On the roots of a polynomial connected with Golomb Costas Arrays

John Sheekey

Claude Shannon Institute
School of Mathematical Science
University College Dublin

23 July 2010 / Fields Institute-Carleton Finite Fields Workshop

Outline

1. Costas Arrays
2. Cross-correlation
3. (Partial) Solution

Definition

A Costas Array C (of order n) is an $n \times n$ grid containing n dots such that

- Each row and each column contains precisely one dot (permutation matrix)
- All displacement vectors (i.e. vector between two dots) are distinct

In other words, the autocorrelation function of C is always either 0 or 1.

Definition

A Costas Array C (of order n) is an $n \times n$ grid containing n dots such that

- Each row and each column contains precisely one dot (permutation matrix)
- All displacement vectors (i.e. vector between two dots) are distinct

In other words, the autocorrelation function of C is always either 0 or 1.

Definition

A Costas Array C (of order n) is an $n \times n$ grid containing n dots such that

- Each row and each column contains precisely one dot (permutation matrix)
- All displacement vectors (i.e. vector between two dots) are distinct

In other words, the autocorrelation function of C is always either 0 or 1.

Construction

- Applications in radar and sonar
- The number of Costas Arrays of a given order is not known. In fact, the existence of Costas Arrays for all n is an open problem.
- However, there are some constructions.

Construction

- Applications in radar and sonar
- The number of Costas Arrays of a given order is not known. In fact, the existence of Costas Arrays for all n is an open problem.
- However, there are some constructions.

Construction

- Applications in radar and sonar
- The number of Costas Arrays of a given order is not known. In fact, the existence of Costas Arrays for all n is an open problem.
- However, there are some constructions.

Definition (Welch Array)

Let α be a primitive element of $\mathbb{F}_p$, p a prime. Define a permutation π on $\{1..p-1\}$ by

$$\pi(i) = \alpha^i$$

Then π is a Costas permutation

Definition (Golomb Array)

Let α and β be primitive elements of $\mathbb{F}_q$, q a power of a prime. Define a permutation π on $\{1..q-2\}$ by

$$\alpha^i + \beta^{\pi(i)} = 1$$

Then π is a Costas permutation. Denote this by $G_{\alpha,\beta}$

Definition (Welch Array)

Let α be a primitive element of $\mathbb{F}_p$, p a prime. Define a permutation π on $\{1..p-1\}$ by

$$\pi(i) = \alpha^i$$

Then π is a Costas permutation

Definition (Golomb Array)

Let α and β be primitive elements of $\mathbb{F}_q$, q a power of a prime. Define a permutation π on $\{1..q-2\}$ by

$$\alpha^i + \beta^{\pi(i)} = 1$$

Then π is a Costas permutation. Denote this by $G_{\alpha,\beta}$

Suppose we had two Golomb arrays of the same order, $G_{\alpha,\beta}$ and G_{α^r,β^s}, where $(r, q-1) = (s, q-1) = 1$. Then the maximum cross-correlation between the two arrays can be shown to equal the number of roots of the polynomial

$$F_{r,s}(z) := z^r + (1-z)^s - 1$$

in $\mathbb{F}_q$.

Conjecture (Rickard)

$F_{r,s}$ has at most $\frac{q+1}{2}$ roots in $\mathbb{F}_q$

Suppose we had two Golomb arrays of the same order, $G_{\alpha,\beta}$ and G_{α^r,β^s}, where $(r, q-1) = (s, q-1) = 1$. Then the maximum cross-correlation between the two arrays can be shown to equal the number of roots of the polynomial

$$F_{r,s}(z) := z^r + (1-z)^s - 1$$

in $\mathbb{F}_q$.

Conjecture (Rickard)

$F_{r,s}$ has at most $\frac{q+1}{2}$ roots in $\mathbb{F}_q$

Suppose we had two Golomb arrays of the same order, $G_{\alpha,\beta}$ and G_{α^r,β^s}, where $(r, q-1) = (s, q-1) = 1$. Then the maximum cross-correlation between the two arrays can be shown to equal the number of roots of the polynomial

$$F_{r,s}(z) := z^r + (1-z)^s - 1$$

in $\mathbb{F}_q$.

Conjecture (Rickard)

$F_{r,s}$ has at most $\frac{q+1}{2}$ roots in $\mathbb{F}_q$

Suppose we had two Golomb arrays of the same order, $G_{\alpha,\beta}$ and G_{α^r,β^s}, where $(r, q-1) = (s, q-1) = 1$. Then the maximum cross-correlation between the two arrays can be shown to equal the number of roots of the polynomial

$$F_{r,s}(z) := z^r + (1-z)^s - 1$$

in $\mathbb{F}_q$.

Conjecture (Rickard)

$F_{r,s}$ has at most $\frac{q+1}{2}$ roots in $\mathbb{F}_q$

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1-z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1-\alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1-z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1-\alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1 - z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1 - \alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1 - z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1 - \alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1-z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1-\alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1 - z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1 - \alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

We consider the case $r = s$, r odd, and denote by F_r.

- 0 and 1 are roots for all r.
- $$F_r(z) = F_r(1-z) = -z^r F_r(\frac{1}{z})$$
- If α is a root, then $1-\alpha$ is a root
- If $\alpha \neq 0$ is a root, then $\frac{1}{\alpha}$ is a root
- So there is an action by S_3 on the roots of the polynomial
- This polynomial also arises in the cross-correlation of m-sequences, and in the study of APN functions
- It is related to Cauchy-Mirimanoff polynomials

Lemma

Let r be odd. Let S denote the set of non-zero roots of F_r over $\mathbb{F}_q$. Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{1-x}{1-y} \in S$$

Proof.

x and y are roots of F_r, so

$$x^r + (1-x)^r = 1$$
$$y^r + (1-y)^r = 1$$
$$\Rightarrow x^r - y^r = (1-y)^r - (1-x)^r$$

□

Lemma

Let r be odd. Let S denote the set of non-zero roots of F_r over $\mathbb{F}_q$. Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{1-x}{1-y} \in S$$

Proof.

x and y are roots of F_r, so

$$x^r + (1-x)^r = 1$$
$$y^r + (1-y)^r = 1$$
$$\Rightarrow x^r - y^r = (1-y)^r - (1-x)^r$$

Lemma

Let r be odd. Let S denote the set of non-zero roots of F_r over $\mathbb{F}_q$. Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{1-x}{1-y} \in S$$

Proof.

x and y are roots of F_r, so

$$x^r + (1-x)^r = 1$$
$$y^r + (1-y)^r = 1$$
$$\Rightarrow x^r - y^r = (1-y)^r - (1-x)^r$$

Lemma

Let r be odd. Let S denote the set of non-zero roots of F_r over $\mathbb{F}_q$. Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{1-x}{1-y} \in S$$

Proof.

x and y are roots of F_r, so

$$x^r + (1-x)^r = 1$$
$$y^r + (1-y)^r = 1$$
$$\Rightarrow x^r - y^r = (1-y)^r - (1-x)^r$$

Lemma

Let r be odd. Let S denote the set of non-zero roots of F_r over $\mathbb{F}_q$. Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{1-x}{1-y} \in S$$

Proof.

x and y are roots of F_r, so

$$x^r + (1-x)^r = 1$$
$$y^r + (1-y)^r = 1$$
$$\Rightarrow x^r - y^r = (1-y)^r - (1-x)^r$$

$\square$

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1$$
$$\Leftrightarrow x^r + (y - x)^r = y^r$$
$$\Leftrightarrow x^r - y^r = (x - y)^r$$
$$\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r$$
$$\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r$$
$$\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1 \\
&\Leftrightarrow x^r + (y - x)^r = y^r \\
&\Leftrightarrow x^r - y^r = (x - y)^r \\
&\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r \\
&\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r \\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$
\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1 \\
&\Leftrightarrow x^r + (y - x)^r = y^r \\
&\Leftrightarrow x^r - y^r = (x - y)^r \\
&\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r \\
&\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r \\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}
$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1$$
$$\Leftrightarrow x^r + (y - x)^r = y^r$$
$$\Leftrightarrow x^r - y^r = (x - y)^r$$
$$\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r$$
$$\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r$$
$$\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$
\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1 \\
&\Leftrightarrow x^r + (y - x)^r = y^r \\
&\Leftrightarrow x^r - y^r = (x - y)^r \\
&\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r \\
&\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r \\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}
$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1 \\
&\Leftrightarrow x^r + (y - x)^r = y^r \\
&\Leftrightarrow x^r - y^r = (x - y)^r \\
&\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r \\
&\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r \\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$
\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1-\tfrac{x}{y})^r = 1\\
&\Leftrightarrow x^r + (y-x)^r = y^r\\
&\Leftrightarrow x^r - y^r = (x-y)^r\\
&\Leftrightarrow (1-y)^r - (1-x)^r = (x-y)^r\\
&\Leftrightarrow (1-x)^r + (x-y)^r = (1-y)^r\\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}
$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r □

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1 \\
&\Leftrightarrow x^r + (y - x)^r = y^r \\
&\Leftrightarrow x^r - y^r = (x - y)^r \\
&\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r \\
&\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r \\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r $\square$

Proof(contd.)

Then $\frac{x}{y}$ is a root

$$
\begin{aligned}
&\Leftrightarrow (\tfrac{x}{y})^r + (1 - \tfrac{x}{y})^r = 1\\
&\Leftrightarrow x^r + (y - x)^r = y^r\\
&\Leftrightarrow x^r - y^r = (x - y)^r\\
&\Leftrightarrow (1 - y)^r - (1 - x)^r = (x - y)^r\\
&\Leftrightarrow (1 - x)^r + (x - y)^r = (1 - y)^r\\
&\Leftrightarrow (\tfrac{1-x}{1-y})^r + (\tfrac{x-y}{1-y})^r = 1
\end{aligned}
$$

$\Leftrightarrow \frac{1-x}{1-y}$ is a root of F_r $\square$

Applying this result to $\frac{1}{x}$ and $\frac{1}{y}$, we also have

Corollary

Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{y}{x}\left(\frac{1-x}{1-y}\right) \in S$$

Applying this result to $\frac{1}{x}$ and $\frac{1}{y}$, we also have

Corollary

Suppose x and y are in S, with $y \neq 1$. Then

$$\frac{x}{y} \in S \Leftrightarrow \frac{y}{x}\left(\frac{1-x}{1-y}\right) \in S$$

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

Suppose now that c is any non-root of F_r. Consider the set

$$\frac{1}{c}S = \{x \mid F_r(cx) = 0\}$$

Let $x \in S \cap \frac{1}{c}S$, i.e. x and cx are both roots of F_r. Then by the previous lemma,

$$\frac{1-x}{1-cx}$$

and

$$c(\frac{1-x}{1-cx})$$

are both non-roots of F_r (as $c = \frac{cx}{x}$ is not a root). Hence for every element x of $S \cap \frac{1}{c}S$, there is an element $\frac{1-x}{1-cx}$ which is not in $S \cup \frac{1}{c}S$.

So if we set

$$U = \{\frac{1-x}{1-cx} \mid x \in S \cap \frac{1}{c}S\}$$

we have that $|U| = |S \cap \frac{1}{c}S|$, and hence

$$|U \cup S \cup \frac{1}{c}S| = 2|S| \leq q-1$$

proving the result:

Theorem

If r is odd and $p-1$ does not divide $r-1$, then the polynomial

$$z^r + (1-z)^r - 1$$

has at most $\frac{q+1}{2}$ roots in F_q.

So if we set

$$U = \{\frac{1-x}{1-cx} \mid x \in S \cap \frac{1}{c}S\}$$

we have that $|U| = |S \cap \frac{1}{c}S|$, and hence

$$|U \cup S \cup \frac{1}{c}S| = 2|S| \leq q-1$$

proving the result:

Theorem

If r is odd and $p-1$ does not divide $r-1$, then the polynomial

$$z^r + (1-z)^r - 1$$

has at most $\frac{q+1}{2}$ roots in F_q.

So if we set

$$U = \{\frac{1-x}{1-cx} \mid x \in S \cap \frac{1}{c}S\}$$

we have that $|U| = |S \cap \frac{1}{c}S|$, and hence

$$|U \cup S \cup \frac{1}{c}S| = 2|S| \leq q-1$$

proving the result:

Theorem

If r is odd and $p-1$ does not divide $r-1$, then the polynomial

$$z^r + (1-z)^r - 1$$

has at most $\frac{q+1}{2}$ roots in F_q.

So if we set

$$U = \{\frac{1-x}{1-cx} \mid x \in S \cap \frac{1}{c}S\}$$

we have that $|U| = |S \cap \frac{1}{c}S|$, and hence

$$|U \cup S \cup \frac{1}{c}S| = 2|S| \leq q-1$$

proving the result:

Theorem

If r is odd and $p-1$ does not divide $r-1$, then the polynomial

$$z^r + (1-z)^r - 1$$

has at most $\frac{q+1}{2}$ roots in F_q.

Summary

- We have proved Rickard's Conjecture for the case $r = s$
- Future work
  - $r \neq s$?
  - Exact number of roots?
  - F_r irreducible over $\mathbb{Z}[z]$?

Summary

- We have proved Rickard's Conjecture for the case $r = s$
- Future work
  - $r \neq s$?
  - Exact number of roots?
  - F_r irreducible over $\mathbb{Z}[z]$?