行政院國家科學委員會專題研究計畫　期中進度報告

關於組合設計理論及其相關應用的研究(2/3)

計畫類別：個別型計畫
計畫編號：NSC92-2115-M-009-006-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立交通大學應用數學系

計畫主持人：黃大原

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 93 年 5 月 25 日

Strongly Regular Graphs associated with Bent Functions

Tayuan Huang and Kuei-Hung You
Department of Applied Mathematics
National Chiao Tung University
Hsinchu Taiwan
thuang@math.nctu.edu.tw

Abstract

Following results of Bernasconi, Codenotti, and VanderKam on a characterization of bent functions, feasible parameters and corresponding eigenvalues of the associated Cayley graphs of bent functions are given; in particular, all of those graphs with at most 280 vertices are included.

1. Introduction

The problem of analyzing the spectral coefficients of Boolean functions has been brought to the framework of spectral analysis of graphs though their associated Cayley graphs, and hence the using of tools from algebraic graph theory for investigations related to the spectral coefficients of Boolean functions with small numbers of distinct coefficients is possible. Among others, a characterization of bent functions in terms of strongly regular graphs by Bernasconi, Codenotti, and VanderKam [1,2] is a successful example. It was shown in [1] that the associated Cayley graph of a bent function is a strongly regular graph by showing that it has exactly three distinct eigenvalues. They further showed that bent functions are the only Boolean functions f with associated strongly regular graph by studying the integral solutions of a quadratic equation in [2]. As a consequence, bent functions can be characterized as Boolean functions with a certain class of strongly regular graphs, followed by a nice interpretation of bent functions in terms of strongly regular graphs.

Further investigation of those strongly regular graphs involved in the characterization of bent functions considered in [1,2] is the purpose of this paper. The definitions of Fourier transformation of Boolean functions, bent functions, and strongly regular graphs are given in section 2. In section 3, some properties of Cayley graphs associated with bent functions are recalled first, then feasible parameters and their corresponding eigenvalues of associated Cayley graphs of bent functions are given; in particular, those graphs with at most 280 vertices are included. As a closed relative of those strongly regular graphs studied in the previous section, strongly regular graphs $SRG(n, k, \lambda, \lambda)$ are studied in section 4.

2. Bent Functions

The Fourier transform of a Boolean function $f(x) : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is defined to be $f^*(x) = \frac{1}{2^n}\sum_{\forall x\in\mathbb{Z}_2^n} f(x)\cdot(-1)^{\langle\lambda,x\rangle}$, which satisfies the property that $f(x) = \frac{1}{2^n}\sum_{\forall\lambda\in\mathbb{Z}_2^n} f^*(\lambda)\cdot(-1)^{\langle\lambda,x\rangle}$. The Cayley graph G_f associated with a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is defined on the vertex set $\mathbb{Z}_2^n$, with $u, w \in \mathbb{Z}_2^n$ adjacent if $w \oplus u \in \Omega_f = f^{-1}(1)$, or equivalently $f(w \oplus u) = 1$. For a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$, the spectrum of G_f is usually denoted by $Spec(G_f) = (|\Omega_f|, \lambda_1, ..., \lambda_{2^n-1})$ where $\lambda_i = \sum_{\forall x\in\mathbb{Z}_2^n} f(x)\cdot(-1)^{\langle b(i),x\rangle} = 2^n \cdot f^*(b(i))$ and $b(i)$ is the binary representation of i; the multiplicity of its largest eigenvalue $f^*(b(0))$ is $2^{n-dim\langle\Omega_f\rangle}$ (which implies the graph G_f is $|\Omega_f|$-regular with $2^{n-dim\langle\Omega_f\rangle}$ connected components and the graph G_f is connected if $dim\langle\Omega_f\rangle = n$). A Boolean functions is characterized by its spectrum if it is possible to identify its associated graph (i.e., determine all the details of its topology) only on the basis of the knowledge of its distinct eigenvalues, i.e., without using any information regarding their eigenvectors, see [6] for example. It is interesting to note that the fewer the number of distinct spectral coefficients are, the stronger are the algebraic properties of the set Ω_f; for instance, it is well-known that if a connected graph has exactly m distinct eigenvalues, then its diameter d satisfies $d \le m - 1$.

A Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called a *bent function* if $((-1)^{f(x)})^*(x) = \pm\frac{1}{\sqrt{2^n}}$ for any $\lambda \in \mathbb{Z}_2^n$, the term of bent was coined by Rothaus [8]. If $f(x)$ is a bent function on $\mathbb{Z}_2^n$ with $n \ge 3$, then $n = 2k$ must be even, and the degree of $f(x)$ is at most k; moreover $f(x)$ is irreducible whenever $deg(f(x)) = k \ge 3$, see [8] for details. The existence of bent functions $f(x)$ is equivalent to the fact that

whether $[(-1)^{f(x+y)}]$ is a Hadamard matrix.

A k-regular graph G is strongly regular if there exist non-negative integers λ and μ such that for all vertices x, y, the number $|G_1(x) \bigcap G_1(y)|$ of vertices adjacent to both x and y is λ if x and y are adjacent, and μ otherwise, where $G_1(x) = \{z | z \in V(G)$ is adjacent to $x\}$. A k-regular connected graph is strongly regular if and only if it has exactly three distinct eigenvalues $\theta_0 = k, \theta, \tau$, with multiplicities $1, m_\theta$, and m_τ respectively. This type of graph G is usually denoted by $SRG(v, k, \lambda, \mu)$ with $v = |V(G)|$, and $Spec(G) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$. A rephrase of Parseval's identity gives that $f^*(b(0)) = \sum_{i=0}^{2^n-1}(f^*(b(i)))^2$ and then yields the following useful equality $(k-\theta)(k-\tau) = 2^r(k+\theta\tau)$ where $k = |\Omega_f|$, and r must be replaced by $dim\langle\Omega_f\rangle$ if G is not connected. If G is strongly regular, then $\lambda = k + \theta\tau + \theta + \tau$ and $\mu = k + \theta\tau$. It was also observed that the class of bent functions is associated to a very special class of strongly regular graphs, and indeed identifies the bent functions precisely. Refer to [3,5] for more details on strongly regular graphs.

3. The Cayley Graphs associated with Bent Functions

If f is a Boolean function on $\mathbb{Z}_2^n$ with connected strongly regular graph G_f, then there exists $y \in \Omega_f$ such that $x \oplus y \in \Omega_f$ for each $x \in \mathbb{Z}_2^n \setminus \Omega_f$, and there exist h elements $z \in \Omega_f$ such that $y \oplus z \in \Omega_f$, where $h = \lambda$ if $y \in \Omega_f$, and μ if $y \notin \Omega_f$ for each $y \in \Omega_f$. In order to find a complete characterization of the class of functions with three distinct nonzero spectral coefficients with additional properties, it was proved in [2] that the quadratic equation $x^2 - 2^n x + (2^n - 1)y^2 = 0$ has integer solutions in x and y only if $y^2 = 0, 1, 2^{n-2}$. As a consequence, bent functions can be characterized as binary functions with a certain class of strongly regular graphs.

Theorem 3.1. $[1, 2]$ *The associated Caley graph G_f of a bent function f is a strongly regular graph $SRG(v, k, \lambda, \lambda)$; moreover, the bent functions are the only Boolean functions f whose associated graph G_f is a strongly regular graph $SRG(v, k, \lambda, \lambda)$*

Those graphs G_f with small numbers of distinct eigenvalues are considered: if G_f has a single eigenvalue, then $G_f = \overline{K_{2^n-1}}$; if G_f has two distinct eigenvalues, then G_f is either $\frac{2^n}{|\Omega_f|+1}K_{|\Omega_f|+1}$ when $b(0) \notin \Omega_f$, or $\frac{2^n}{|\Omega_f|}K_{|\Omega_f|}$ with loops otherwise; if G_f has three eigenvalues, then $(k, \theta, \tau) = (|\Omega_f|, 0, -|\Omega_f|)$ if and only if G_f is the complete bipartite graph between vertices in Ω_f and in $\mathbb{Z}_2^n \setminus \Omega_f$; $(k, \theta, \tau) = (|\Omega_f|, 0, \tau)$ if and only if G_f is a complete multipartite graph with $\overline{G_f} = (-\frac{|\Omega_f|}{\tau} + 1)K_{-\tau}$. If G_f is connected, then G_f is a $SRG(2^n, |\Omega_f|, \lambda, \mu)$ with

$$Spec(G_f) = (|\Omega_f|^1, (\tfrac{1}{2}(\lambda - \mu + \sqrt{\Delta}))^{(\frac{-\tau(2^n-1)-|\Omega_f|}{\theta-\tau})}, (\tfrac{1}{2}(\lambda - \mu - \sqrt{\Delta}))^{(\frac{-\theta(2^n-1)+|\Omega_f|}{\theta-\tau})})$$

where $\Delta = (\lambda - \mu)^2 - 4(\mu - |\Omega_f|)$.

Theorem 3.2. *If f is a bent function with connected G_f, then G_f is a strongly regular graph $SRG(v, k, \lambda, \lambda)$ with (v, k, λ) is either*

$$(2^n, 2^{n-1} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1})$$

or

$$(2^n, 2^{n-1} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1})$$

and with spectrum $Spec(G_f)$ either

$$((2^{n-1} + 2^{\frac{n}{2}-1})^{(1)}, (2^{\frac{n}{2}-1})^{(2^{n-1}-2^{\frac{n}{2}-1}-1)}, (-2^{\frac{n}{2}-1})^{(2^{n-1}+2^{\frac{n}{2}-1})})$$

or

$$((2^{n-1} - 2^{\frac{n}{2}-1})^{(1)}, (2^{\frac{n}{2}-1})^{(2^{n-1}-2^{\frac{n}{2}-1})}, (-2^{\frac{n}{2}-1})^{(2^{n-1}+2^{\frac{n}{2}-1}-1)})$$

respectively.

A table of all feasible parameters of strongly regular graphs with at most 280 vertices and related information is given in [4, pp671]. Those strongly regular graphs mentioned above with at most 280 vertices are included below in table 1, 2 respectively for complete purpose.

Table 1. case 1

Parameters	Spectrum	Examples
$4, 3, 2, 2$	$(3^{(1)}, 1^{(0)}, -1^{(3)})$	K_4
$16, 10, 6, 6$	$(10^{(1)}, 2^{(5)}, -2^{(10)})$	Clebsch graph; two graph
$64, 36, 20, 20$	$(36^{(1)}, 4^{(27)}, -4^{(36)})$	Two graph
$256, 136, 72, 72$	$(136^{(1)}, 8^{(119)}, -8^{(136)})$	Two graph

Table 2. case 2

Parameters	Spectrum	Examples
$4, 1, 0, 0$	$(1^{(1)}, 1^{(1)}, -1^{(2)})$	$\overline{K_4}$
$16, 6, 2, 2$	$(6^{(1)}, 2^{(6)}, -2^{(9)})$	Shirkhande; two graph; projective binary $[6, 4]$ code
$64, 28, 12, 12$	$(28^{(1)}, 4^{(28)}, -4^{(35)})$	QA$(4, 8)$; two graph; projective binary $[28, 6]$ code
$256, 120, 56, 56$	$(120^{(1)}, 8^{(120)}, -8^{(135)})$	QA$(8, 16)$; two graph; projective binary $[120, 8]$ code

4. Strongly Regular Graphs $SRG(v, k, \lambda, \lambda)$

The Friendship theorem shows that a connected graph with a unique common neighbor for any pairs of distinct vertices has a vertex adjacent to all other vertices, and K_3 is the unique such regular graph. We now consider those connected k-regular graphs such that any two distinct vertices has a constant λ common neighbors, they are indeed strongly regular graphs $SRG(v, k, \lambda, \lambda)$. When $\lambda = 1$, then $G = K_3$ as just mentioned. The Cayley graphs associated with bent functions provide a family of such graphs, as shown in Theorem 3.2.The symplectic graphs $Sp(2m)$ [5] offer another family of such strongly regular graphs with parameters $(2^{2m}-1, 2^{2m-1}, 2^{2m-2}, 2^{2m-2})$ for positive integers m, note that K_3 is the symplectic graph $Sp(2)$; some examples with small number of vertices are known already, for example:

Table 3. Symplectic graphs

Parameters	Spectrum	Example
$3, 2, 1, 1$	$(2^{(1)}, 1^{(0)}, -1^{(2)})$	
$15, 8, 4, 4$	$(8^{(1)}, 2^{(5)}, -2^{(9)})$	Two graph-*
$63, 32, 16, 16$	$(32^{(1)}, 4^{(27)}, -4^{(35)})$	Two graph-*; S$(2, 4, 28)$
$255, 128, 64, 64$	$(128^{(1)}, 8^{(119)}, -8^{(135)})$	Two graph-*; S$(2, 8, 120)$

where two graph-* is the graph with isolated point added belongs to the switching class of a regular two graph, and S$(2, k, v)$ is the block graph of a 2-$(v, k, 1)$ design. Some necessary conditions among v, k, λ and their spectrum is given in the following theorems.

Theorem 4.1. *Suppose there exists a $SRG(v, k, \lambda, \lambda)$ with $\lambda > 1$, and with distinct eigenvalues $k > \theta > \tau$, then*

1. *$\theta = -\tau = \sqrt{k-\lambda}$, $\theta\tau = -(k-\lambda)$ are integers with multiplicities $m_\theta = \frac{1}{2}((n-1) - \frac{k}{\sqrt{k-\lambda}})$, and $m_\tau = \frac{1}{2}((n-1) + \frac{k}{\sqrt{k-\lambda}})$ respectively.*
2. *$\theta \mid \lambda$ and $(v, k) = (\frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}, \theta^2+\lambda)$.*

Proof. 1. Omitted. 2. Let $t = \frac{k}{\sqrt{k-\lambda}}$, which is a positive integer by 1. Hence $k = \frac{t^2 \pm t\sqrt{t^2-4\lambda}}{2}$, both t and $b = \sqrt{t^2-4\lambda}$ are of the same parity; since $t^2 - 4\lambda = b^2$, it follows that $4\lambda = (t+b)(t-b)$,

$$t + b = \frac{k}{\sqrt{k-\lambda}} + \sqrt{(\frac{k}{\sqrt{k-\lambda}})^2 - 4\lambda} \text{ and}$$
$$t - b = \frac{k}{\sqrt{k-\lambda}} - \sqrt{(\frac{k}{\sqrt{k-\lambda}})^2 - 4\lambda}$$

must be even. Let $t + b = 2h_1$ and $t - b = 2h_2$ for some positive integers $h_1 > h_2$, hence $\lambda = h_1 h_2$, then $t = h_1 + h_2$, $b = h_1 - h_2$, and k is either $h_1(h_1+h_2)$ or $h_2(h_1+h_2)$. Note that $\theta = \sqrt{k-\lambda}$ is either h_1 (in case $k = h_1(h_1 + h_2)$) or h_2 (in case $k = h_2(h_1+h_2)$), hence $\theta \mid \lambda$. It follows that $n = \frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}$ in either case as required. □

Since $\theta = -\tau$ as shown in Theorem 4.1, a $SRG(v, k, \lambda, \lambda)$ turns out to be a Ramanujan graph [7]. Indeed, the above lemma paves a way for studying possible feasible parameters (v, k, λ, λ) for a given λ with a pair (h_1, h_2) either $(\theta, \frac{\lambda}{\theta})$ or $(\frac{\lambda}{\theta}, \theta)$. The trivial decomposition of $\lambda = 1 \cdot \lambda$ with $(h_1, h_2) = (\lambda, 1)$ leads to $(v, k, \lambda) = (\lambda^2(\lambda+2), \lambda(\lambda+1), \lambda)$ or $(\lambda+2, \lambda+1, \lambda)$. Another extremal cases with h_1, h_2 closed to $\sqrt{\lambda}$ are considered for $\lambda = 2^{2m}$ and $2^m(2^m+1)$ respectively. If $\lambda = 2^{2m}$ with $(h_1, h_2) = (2^m, 2^m)$, then

$$(v, k, \lambda) = (2^{2m+2} - 1, 2^{2m+1}, 2^{2m})$$

which is identical with those of the symplectic graphs; if $\lambda = 2^m(2^m+1)$ with $(h_1, h_2) = (2^m+1, 2^m)$, then

$$(v, k) = (2^2(2^m+1)^2, (2^m+1)(2^{m+1}+1)) \text{ or } (2^m(2^{m+2}), 2^m(2^{m+1}+1));$$

and the former type is realized by a set of 2^m MOLS of order $2^{m+1}+2$, called *Latin square graphs*.

Theorem 4.2. *Suppose $\lambda = p \cdot q$ for distinct primes with $p > q$.*

1. *If $q \geq 3$, then $(v, \theta) = (\frac{p(p+q-1)(p+q+1)}{q}, p)$, and $p = 2cq \pm 1$ for some integer c.*
2. *If $q = 2$, then $(v, \theta) = (\frac{p(p+1)(p+3)}{2}, p)$ or $(16, 2)$.*

Proof. Let $v = \frac{q(p+q-1)(p+q+1)}{p}$ by Theorem 4.1. Since p, q are primes and v is an integer, $(p+q-1)(p+q+1) \equiv 0 (\text{mod } p)$, and hence $q^2 \equiv 1 (\text{mod } p)$, and hence $q \equiv 1$ or $-1 (\text{mod } p)$. Because p is a prime, it follows that $q = cp \pm 1$ for some even integer c.

If $3 \leq q < p$, then $q = 1$ or $p-1$, a contradiction. Because p and q are odd primes and $p = cq \pm 1$ for some even integer c if $v = \frac{p(p+q-1)(p+q+1)}{q}$. It is easy to check that $\theta = p$ by theorem 4.1.

For $q = 2$, since p is odd, $(p+1)(p+3)$ is even, then either $(v, \theta) = (\frac{p(p+1)(p+3)}{2}, p)$ or $(v, \theta) = (\frac{2(p+1)(p+3)}{p}, 2)$. The only choice for p in the later case is 3, and hence $(v, \theta) = (16, 2)$. □

References

[1] A. Bernasconi and B. Codenotti, "Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem", *IEEE Trans. Computers*, Vol.48, No.3, Mar. 1999, pp. 345-351.

[2] A. Bernasconi and B. Codenotti, and J. VanderKam, "A Characterization of Bent Functions in terms of Strongly Regular Graphs", *IEEE Transactions on Computers*, Vol.50 No.9, September 2001, pp. 984-985.

[3] N. Biggs, *Algebraic Graph Theory 2nd edition*, Cambridge University Press, 1993.

[4] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, 1996.

[5] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer GTM 207, 2001.

[6] T. Huang and C. R. Liu, ”Spectral Characterization of Generalized Odd Graphs”, *Graph and Combinatorics*, 15, 1999, pp.195-209.

[7] A. Lubotzky, R. Phillips, and P. Sarnak, ”Ramanujan Graphs”, *Combinatorical*, vol.8, 1988, pp. 261-277.

[8] O. S. Rothaus, ”On Bent Functions”, *J. Combinatorial Theory (A)*, vol. 20, 1976, pp. 300-305.