行政院國家科學委員會專題研究計畫　成果報告

關於組合設計理論及其相關應用的研究(3/3)

計畫類別：個別型計畫
計畫編號：NSC93-2115-M-009-003-
執行期間：93 年 08 月 01 日至 95 年 01 月 31 日
執行單位：國立交通大學應用數學系(所)

計畫主持人：黃大原

報告類型：完整報告
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 95 年 1 月 17 日

Bent 函數及其相關的強正則圖

黃大原、游貴弘

布林函數 Walsh 質譜的計算的複雜度，一般而言十分困難。然而某些特定族類的該函數的值譜所具有的特殊性質，能有效降低其複雜度。值得一提的是布林函數 f 的值譜分析可轉化爲凱氏圖 Cayley Graphs 的質譜相關問題，因而代數圖論在 Bent 函數的研究裏，伴演一個十分積極的角色，由其是相異係數不大時爲然。我們據以得到其所對應的強正則圖的參數及其值譜；並且列出點數不超過 280 的所有可能情形。

The complexity of computing the Walsh spectrum of Boolean functions is difficult in general, however several interesting classes of such functions have a very special spectrum, whose ad hoc computation can be carried out significantly faster than in the general case. It is worth to note that the spectral analysis of Boolean functions can be viewed as a Cayley graph eigenvalue problem, this observations allow the using of tools from algebraic graph theory for investigations related to the spectral coefficients of Boolean functions, especially when the number of distinct coefficients is small. The main motivation for introducing the graph G_f is that its spectrum coincides with the Walsh spectrum of its associated Boolean function $f(x)$. This brings the problem of analyzing the spectral coefficients of Boolean functions into the framework of spectral analysis of graphs, i.e., it makes it possible to use techniques from graph spectra for the evaluation of spectral coefficients. More precisely, the results from algebraic graph theory can be applied to analyze Boolean functions with a few distinct spectral coefficients, the fewer is the number of distinct coefficients, the stronger are the algebraic properties of the function; this leads to a nice interpretation for the well-known class of bent functions in terms of strongly regular graphs.

Strongly Regular Graphs associated with Bent Functions

Tayuan Huang and Kuei You

Department of Applied Mathematics

National Chiao-Tung University

Hsinchu, Taiwan

thuang@math.nctu.edu.tw

The complexity of computing the Walsh spectrum of Boolean functions is difficult in general, however several interesting classes of such functions have a very special spectrum, whose ad hoc computation can be carried out significantly faster than in the general case. It is worth to note that the spectral analysis of Boolean functions can be viewed as a Cayley graph eigenvalue problem, this observations allow the using of tools from algebraic graph theory for investigations related to the spectral coefficients of Boolean functions, especially when the number of distinct coefficients is small. The main motivation for introducing the graph G_f is that its spectrum coincides with the Walsh spectrum of its associated Boolean function $f(x)$. This brings the problem of analyzing the spectral coefficients of Boolean functions into the framework of spectral analysis of graphs, i.e., it makes it possible to use techniques from graph spectra for the evaluation of spectral coefficients. More precisely, the results from algebraic graph theory can be applied to analyze Boolean functions with a few distinct spectral coefficients, the fewer is the number of distinct coefficients, the stronger are the algebraic properties of the function; this leads to a nice interpretation for the well-known class of bent functions in terms of strongly regular graphs.

1. Bent Functions

The Fourier transform of a Boolean function $g(x): Z_2^n \to Z_2$ is defined to be

$$g^*(\lambda) = \frac{1}{2^n} \sum_{\forall x \in Z_2^n} g(x) \cdot (-1)^{\langle \lambda, x \rangle}.$$

It is known that $g(x) = \sum_{\forall \lambda \in Z_2^n} g^*(\lambda) \cdot (-1)^{\langle \lambda, x \rangle}$. A Boolean function $f: Z_2^n \to Z_2$ is called a *bent function* if $\left((-1)^{f(x)}\right)^*(\lambda) = \pm \frac{1}{\sqrt{2^n}}$ for any $\lambda \in Z_2^n$, the term of bent was coined by Rothaus [9].

Theorem [9]

If $f(x)$ is a bent function on Z_2^n with $n \geq 3$, then $n = 2k$ must be even, and the degree of $f(x)$ is at most k; moreover $f(x)$ is irreducible whenever $\deg(f(x)) = k \geq 3$.

Some basic properties of bent functions together with their relationships with some combinatorial structures are summarized in the following theorem. The Boolean function $f(x)$ is bent if and only if the matrix $[(-1)^{f(x+y)}]$ is a Hadamard matrix. The Fourier transform of a bent function is again a bent function.

2. The Cayley Graphs associated with Bent Functions

The Cayley graph $G_f = (V(f), E_f)$ associated with a Boolean function $f : Z_2^n \to Z_2$ is defined on the vertex set $V(f) = Z_2^n$, with $u, w \in Z_2^n$ adjacent if $w \oplus u \in \Omega_f = f^{-1}(1)$, or equivalently $f(w \oplus u) = 1$. The graph G_f is $|\Omega_f|$ - regular with $2^{n-\dim\langle \Omega_f \rangle}$ connected components, the graph G_f is connected if $\dim\langle \Omega_f \rangle = n$. The spectrum of G_f is usually denoted by $Spec(G_f)$ = $(|\Omega_f|, \lambda_1, ..., \lambda_{2^n-1})$ where $\lambda_i = \sum_{\forall x \in Z_2^n} f(x).(-1)^{\langle b(i), x \rangle} = 2^n \cdot f^*(b(i))$

Upper and lower bounds on the rank (over the real field) of the adjacency matrix A_f of G_f i.e., the number of nonzero spectral coefficients of the function f, are given in terms of degrees of polynomials representation of f. Some properties of the Fourier coefficients and its associated Cayley graphs are given in the following.

Theorem [1] If $f : Z_2^n \to Z_2$, and $\lambda_i, 0 \le i \le 2^n - 1$, are the eigenvalues of the graph G_f, then

a. $\lambda_i = 2^n f^*(b(i))$ for $0 \le i \le 2^n - 1$;

b. 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. 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 k-regular graph G is *strongly regular* if there exist nonnegative integers a and c such that for all vertices u, v, the number $| G_1(u) \cap G_1(v) |$ of vertices adjacent to both u and v is a if u and v are adjacent, and c otherwise. A k- regular connected graph is strongly regular if and only if it has exactly three distinct eigenvalues $\lambda_0 = k$, λ_1, λ_2. A rephrase of Parseval's identity gives that $f^*(b(0)) = \sum_{i=0}^{2^{k-1}} (f^*(b(i)))^2$ and then yields the following useful quality $(k - \lambda_1)(k - \lambda_2) = 2^r (k + \lambda_1 \lambda_2)$ 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 $a = k + rs + r + s$ and $c = k + rs$. It was also observed that the class of bent functions is associated to a very special class of strongly regular graphs indeed exactly identifies the bent functions.

Theorem [1]

If G_f is a connected strongly regular graph, then there exists $v \in \Omega_f$ such that $u \oplus v \in \Omega_f$ for each $u \in Z_2^n \setminus \Omega_f$, and there exist h elements $w \in \Omega_f$ such that $v \oplus w \in \Omega_f$, where $h = e$ if $v \in \Omega_f$, and d if $v \notin \Omega_f$. for each $v \in Z_2^n$,

In order to find a complete characterization of the class of functions with three distinct nonzero spectral coefficients and with the additional property $a = c$, we are then left with the problem of understanding whether or not there exists other integer solutions to $x^2 - 2^n x + (2^n - 1)y^2 = 0$. It was proved in [2] that the equation 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 [1,2]

a. The associated Caley graph G_f of a bent function is a strongly regular graph $SRG(v,k,\lambda,\lambda)$.

b. The bent functions are the only binary 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 either $G_f = \frac{2^n}{|\Omega_f|+1} K_{|\Omega_f|+1}$ when $b(0) \notin \Omega_f$, or $G_f = \frac{2^n}{|\Omega_f|} K_{|\Omega_f|}$ with loops otherwise; if G_f has three eigenvalues, then

a. $(\lambda_0, \lambda_1, \lambda_2) = (|\Omega_f|, 0, -|\Omega_f|)$ if and only if G_f is the complete bipartite graph between vertices in Ω_f and in $Z_2^k \setminus \Omega_f$.

b. $(\lambda_0, \lambda_1, \lambda_2) = (|\Omega_f|, 0, \lambda_2)$ if and only if G_f is a complete multipartite graph with $\overline{G_f} = (-\frac{|\Omega_f|}{\lambda_2} + 1) K_{-\lambda_2}$ and with $Spec(G_f) = ((2^{n-1})^{(1)}, (0)^{(2^n - 1 + \frac{2^{n-1}}{\lambda_2})}, (\lambda_2)^{(-\frac{2^{n-1}}{\lambda_2})})$

c. if G_f is connected, then G_f is a $SRG(2^n, |\Omega_f|, e, d)$ with

$$Spec(G_f) = \left(|\Omega_f|^1, \left(\frac{1}{2}\left(e - d + \sqrt{(e-d)^2 - 4(d - |\Omega_f|)}\right)\right)^{\left(\frac{-\lambda_2(2^n-1)-|\Omega_f|}{\lambda_1-\lambda_2}\right)},\right.$$
$$\left.\left(\frac{1}{2}\left(e - d - \sqrt{(e-d)^2 - 4(d - |\Omega_f|)}\right)\right)^{\left(\frac{\lambda_1(2^n-1)+|\Omega_f|}{\lambda_1-\lambda_2}\right)}\right)$$

Theorem if f is a bent function with connected G_f, then G_f is a strongly regular graph SRG(v,k,) with

$$(v,k,l.\,) = (2^n, 2^{n-1} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}) \text{ or}$$
$$(2^n, 2^{n-1} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1})$$

$$Spec(G_f) = ((2^{n-1}+2^{\frac{n}{2}-1})^{(1)}, (2^{\frac{n}{2}-1})^{(2^{n-1}-2^{\frac{n}{2}-1}-1)}, (-2^{\frac{n}{2}-1})^{(2^{n-1}+2^{\frac{n}{2}-1})}) \quad \text{or}$$

$$Spec(G_f) = ((2^{n-1}-2^{\frac{n}{2}-1})^{(1)}, (2^{\frac{n}{2}-1})^{(2^{n-1}-2^{\frac{n}{2}-1})}, (-2^{\frac{n}{2}-1})^{(2^{n-1}+2^{\frac{n}{2}-1}-1)}).$$

3. Strongly Regular Graphs *SRG*(*n*,*k*,*λ*,*λ*)

The Friendship theorem shows that a connected graph with a unique common neighbor for any pairs of distinct vertices has a vertex adjacent to its 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 number of λ common neighbors, they are strongly regular graphs $SRG(n, k, \lambda, \lambda)$. When $\lambda = 1$, then G = K_3 as just mentioned. The symplectic graphs $Sp(2m)$ offer a 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 $Sp(2)$. The Cayley graphs associated with bent functions provide another family of such graphs.

Theorem: Suppose there exists a $SRG(n, k, \lambda, \lambda)$ 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
$$m_\theta = \frac{1}{2}((n-1) - \frac{k}{\sqrt{k-\lambda}}), \text{ and } m_\tau = \frac{1}{2}((n-1) + \frac{k}{\sqrt{k-\lambda}}).$$
2. $\theta \mid \lambda$ and $(n,k) = (\frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}, \theta^2+\lambda)$.

Proof: (1). Available in monographs, 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 $4\lambda = (t+b)(t-b)$, both

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

must be even. Let $t + b = 2h_1$ and $t - b = 2h_2$ for some positive integers $h_1 > h_2$, hence $\lambda = h_1h_2$, 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. Q.E.D.

The above lemma paves a way for studying possible feasible parameters (v, k, λ, λ) for a given λ with a pair $(h_1, h_2) = (\theta, \lambda/\theta)$ or $(\lambda/\theta, \theta)$. The trivial decomposition of $\lambda = 1 \cdot \lambda$

with $(h_1,h_2)=(\lambda,1)$ leads to (v, k, λ, λ) = $(\lambda^2(\lambda+2),\lambda(\lambda+1),\lambda,\lambda)$ or $(\lambda+2,\lambda+1,\lambda,\lambda)$.
The other extremal cases with h_1,h_2 close 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, λ, λ) = $(2^{2m+2}-1,2^{2m+1},2^{2m},2^{2m})$ which is identical with those of the symplectic graphs.

If $\lambda=2^m(2^m+1)$, then (v, k, λ, λ) =

$(2^2(2^m+1)^2,(2^m+1)(2^{m+1}+1),2^m(2^m+1),2^m(2^m+1))$ or

$(2^m(2^{m+2}),2^m(2^{m+1}+1),2^m(2^m+1),2^m(2^m+1))$

respectively with $(h_1,h_2)=(2^m+1,2^m)$ respectively. For the symplectic graphs *Sp*(2(*m*+1)), which is a $SRG(2^{2m+2}-1,2^{2m+1},2^{2m},2^{2m})$ with spectrum

$Spec(G)=((2^{2m+1})^1,(2^m)^{2^{2m+1}-2^m-1},(-2^m)^{2^{2m+1}+2^m-1})$,

some examples with small number of vertices are known already, for example:

SRG(3, 2, 1, 1) with $Spec(G)=(2^1,1^0,(-1)^2)$,

SRG(15, 8, 4, 4) with $Spec(G)=(8^1,2^5,(-2)^9)$,

SRG(63, 32, 16, 16) with $Spec(G)=(32^1,4^{27},(-4)^{35})$, and

SRG(255, 128, 64, 64) with $Spec(G)=(128^1,8^{119},(-8)^{135})$.

References:

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

[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, 984-985 September (2001)

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

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

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

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

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