Remark 2

In [5], the authors stated that weak regularity is necessary for Theorem 1 since it does not hold for the ternary non-weakly regular bent function $Tr_6(w^7x^{98})$.

Later, Ozbudak and Pelen observed a relation between following sporadic examples of ternary non-weakly regular bent functions and strongly regular graphs [2].

- For the following examples we have $q = 729$, and $N = 13$. Let $w$ be a fixed primitive element of $\mathbb{F}_{3^6}$.
- $C_0$ be the multiplicative subgroup of $\mathbb{F}_{3^6}$ generated by $w^{13}$. For $1 \leq i \leq 12$, $C_i$ denotes the $i$-th cyclotomic coset of $C_0$ and given by $C_i = w^i C_0$. 
Example 4

\( f_2 : \mathbb{F}_{3^6} \rightarrow \mathbb{F}_3, f_2(x) = Tr_6(w^7x^{98}) \) is non-weakly regular of Type \((-\)). Dual of \( f_2 \) is not bent and corresponding partial difference sets and strongly regular graphs are non-trivial.

- \( B_+(f_2) \) is a \((729, 504, 351, 342)\)-PDS in \( \mathbb{F}_{3^6} \)
- \( B^*(f_2) \) is a \((729, 224, 62, 71)\)-PDS in \( \mathbb{F}_{3^6} \)

By using \textit{Magma}, we compute \( B_+(f_2) \) and \( B_-(f_2) \). We observe that \( B_+(f_2) = \bigcup_{i \in \{0, 3, 5, 6, 7, 8, 9, 11, 12\}} C_i \) and \( B_-(f_2) = \bigcup_{i \in \{1, 2, 4, 10\}} C_i \). Hence \( B_+(f_2) \) and \( B^*(f_2) \) are 2-class fusion schemes and correspond to non-trivial strongly regular graphs.
Example 5

$f_3 : \mathbb{F}_{3^6} \rightarrow \mathbb{F}_3$, $f_3(x) = Tr_6(w^7x^{14} + (w^{35}x^{70}))$ is non-weakly regular of Type $(-)$. Dual of $f_3$ is not bent. Corresponding partial difference sets are non trivial.

- $B_+(f_3)$ is a $(729, 504, 351, 342)$- regular PDS in $\mathbb{F}_{3^6}$.
- $B_*(f_3)$ is a $(729, 224, 62, 71)$- regular PDS in $\mathbb{F}_{3^6}$.

Again by *Magma* computations we have,

$B_+(f_3) = \bigcup_{i \in \{0,1,2,4,5,6,9,11,12\}} C_i$ and $B_-(f_3) = \bigcup_{i \in \{3,7,8,10\}} C_i$. Hence $B_+(f_3)$ and $B_*(f_3)$ are 2-class fusion schemes and correspond to non trivial strongly regular graphs.

Remark 3

Non-trivial strongly regular graphs correspond to $f_2$ and $f_3$ are from a unital: projective 9–ary $[28, 3]$ code with weights 24, 27; $VO^- (6, 3)$ affine polar graph ([9]).
Finite Projective Planes

- $q$: odd prime and $PG(2, q)$ finite projective plane of order $q$
- $\mathcal{L} := \{\ell_i\}_{i=1}^{q^2+q+1}$ be the set of lines and $\mathcal{B} := \{P_i\}_{i=1}^{q^2+q+1}$ be the set of points in $PG(2, q)$.
- Equivalently, symmetric $(q^2 + q + 1, q + 1, 1)$–design
- Consider the regular action of $\mathbb{F}_3^*/<w^{13}>$ over the set of cyclotomic cosets $\{C_0^{(13,729)}, C_1^{(13,729)}, \ldots, C_{12}^{(13,729)}\}$.
- **Further Observations:** This action induces an automorphism of order 13 on $PG(2, 3)$. The cyclotomic cosets correspond to points of $PG(2, 3)$ and $B_-(f_2)$ corresponds to a line of $PG(2, 3)$. Similar arguments hold for $B_-(f_3)$.
- Namely, if we multiply the set
  \[
  \{C_1^{(13,729)}, C_2^{(13,729)}, C_4^{(13,729)}, C_{10}^{(13,729)}\}
  \]
  by $w$ recursively we obtain all of the lines in $PG(2, 3)$. 
• Let \( \ell_0 := \{C_1, C_2, C_4, C_{10}\} \), \( \ell_i := w^i \ell_0 \), \( i \in \{1, \ldots, 12\} \) are the 13 lines in \( PG(2, 3) \). Then,

\[
\mathcal{L} = \{\{C_1, C_2, C_4, C_{10}\}, \{C_2, C_3, C_5, C_{11}\}, \{C_3, C_4, C_6, C_{12}\}, \\
\{C_4, C_5, C_7, C_0\}, \{C_5, C_6, C_8, C_1\}, \{C_6, C_7, C_9, C_2\}, \\
\{C_7, C_8, C_{10}, C_3\}, \{C_8, C_9, C_{11}, C_4\}, \{C_9, C_{10}, C_{12}, C_5\}, \\
\{C_{10}, C_{11}, C_0, C_6\}, \{C_{11}, C_{12}, C_1, C_7\}, \{C_{12}, C_0, C_2, C_8\}, \\
\{C_0, C_1, C_3, C_9\}\}
\]

• Observe that \( B_-(f_3) = \ell_6 \).

• \( B_-(f_2), B_-(f_3) \) can be viewed as lines at infinity and \( B_+(f_2), B_+(f_3) \) can be viewed as the affine plane \( AG(2, 3) \).

• In [4], The authors stated that "Non-weak regularity of \( f_2 \) was verified by computer calculations, however, proving this result theoretically and probably finding the whole class of similar functions remains an open problem."
• It is natural to think that these two functions belong to an infinite class of non-weakly regular bent functions arising from finite geometry.

**Conjecture 1**

Let $q = p^{2m}$, $m \geq 2 \in \mathbb{Z}$, and $N = \frac{p^m - 1}{p - 1}$. Then, there exists a non-weakly regular bent function $f : \mathbb{F}_q \to \mathbb{F}_p$ with $B_-(f) = \bigcup_{j \in I_1} C_j^{(N,q)}$ corresponds to a hyperplane of $PG(m - 1, p)$ at infinity, and $B_+(f) = \bigcup_{j \in I_0} C_j^{(N,q)}$ corresponds to $AG(m - 1, p)$, where $I_0$, $I_1$ be a partition of the set $\{0, 1, 2, \ldots \frac{p^m - 1}{p - 1} - 1\}$ with $|I_0| = p^m - 1$, $|I_1| = \frac{p^m - 1}{p - 1}$. 
Irreducible Cyclic Codes

**Definition 4 (Irreducible Cyclic Codes)**

\[ f(x) : \text{an irreducible divisor of } x^r - 1 \in \mathbb{F}_p[x], \text{ where } \gcd (r, p) = 1. \]

The cyclic code of length \( r \) over \( \mathbb{F}_p \) generated by \( \frac{x^m - 1}{f(x)} \) is called an irreducible cyclic code.

Alternatively, Let \( q = p^m \) and \( N \) be an integer dividing \( q - 1 \). Put \( n = \frac{q-1}{N} \). Let \( \alpha \) be a primitive element of \( \mathbb{F}_q \) and let \( \theta = \alpha^N \). The set

\[ C(N, q, \beta) = \{ c(\beta) := (\text{Tr}(\beta), \text{Tr}(\beta \theta), \text{Tr}(\beta \theta^2), \ldots, \text{Tr}(\beta \theta^{n-1})) : \beta \in \mathbb{F}_q \} \]

is called an irreducible cyclic \([n, m_0]\) code over \( \mathbb{F}_q \), where \( m_0 \) divides \( m \).
Theorem 2 (McEliece)

Let \( N_0 := \gcd(N, \frac{q-1}{p-1}) \). Then,

\[
\text{wt}(\bar{c}(\beta)) = \frac{n(p-1)}{p} - \frac{p-1}{pN} \psi_1(\beta C_0^{(N_0, q)}).
\]

Hence, find the weight distribution of the irreducible cyclic codes is equivalent to the evaluation of the eigenvalues of the cyclotomic schemes.
• Let us consider the case $q = p^{2m}$, $m \geq 2 \in \mathbb{Z}$, and $N = \frac{p^{m-1}}{p-1}$.

• It is easy to see that $\mathbb{F}_p^* \subset C_0^{(N,q)}$. Hence, the eigenvalues of the corresponding cyclotomic scheme are integers.

• Let $\chi$ be a multiplicative character of order $N$ of $\mathbb{F}_q$. Then the following equation gives the relation between Gauss sums and Gauss periods:

$$G(\chi) = \sum_{i=0}^{N-1} \psi_1(C_i^{(N,q)})\chi(w^i),$$

where $w$ is a primitive element of $\mathbb{F}_q$.

• $m = 2$: semiprimitive case. $C(N, q, \beta)$ is a two weight irreducible cyclic code.
Three-Weight Irreducible Cyclic Codes

- By Gauss Sum we have

\[ G(\chi) = \sum_{i=0}^{N-1} \eta_i \xi_N^i, \]

where \( \eta_i = \Psi_1(C_i^{(N,q)}) \) are Gauss periods and \( \xi_N = e^{\frac{2\pi i}{N}} \).

- \( \eta_i \)'s are integers. Hence, \( G(\chi) \in \mathbb{Z}[\xi_N] \).

- \( m = 3 \): For \( p = 3, 5, 7 \) by Magma we verify that \( C(N, q, \beta) \) is a three-weight irreducible cyclic code.

**Conjecture 2**

Let \( p \) be an odd prime, \( q = p^6 \), and \( N = p^2 + p + 1 \). Then, \( C(N, q, \beta) \) is a three-weight irreducible cyclic code.
Thanks...
F. Özbudak, R.M. Pelen "Duals of non weakly regular bent functions are not weakly regular and generalization to plateaued functions"; Finite Fields and Their Applications, vol. 64, June 2020.


