Costas arrays from projective planes of prime order

David Thomson

Carleton University, Ottawa (Canada)

December 13, 2013

Table of Contents

Two motivating examples

Latin squares

Definition. A Latin square of order n is an $n \times n$ array on n symbols such that no two symbols appear in the same row or column.

1	2	3	4	5	6
6	1	2	3	4	5
5	6	1	2	3	4
4	5	6	1	2	3
3	4	5	6	1	2
2	3	4	5	6	1

- The elements of a Latin square can be taken to represent treatments to some (row) subject in some time sequence.

Latin squares

Definition. A Latin square of order n is an $n \times n$ array on n symbols such that no two symbols appear in the same row or column.

1	2	3	4	5	6
6	1	2	3	4	5
5	6	1	2	3	4
4	5	6	1	2	3
3	4	5	6	1	2
2	3	4	5	6	1

- The elements of a Latin square can be taken to represent treatments to some (row) subject in some time sequence.
- However, if, e.g., treatment 2 is affected by treatment 1, every row but the final row will show this.

Better Latin squares

1	2	3	4	5	6
6	1	2	3	4	5
5	6	1	2	3	4
4	5	6	1	2	3
3	4	5	6	1	2
2	3	4	5	6	1

1	2	3	4	5	6
4	1	5	2	6	3
5	3	1	6	4	2
2	4	6	1	3	5
3	6	2	5	1	4
6	4	5	3	2	1

Good Latin squares should have few repeated digrams. Generally speaking, the rows or columns of a Latin square should "resemble" each other as little as possible.

Better Latin squares

1	2	3	4	5	6
6	1	2	3	4	5
5	6	1	2	3	4
4	5	6	1	2	3
3	4	5	6	1	2
2	3	4	5	6	1

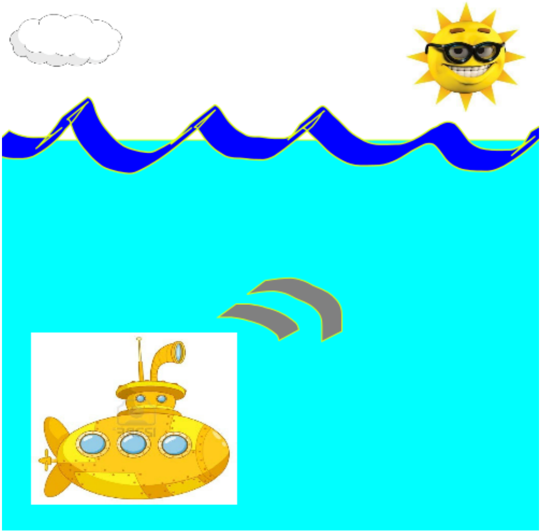
1	2	3	4	5	6
4	1	5	2	6	3
5	3	1	6	4	2
2	4	6	1	3	5
3	6	2	5	1	4
6	4	5	3	2	1

Good Latin squares should have few repeated digrams. Generally speaking, the rows or columns of a Latin square should "resemble" each other as little as possible.

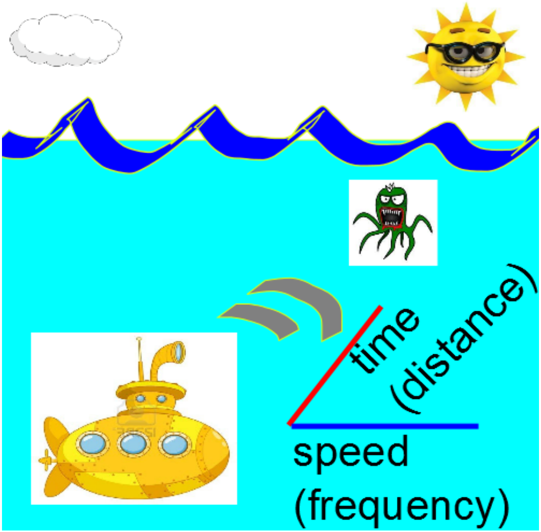
Gilbert (1965) constructs Latin squares of even order with the property that no diagrams $a()_k b$ are repeated either vertically or horizontally, where $()_k$ means there is a gap of k columns/rows.

In his construction, Gilbert places the symbol $P_1(i) + P_2(j)$ in position (i, j), where P_1 And P_2 permutations with distinct differences.

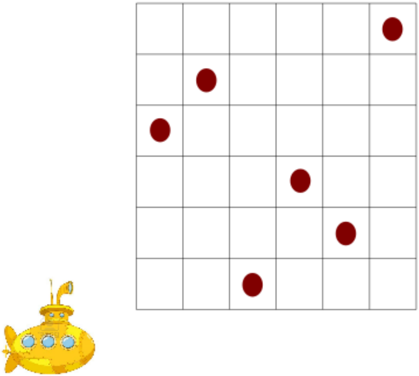
RADAR and SONAR



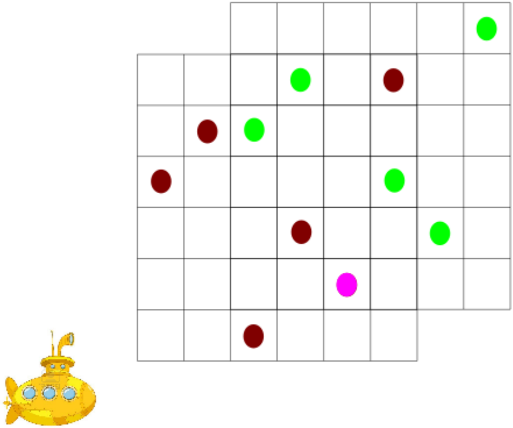
RADAR and SONAR



RADAR and SONAR



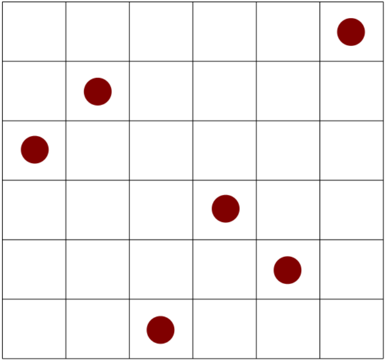
RADAR and SONAR



- On any diagonal shift, the array contains at most one overlapping dot.
- This is the ideal autocorrelation property.

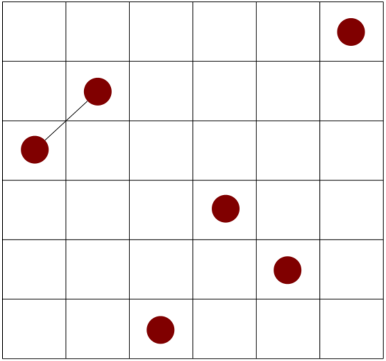
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



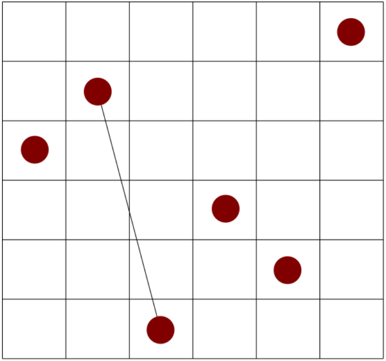
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



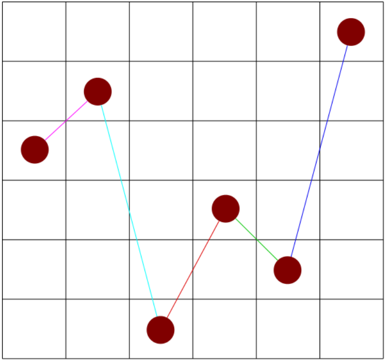
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



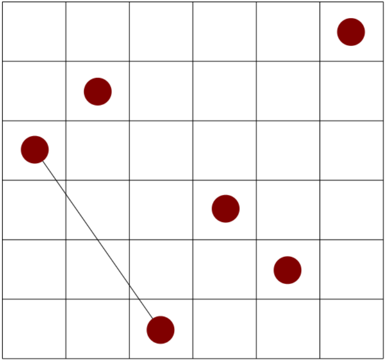
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



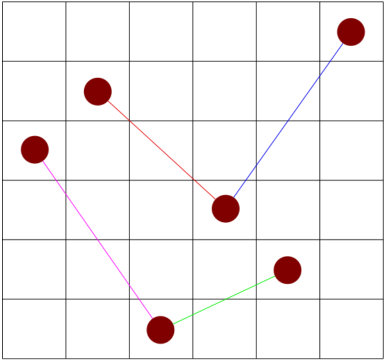
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



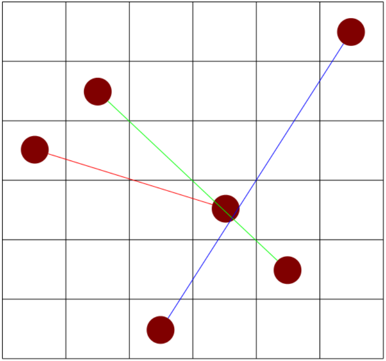
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



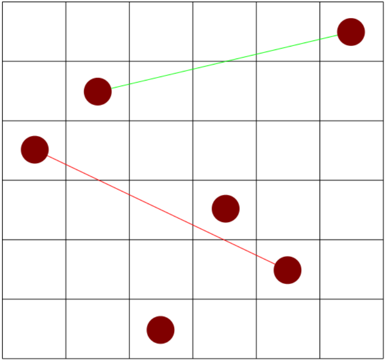
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



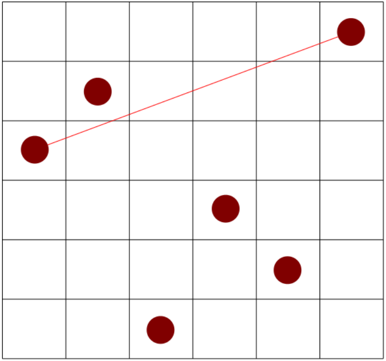
Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



Costas arrays

- A Costas array is a permutation array (exactly one dot in every row/column) such that every vector (left-to-right) joining the dots is distinct.



Formalizing Costas arrays

Definition. Let $[n] = \{1, 2, \ldots, n\}$ and let $f\colon [n] \to [n]$ be a permutation, then f satisfies the distinct differences property if

$$f(i+k) - f(i) = f(j+k) - f(j)$$

if and only if either $k = 0$ or $i = j$ for $k = 1, 2, \ldots, n-j$.

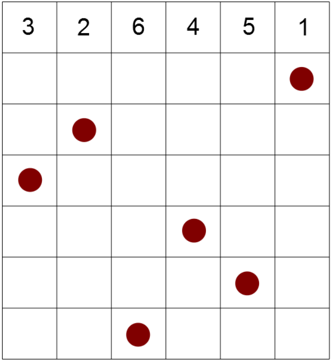
1. If f is a permutation which satisfies the distinct differences property, we say f is a Costas permutation.
2. If f is a Costas permutation and $f(1) = y_1, f(2) = y_2, \ldots, f(n) = y_n$, then $(y_1, y_2, \ldots, y_n)$ is a Costas sequence.
3. The permutation array generated by by a Costas permutation f (that is, with a dot in cell (x, y) if and only if $f(x) = y$) is a Costas array.

Trivia about Costas arrays

- Discovered independently by Gilbert and Costas (1965)
- Two main constructions (and some variants)
  1. Welch (1982), but originally due to Gilbert (1965) - order $p-1$, where p is prime
  2. Lempel-Golomb (1984) - order $q-2$, where q is a prime power.
- No non-finite fields constructions exist.
- Though exhaustive searches of order 28 do exist it is not known whether Costas arrays of order 32 (any many larger orders) exist.
- New Interest. Jedwab and Wodlinger (2013) - 2 nice papers on periodic and structural properties, respectively.

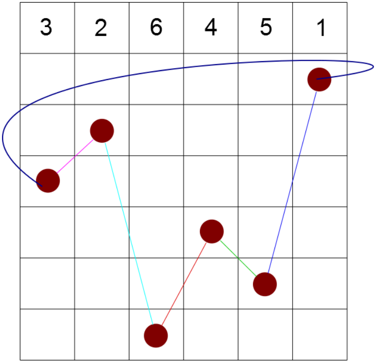
Periodicity properties of Costas arrays

Introducing periodicity



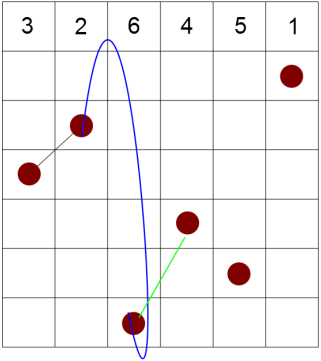
- Costas: the line segments joining any two dots are distinct.
- Domain-periodic: the line segments joining any two dots are distinct when the array is wrapped horizontally.
- Range-periodic: the line segments joining any two dots are distinct when the array is wrapped vertically.

Introducing periodicity



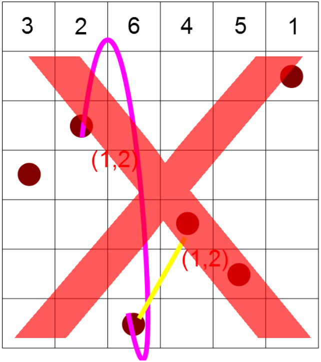
- Costas: the line segments joining any two dots are distinct.
- Domain-periodic: the line segments joining any two dots are distinct when the array is wrapped horizontally ($\Delta x = 1$).
- Range-periodic: the line segments joining any two dots are distinct when the array is wrapped vertically.

Introducing periodicity



- Costas: the line segments joining any two dots are distinct.
- Domain-periodic: the line segments joining any two dots are distinct when the array is wrapped horizontally.
- Range-periodic: the line segments joining any two dots are distinct when the array is wrapped vertically ($\Delta x = 1$).

Introducing periodicity



NOT range-periodic Costas! (mod 6)

Combinatorial interpretation of periodicity I

The difference triangle is a useful tool to determine if a permutation is Costas.

Example. Consider the sequence

3 2 6 4 5 1

Combinatorial interpretation of periodicity I

The difference triangle is a useful tool to determine if a permutation is Costas.

Example. Consider the sequence

$$\begin{array}{cccccc} 3 & 2 & 6 & 4 & 5 & 1 \\ & 1 & -4 & 2 & -1 & 4 \end{array}$$

Combinatorial interpretation of periodicity I

The difference triangle is a useful tool to determine if a permutation is Costas.

Example. Consider the sequence

3	2	6	4	5	1
	1	-4	2	-1	4
		-3	-2	1	3

Combinatorial interpretation of periodicity I

The difference triangle is a useful tool to determine if a permutation is Costas.

Example. Consider the sequence

3	2	6	4	5	1
	1	-4	2	-1	4
		-3	-2	1	3
			-1	-3	5
				-2	1
					2

Since the entries in each row are distinct, the sequence is Costas.

Combinatorial interpretation of periodicity I

The difference triangle is a useful tool to determine if a permutation is Costas.

Example. Consider the sequence

3	2	6	4	5	1
	1	−4	2	−1	4
		−3	−2	1	3
			−1	−3	5
				−2	1
					2

Since the entries in each row are distinct, the sequence is Costas.

Modulo 7:

3	2	6	4	5	1
	1	3	2	6	4
		4	5	1	3
			6	4	5
				5	1
					2

Since the entries in each row are distinct modulo 7, the sequence is range-periodic Costas.

Combinatorial interpretation of periodicity II

The difference square is a useful tool to determine if a permutation is domain-periodic Costas.

Example. Consider the sequence

3	2	6	4	5	1
−2	1	−4	2	−1	4
2	−1	−3	−2	1	3
1	3	−5	−1	−3	5
3	2	−1	−3	−2	1
−1	4	−2	1	−4	2

Since the entries in each row are distinct, the sequence is domain-periodic Costas.

Combinatorial interpretation of periodicity II

The difference square is a useful tool to determine if a permutation is domain-periodic Costas.

Example. Consider the sequence

3	2	6	4	5	1
−2	1	−4	2	−1	4
2	−1	−3	−2	1	3
1	3	−5	−1	−3	5
3	2	−1	−3	−2	1
−1	4	−2	1	−4	2

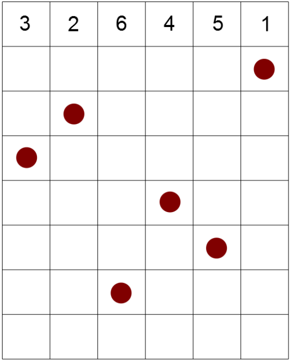
Since the entries in each row are distinct, the sequence is domain-periodic Costas.

Modulo 7:

3	2	6	4	5	1
5	1	3	2	6	4
2	6	4	5	1	3
1	3	2	6	4	5
3	2	6	4	5	1
6	4	5	1	3	2

Since the entries in each row are distinct modulo 7, the sequence is domain periodic (mod 6) and range-periodic Costas (mod 7).

Domain periodic modulo 6, range periodic modulo 7



- Circular: the line segments joining any two dots are distinct when the augmented array is wrapped around a torus.

Definition. (Following Jedwab and Wodlinger) The (wrapped) vectors (x, y), with $x \in \mathbb{Z}_6$ and $y \in \mathbb{Z}_7$, are toroidal.

The exponential-Welch construction

Exponential-Welch Construction. Let p be prime and let α be a primitive element of $\mathbb{F}_p$. Then $\alpha^i(\alpha, \alpha^2, \ldots, \alpha^{p-1})$ is a Costas sequence.

Let $f(i) = \alpha^i$, then f is domain-periodic modulo $p - 1$ (since $\alpha^{p-1} = 1$) and range-periodic modulo p.

(Re)-Definition. A Costas sequence is circular if it is domain-periodic (mod m) and range periodic (mod $m + 1$).

Conjecture. (**Golomb and Moreno, 1996)** A Costas sequence is circular if and only if it is exponential-Welch.

Costas polynomials

Fixing some notation

Definition. Let G_1 and G_2 be finite (Abelian) groups and let $f : G_1 \to G_2$. The difference map of f at $a \in G_1^*$ is denoted

$$\Delta_{f,a}(x) = f(x+a) - f(x) \in G_2.$$

Fixing some notation

Definition. Let G_1 and G_2 be finite (Abelian) groups and let $f\colon G_1 \to G_2$. The difference map of f at $a \in G_1^*$ is denoted

$$\Delta_{f,a}(x) = f(x+a) - f(x) \in G_2.$$

Definition. Let $\lambda_{a,b}(f) = |\Delta_{f,a}^{-1}(b)|$. The row-$a$-deficiency of f is

$$D_{r=a}(f) = \sum_{b \in G_2} (1 - \delta_{\lambda_{a,b}(f)}),$$

where $\delta_i = 0$ if $i = 0$ and $\delta_i = 1$ otherwise. The deficiency of f is

$$D(f) = \sum_{a \in G_1^*} D_{r=a}(f).$$

Deficiency and Costas arrays

If $f\colon \mathbb{Z}_m \to \mathbb{Z}_m$ generates a permutation array which is domain and range-periodic, then its toroidal vectors are given by $(d, \Delta_{f,d}(x))$.

Proposition. If f generates a permutation array of order m, the number of missing toroidal vectors of f is given by the deficiency of f, $D(f)$.

Theorem. (Panario et al., 2011) If f is a permutation of $\mathbb{Z}_m$, then

$$D(f) \geq \begin{cases} (m-1) + (m-1) & m \text{ is odd,} \\ (m-1) + (m-3) & m \text{ is even.} \end{cases}$$

Deficiency and Costas arrays

If $f : \mathbb{Z}_m \to \mathbb{Z}_m$ generates a permutation array which is domain and range-periodic, then its toroidal vectors are given by $(d, \Delta_{f,d}(x))$.

Proposition. If f generates a permutation array of order m, the number of missing toroidal vectors of f is given by the deficiency of f, $D(f)$.

Theorem. (Panario et al., 2011) If f is a permutation of $\mathbb{Z}_m$, then

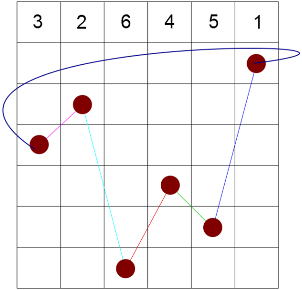
$$D(f) \geq \begin{cases} (m-1) + (m-1) & m \text{ is odd,} \\ (m-1) + (m-3) & m \text{ is even.} \end{cases}$$

Corollary. (Jedwab and Wodlinger) A square permutation array of order m never contains every toroidal vector (non-horizontal, non-vertical).

Thus, a circular Costas array is the smallest variant of a Costas array containing every toroidal vector.

Difference maps for circular Costas sequences

A circular Costas sequence is given by a map $f\colon \mathbb{Z}_m \to \mathbb{Z}_{m+1}$ such that $f(0) = 0$ and $\Delta_{f,d}(x) = f(x+d) - f(x)$ is injective for all d.



Hence,

$$\sum_x \Delta_{f,d}(x) = \gamma_2 = 0,$$

where γ_2 is the sum of the order 2 elements of $\mathbb{Z}_{m+1}$. Therefore $m+1$ is odd.

Permutation polynomials from circular Costas arrays

Moreover, using a special kind of symmetry of the difference square:

Theorem. (Etzion, Golomb and Taylor, 1989) If $f : \mathbb{Z}_m \to \mathbb{Z}_{m+1}$ defines a circular Costas sequence, then $m + 1$ is prime.

Permutation polynomials from circular Costas arrays

Moreover, using a special kind of symmetry of the difference square:

Theorem. (Etzion, Golomb and Taylor, 1989) If $f\colon \mathbb{Z}_m \to \mathbb{Z}_{m+1}$ defines a circular Costas sequence, then $m+1$ is prime.

Thus, if f is any circular Costas permutation, without loss of generality, view $f\colon \mathbb{F}_p^* \to \mathbb{F}_p$, where $\Delta_{f,d}(x) = f(xd) - f(x)$ is an injection for all $d \neq 1$.

Let $f\colon \mathbb{F}_p^* \to \mathbb{F}_p$ be circular Costas. Then by defining $f(0) = 0$, f can be given (by Lagrange Interpolation) by a permutation polynomial of degree at most $p-1$.

Costas polynomials over prime fields

Definition. Let $f \in \mathbb{F}_q[x]$, with $f(0) = 0$ and

$$\Delta_{f,d}(x) = f(xd) - f(x)$$

is a permutation polynomial of $\mathbb{F}_q$, for all $d \neq 1$, then f is a Costas polynomial.

Conjecture. (Golomb and Moreno, 1996) If $f \in \mathbb{F}_p[x]$ is a Costas polynomial, then $f(x) = x^s$, where $\gcd(s, p-1) = 1$.

Equivalent Conjectures

Proposition. The Golomb-Moreno conjectures are equivalent.

Proof. Let $(y_i)_{i=1}^{q-1}$ be a circular Costas sequence. Hence $y_{i+k} - y_i$ are distinct for all $i, k \neq 0$.

Let α be primitive in $\mathbb{F}_p$ and set $f(\alpha^i) = y_i$ for all i. The Costas property states $f(\alpha^{i+k}) - f(\alpha^i)$ permutes the elements of $\mathbb{F}_p^*$. That is, $f(xd) - f(x)$ permutes the elements of $\mathbb{F}_p^*$ for $d \neq 1$.

Moreover, if (y_i) is exponential-Welch, then $y_i = \beta^i$ for some primitive β. Thus, $y_i = \alpha^{si}$ with $\gcd(s, p-1) = 1$ and so $f(x) = x^s$.

Equivalent Conjectures

Proposition. The Golomb-Moreno conjectures are equivalent.

Proof. Let $(y_i)_{i=1}^{q-1}$ be a circular Costas sequence. Hence $y_{i+k} - y_i$ are distinct for all $i, k \neq 0$.

Let α be primitive in $\mathbb{F}_p$ and set $f(\alpha^i) = y_i$ for all i. The Costas property states $f(\alpha^{i+k}) - f(\alpha^i)$ permutes the elements of $\mathbb{F}_p^*$. That is, $f(xd) - f(x)$ permutes the elements of $\mathbb{F}_p^*$ for $d \neq 1$.

Moreover, if (y_i) is exponential-Welch, then $y_i = \beta^i$ for some primitive β. Thus, $y_i = \alpha^{si}$ with $\gcd(s, p-1) = 1$ and so $f(x) = x^s$.

The remainder of this talk is to prove and extend the conjecture: Joint work with A. Muratović-Ribić (Sarajevo), A. Pott (Magdeburg) and S. Wang (Carleton).

Proof of a conjecture of Golomb and Moreno

Direct product difference sets

Definition. Let G be a finite group, $|G| = n^2 - n$ and let $G = H \times E$, where $|E| = n = |H| + 1$. A subset R of G with the property that the non-identity quotients consist of every element of $G \setminus \{H, E\}$ exactly once and no element of H or E appears as a quotient is a direct product difference set.

Example. Let $E = \mathbb{F}_q$ and $H = \mathbb{F}_q^*$. Now, let $f\colon \mathbb{F}_q^* \to \mathbb{F}_q$ and consider $R = \{(x, f(x))\colon x \in \mathbb{F}_q^*\} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q$.

Direct product difference sets

Definition. Let G be a finite group, $|G| = n^2 - n$ and let $G = H \times E$, where $|E| = n = |H| + 1$. A subset R of G with the property that the non-identity quotients consist of every element of $G \setminus \{H, E\}$ exactly once and no element of H or E appears as a quotient is a direct product difference set.

Example. Let $E = \mathbb{F}_q$ and $H = \mathbb{F}_q^*$. Now, let $f\colon \mathbb{F}_q^* \to \mathbb{F}_q$ and consider $R = \{(x, f(x))\colon x \in \mathbb{F}_q^*\} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q$.

To avoid H, the map $f(x) \neq 0$. Moreover, if R is a d.p.d.s, then $f(\mathbb{F}_q^*) = \mathbb{F}_q \setminus \{0\}$. Here, f is the associated function of R.

By a counting argument, all quotients must be distinct, thus, if $xy^{-1} = x'y'^{-1}$, then

$$f(x) - f(y) = f(x') - f(y').$$

Sketch

Heavily relying on [Section 5.3, Pott]:

Theorem. If R is a direct product difference set, then G acts as a quasiregular collineation group on a Type (f) projective plane Π of order n.

Theorem. If $n = q = p$ and $H = \mathbb{F}_p^*$, then Π is Desarguesian.

Theorem. The plane Π is Desarguesian if and only if H is cyclic and R is equivalent to a direct product difference set whose associated function is an isomorphism (up to equivalence).

Lemma. If f is an automorphism of $\mathbb{F}_p^*$, then
$f : x \mapsto x^s, \gcd(s, p-1) = 1.$

Tying up the proof

Theorem. Let f be a Costas polynomial over $\mathbb{F}_p$, then f is a monomial.

Let f be a Costas polynomial and consider the restriction of f to $\mathbb{F}_p^*$ (we abuse notation slightly by still using the symbol f). Thus f is an injection and $f(xd) - f(x)$ permutes the elements of $\mathbb{F}_p^*$ for all $d \neq 1$.

Let

$$xy^{-1} = x'y'^{-1} = d^{-1}$$

for $d \neq 0, 1$. Then

$$f(xd) - f(x) = f(x'd) - f(x'),$$

and we have $x = x'$ and so $y = y'$. Thus, $R = \{(x, f(x)) \colon x \in \mathbb{F}_p^*\}$ is a direct product difference set.

Since $f(0) = 0$, by the previous slide $f(x) = x^s, \gcd(s, p-1)$.

Connection to planar functions

Definition. A planar function over $\mathbb{F}_q$ is a map $f\colon \mathbb{F}_q \to \mathbb{F}_q$ such that $f(x+a) - f(x)$ is a permutation for all $a \neq 0$.

1. (Hiramine, 1989 / Gluck, 1990 / Ronyai and Szonyi, 1989): Planar functions over $\mathbb{F}_p$, $p > 3$, are quadratic.
2. (Coulter, 2006): Characterize planar monomials over $\mathbb{F}_{p^2}$.
3. (Zieve, 2013): Characterize planar monomials over $\mathbb{F}_q$.

Costas polynomials are a semi-multiplicative analogue of planar functions.

Connection to planar functions

Definition. A planar function over $\mathbb{F}_q$ is a map $f\colon \mathbb{F}_q \to \mathbb{F}_q$ such that $f(x+a) - f(x)$ is a permutation for all $a \neq 0$.

1. (Hiramine, 1989 / Gluck, 1990 / Ronyai and Szonyi, 1989): Planar functions over $\mathbb{F}_p$, $p > 3$, are quadratic.
2. (Coulter, 2006): Characterize planar monomials over $\mathbb{F}_{p^2}$.
3. (Zieve, 2013): Characterize planar monomials over $\mathbb{F}_q$.

Costas polynomials are a semi-multiplicative analogue of planar functions.

Two questions:

1. Can we characterize Costas polynomials over small extensions?
2. Can we characterize special classes of Costas polynomials for general finite fields?

Costas polynomials over general finite fields

Costas polynomials over non-prime fields

Let $q = p^e$ and let $L(x) = \sum_{i=0}^{e-1} a_i x^{p^i}$. Then L is a linearized polynomial.

Linearized polynomials are linear operators on finite fields. We have

$$\begin{aligned}\Delta_{L,d}(x) = L(xd) - L(x) &= \sum_{i=0}^{e-1} a_i (xd)^{p^i} - \sum_{i=0}^{e-1} a_i x^{p^i} \\ &= \sum_{i=0}^{e-1} a_i (d-1)^{p^i} x^{p^i} \\ &= L(x(d-1))\end{aligned}$$

Costas polynomials over non-prime fields

Let $q = p^e$ and let $L(x) = \sum_{i=0}^{e-1} a_i x^{p^i}$. Then L is a linearized polynomial.

Linearized polynomials are linear operators on finite fields. We have

$$\begin{aligned}\Delta_{L,d}(x) = L(xd) - L(x) &= \sum_{i=0}^{e-1} a_i (xd)^{p^i} - \sum_{i=0}^{e-1} a_i x^{p^i} \\ &= \sum_{i=0}^{e-1} a_i (d-1)^{p^i} x^{p^i} \\ &= L(x(d-1))\end{aligned}$$

Proposition. A linearized polynomial L is Costas if and only if L is a permutation polynomial.

Compositions of Costas polynomials

Proposition. Let f be a Costas polynomial and g is a linearized permutation polynomial, then $g \circ f$ is a Costas polynomial.

Proof. We have

$$\begin{aligned}(g \circ f)(xd) - (g \circ f)(x) &= g(f(xd)) - g(f(x)) \\ &= g(f(xd) - f(x)) \\ &= g(y),\end{aligned}$$

where $y = \Delta_{f,d}(x)$, which is a permutation for all $d \neq 1$.

Equivalent d.p.d.s

Recall. We saw previously that Type (f) Desarguesian planes over $\mathbb{F}_q$ are characterized by direct product difference sets whose associated function was equivalent to an automorphism of $\mathbb{F}_q^*$.

Definition. Two d.p.d.s R_1 and R_2 are equivalent if $R_1 = \psi(R_2)$, where $\psi = (\psi_H, \psi_E)$ and ψ_H is an automorphism of H and ψ_E is an automorphism of E which fixes 0. If $H = \mathbb{F}_q^*$ and $E = \mathbb{F}_q$, then these automorphisms agree with the above proposition.

Corollary. If other direct product difference sets in $\mathbb{F}_q^* \times \mathbb{F}_q$ exist, then $G = \mathbb{F}_q^* \times \mathbb{F}_q$ acts as a quasiregular collineation group of a non-Desarguesian plane over $\mathbb{F}_q$.

Some corollaries and conjectures

Remark. Jungnickel and de Resmini (2002) - “Indeed, it seems quite reasonable to conjecture that a plane with an abelian group of type (f) must be Desarguesian.”

Conjecture. If $q = p^n$ for some n, the only Costas polynomials of $\mathbb{F}_q$ are of the form

$$f(x) = \sum_{i=0}^{n-1} a_i x^{s \cdot p^i},$$

where $\sum_{i=0}^{n-1} a_i x^{p^i}$ is a permutation polynomial and $\gcd(s, q-1) = 1$.

And don't try to find circular Costas maps of other sizes...

Theorem. (**Prime Power Conjecture for planes of Type (f)**) Jungnickel and de Resmini (2002) - Let G be an Abelian collineation group of order $n(n-1)$ of a projective plane of order n. Then n must be a power of a prime p and the p-part of G is elementary Abelian.

Corollary. Let $f : G_1 \to G_2$ be a Costas "polynomial" with G_1 cyclic, then $G_1 \cong \mathbb{F}_q^*$.