Strongly Regular Cayley Graphs: Constructions and Problems

Qing Xiang

University of Delaware
Newark, DE 19716, USA
xiang@math.udel.edu

July, 2010

Introduction

- This talk is about strongly regular Cayley graphs, or equivalently, partial difference sets.
- The constructions we will talk about use finite fields, semifields, quadratic forms over finite fields (or more generally, p-ary bent functions), and cyclotomy.
- There are still many problems in this area. We will mention a few of them.

Definitions and Examples

Strongly Regular Graphs

A *strongly regular graph srg* (v, k, λ, μ) is a graph with v vertices that is regular of valency k and that has the following properties:

- For any two adjacent vertices x, y, there are exactly λ vertices adjacent to both x and y.
- For any two nonadjacent vertices x, y, there are exactly μ vertices adjacent to both x and y.

For example, a 5-cycle is a $(5, 2, 0, 1)$-srg, and the Petersen graph is a $(10, 3, 0, 1)$-srg. From the point of view of association schemes, strongly regular graphs are equivalent to 2-class association schemes.

Theorem. For a simple graph Γ of order v, not complete or edgeless, with adjacency matrix A, the following are equivalent:

- Γ is strongly regular with parameters (v, k, λ, μ) for certain integers k, λ, μ,
- $A^2 = kI + \lambda A + \mu(J - I - A)$ for certain real numbers k, λ, μ,
- A has precisely two distinct restricted eigenvalues.

Theorem (Hoffman and Singleton). Suppose $(v, k, 0, 1)$ is the parameter set of a strongly regular graph. Then $(v, k) = (5, 2)$, (10, 3), (50, 7) or (3250,57).

Long-standing Open Problem. Does there exist an srg $(3250, 57, 0, 1)$?

Partial Difference Sets

Let G be a (multiplicative) group of order v. A k-element subset D of G is called a (v, k, λ, μ) partial difference set in G (PDS) provided that the list of "differences" $d_1 d_2^{-1}, d_1, d_2 \in D, d_1 \neq d_2$ contains each nonidentity element of D exactly λ times and each nonidentity element in $G \setminus D$ exactly μ times.

Using group ring notation, we have D is a (v, k, λ, μ) partial difference set in G if and only if

$$DD^{(-1)} = \gamma 1_G + \lambda D + \mu(G - D),$$

where $\gamma = k - \mu$ if $1_G \notin D$ and $\gamma = k - \lambda$ if $1_G \in D$.

We will usually assume that $1_G \notin D$ and $D^{(-1)} = D$, in which case, we have

$$D^2 = (k - \mu)1_G + (\lambda - \mu)D + \mu G.$$

Relationship between SRG and PDS

- An srg (v, k, λ, μ) with a regular automorphism group G is equivalent to a (v, k, λ, μ) PDS in G.
- PDS in elementary abelian p-groups are also closely related to 2-weight codes and two-intersection sets in finite geometry.

Examples.

- The Paley PDS: Let $\mathbb{F}_q$ be the finite field of size q, where $q \equiv 1 \pmod 4$. Then the set of nonzero squares of $\mathbb{F}_q$ is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ PDS.
- Let $Q : \mathbb{F}_q^{2m} \to \mathbb{F}_q$ be a nonsingular quadratic form, where q is a prime power, and let $D = \{x \in \mathbb{F}_q^{2m} \mid Q(x) = 0\} \setminus \{0\}$. Then D is a PDS in $(\mathbb{F}_q^{2m}, +)$. The parameters of D are $(q^{2m}, r(q^m - \epsilon), \epsilon q^m + r^2 - 3\epsilon r, r^2 - \epsilon r)$, where $\epsilon = 1$ or -1 according as Q is hyperbolic or elliptic, and r also depends on the type of Q.
- There are many known constructions, see the survey papers by Calderbank and Kantor, and by S. L. Ma. (I recommend highly the NOTES on Spectra of Graphs, by A. E. Brouwer and W. Haemers.)

Recent Constructions

Theorem (WQWX, Des. Codes and Cryptogr. 2007)
Let $(K, +, *)$ be a presemifield with commutative multiplication. Then $\{x * x \mid x \in K, x \neq 0\}$ is a PDS with Paley parameters or a skew Hadamard difference set according as $|K| \equiv 1 \pmod 4$ or $3 \pmod 4$.

- Semifields

Let $(K, +, *)$ be a set equipped with two binary operations $+$ and $*$. We call $(K, +, *)$ a *presemifield* if the two operations satisfy the following conditions:
(i) K is an abelian group with respect to $+$;
(ii) $x * (y + z) = x * y + x * z$, $(x + y) * z = x * z + y * z$ for all $x, y, z \in K$;
(iii) if $x * y = 0$, then $x = 0$ or $y = 0$.
If furthermore there exists $1 \in K$ such that $1 * x = x * 1 = x$ for all $x \in K$, then we call $(K, +, *)$ a *semifield*.

- Dickson semifields: Assume that q is an odd prime power. Let j be a nonsquare in $K = \mathbb{F}_q$, and let $1 \neq \sigma \in Aut(K)$. The Dickson semifield $(K^2, +, *)$ is defined by

$$(a, b) * (c, d) = (ac + jb^\sigma d^\sigma, ad + bc).$$

- Ganley semifields: Let $K = \mathbb{F}_q$, $q = 3^r$, with $r \geq 3$ odd. The Ganley semifield $(K^2, +, *)$ is defined by

$$(a, b) * (c, d) = (ac - b^9 d - bd^9, ad + bc + b^3 d^3).$$

- Cohen-Ganley semifields: Let $q \geq 9$ be a power of 3 and let $j \in K = \mathbb{F}_q$ be a nonsquare. The Cohen-Ganley semifield $(K^2, +, *)$ is defined by

$$(a, b) * (c, d) = (ac + jbd + j^3(bd)^9, ad + bc + j(bd)^3).$$

- Zha-Kyureghyan-Wang semifields: ...
- ...

Affine Polar Graphs

Construction. Let $Q : \mathbb{F}_q^n \to \mathbb{F}_q$ be a nonsingular quadratic form, where n is even and q is a power of an odd prime p, and let $D = \{x \in \mathbb{F}_q^n \mid Q(x) \text{ is a } \textit{nonzero square}\}$. Then D is a PDS in $(\mathbb{F}_q^n, +)$. The corresponding strongly regular graph $\mathrm{Cay}(\mathbb{F}_q^n, D)$ is the so-called affine polar graph.

Two Generalizations of the Affine Polar Graphs

- Theorem (FWXY, 2010) Let p be a prime, $e \geq 2$, $q = p^{2j\gamma}$, where $\gamma \geq 1$, $e|(p^j + 1)$ and j is the smallest such positive integer. Let C_i, $0 \leq i \leq e-1$, be the cyclotomic classes of $\mathbb{F}_q$ of order e, and $Q : V = \mathbb{F}_q^{2m} \to \mathbb{F}_q$ be a nonsingular quadratic form. Then each of the sets

$$D_{C_i} := \{x \in V \mid Q(x) \in C_i\},\ 0 \leq i \leq e-1,$$

  is a PDS in $(V, +)$ with parameters $(q^{2m}, (q^m - \epsilon)r, \epsilon n + r^2 - 3\epsilon r, r^2 - \epsilon r)$, where $r = \frac{q^{m-1}(q-1)}{e}$, and $\epsilon = 1$ or -1 according as Q is hyperbolic or elliptic.
- In the second generalization we replace the quadratic form in the affine polar graph construction by weakly regular p-ary bent functions

Remarks on the first generalization

- It is interesting to note that the first generalization is valid when $p = 2$ while the Construction of affine polar graph only works when p is odd.
- When the quadratic form Q in the first generalization is of elliptic type, the PDS D_{C_i}, $0 \leq i \leq (e-1)$, have negative Latin square type parameters. Negative Latin square type PDS are harder to come by than Latin square type PDS. Besides the examples arising from elliptic quadrics and the PDS arising from the affine polar graph Construction, there is one more general class of negative Latin square type PDS in elementary abelian p-groups coming from the "difference of two quadrics" construction by Andries Brouwer. The negative Latin square type PDS arising from the first generalization have very different parameters from those known examples since there is quite a bit of freedom to choose the parameter $f = (q-1)/e$.

p-ary Bent Functions

- $f : \mathbb{F}_p^n \to \mathbb{F}_p$
- The Walsh coefficient of f at $b \in \mathbb{F}_p^n$ is defined by

$$\mathcal{W}_f(b) = \sum_{x \in \mathbb{F}_p^n} \omega^{f(x)+b\cdot x},$$

  where ω is a complex primitive pth root of unity.
- We say that f is bent if $|\mathcal{W}_f(b)|^2 = p^n$ for all $b \in \mathbb{F}_p^n$.
- When $p = 2$, we get the usual bent functions.
- These generalized bent functions were introduced by Kumar, Scholtz and Welch in 1985, who (actually) considered $f : (\mathbb{Z}/q\mathbb{Z})^n \to \mathbb{Z}/q\mathbb{Z}$, q not necessarily a prime power.

Regular, weakly regular bent functions

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a p-ary bent function.

- We say that f is regular if $p^{-n/2}\mathcal{W}_f(b)$ is a pth root of unity for all $b \in \mathbb{F}_p^n$.
- We say that f is weakly regular if there exists a complex u such that $|u| = 1$ and $up^{-n/2}\mathcal{W}_f(b)$ is a pth root of unity for all $b \in \mathbb{F}_p^n$.
- For examples of weakly regular p-ary bent functions that are not quadratic forms, see the recent paper "Proofs of two conjectures on ternary weakly regular bent functions" (by HHKWX), IEEE Trans. Inform. Theory, 55 (2009), 5272–5283.

The Second Generalization

- The following relationship between (binary) bent functions and difference sets is well known: Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $D_f = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ (i.e., D_f is the inverse image of 1 under f). Then f is a bent function if and only if D_f is a $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$ difference set in $(\mathbb{F}_2^n, +)$.
- Note that since $(\mathbb{F}_2^n, +)$ is an elementary abelian 2-group, any difference set in $(\mathbb{F}_2^n, +)$ is automatically a partial difference set.
- Let p be an odd prime, and let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a weakly regular bent function. Then

$$D_f = \{x \in \mathbb{F}_p^n \mid f(x) \text{ is a nonzero square}\}$$

is a partial difference set in $(\mathbb{F}_p^n, +)$. This is a theorem by FWXY (2010), and independently by Tan, Chee and Zhang (2010).

Open Problems

- p-ranks
- **Theorem** (Brouwer and Van Eijl, 1992) Let $q = p^t$ be a prime power congruent to 1 modulo 4, and let A be the adjacency matrix of the Paley graph $P(q)$. Then

$$\mathrm{rk}_p(2A + I) = (\frac{p+1}{2})^t.$$

It is an open problem to compute the p-ranks of $2A + I$, where A are adjacency matrices of the pseudo-Paley graphs from semifields.

Order	Paley graphs	Dickson	Ganley
3^4	16	20	N/A
3^6	64	85	88
3^8	256	376	N/A
3^{10}	1024	1654	1534

Open Problems

Let $q = 3^t$, let A be the adjacency matrix of $\mathrm{Cay}(K^2, D(3^t, \sigma))$, and let $r_t = \mathrm{rk}_3(2A + I)$. The first five terms of the sequence $(r_t)_{t \geq 1}$ were computed by both Guobiao Weng and David Saunders. After computing two more terms of the 3-ranks of $2A + I$ ($r_1 = 4, r_2 = 20, r_3 = 85, r_4 = 376, r_5 = 1654, r_6 = 7283, r_7 = 32064$), the following conjecture emerges.

- **Conjecture** (Dave Saunders). Let r_t be defined as above. Then

$$r_t = 4r_{t-1} + 2r_{t-2} - r_{t-3},$$

for all $t \geq 4$.

Open Problems on Constructions

- Construct PDS (Latin square type or negative Latin square type) in groups of non-prime-power orders. (Some work in this direction was done recently by John Polhill.)
- (Edwin van Dam and Xiang) Does there exist an infinite family of PDS with parameters $(v = 2^{3e}, k = 2^{2e} + 2^e + 1, \lambda = 2^e + 4, \mu = 2^e + 2)$?.
- (Harold N. Ward) Does there exist an infinite family of PDS with parameters $(v = q^4, k = \frac{3(q^2+1)(q-1)}{2}, \lambda, \mu, r, s)$, $r = \frac{3(q-1)}{2}$, $s = \frac{3(q-1)}{2} - q^2$? When $q = 3$ or 5, it is known that PDS with these parameters exist.