國 立 交 通 大 學

應用數學系

碩 士 論 文

強正則圖的研究

A Study of Strongly Regular Graph

SRG*(*v*, *k*, *λ*, *μ*) base on *μ* – *λ

研 究 生：尤 貴 弘

指導老師：黃 大 原　教 授

中 華 民 國 九 十 三 年 六 月

強正則圖的研究

A Study of Strongly Regular Graph

$SRG(v, k, \lambda, \mu)$ base on $\mu - \lambda$

研 究 生：尤貴弘　　**Student**: Kuei-Hong You

指導老師：黃大原 教授　**Advisor**: Tayuan Hwang

國 立 交 通 大 學

應用數學系

碩 士 論 文

A Thesis

Submitted to Department of Applied Mathematics

College of Science

National Chiao Tung University

In partial Fulfillment of Requirement

For the Degree of Master

In

Applied Mathematics

June 2004

Hsinchu, Taiwan, Republic of China

中 華 民 國 九 十 三 年 六 月

強正則圖的研究

研 究 生：尤 貴 弘　　指導老師：黃 大 原 教 授

國 立 交 通 大 學

應 用 數 學 系

摘　要

Friendship定理說明當一個連通圖形滿足任兩點恰有一共同鄰點時，除了三個點的完全圖之外，此圖必不為正則圖。也就是說所有 $\lambda = \mu = 1$ 的強正則圖只有K_3一個。在這篇文章中，我們從 λ 的分解來討論一些 $\lambda = \mu > 1$ 時的正則圖存在的必要條件，並且討論如Ramanujan圖及Symplectic圖等屬於該類圖形的一些性質。除此之外，文章中亦整理了一些 $\mu - \lambda$ 值不大的正則圖。

中 華 民 國 九 十 三 年 六 月

A Study of Strongly Regular Graphs $SRG(v, k, \lambda, \mu)$ based on $\mu - \lambda$

Student: Kuei-Hong You Advisor: Tayuan Huang

Department of Applied Mathematics
National Chiao Tung University
Hsinchu 30050 Taiwan R.O.C.

June 23, 2004

Abstract

The friend theorem excludes all strongly regular graphs with $\mu = \lambda = 1$ except K_3. In this thesis, we study some necessary conditions for strongly regular graphs with $\mu = \lambda > 1$ based on the decompositions of λ, including the families of Ramanujan graphs and symplectic graphs as examples. A survey of strongly regular graphs with small value of $\mu - \lambda$ were also given in this thesis.

誌　謝

在這兩年的研究所生活中，感謝我的指導老師黃大原教授對我的包容及在學業及生活上諸多指導及關心，讓我順利的完成論文，並在各個方面都受益良多。也感謝陳秋媛老師的關心與翁志文老師、黃光明老師及傅恆霖老師的教導，讓我接觸到數學中更多不同的領域。

其次，要謝謝組合組的所有同學們，抄君、正傑、昭芳、喻培、宏嘉、榮丰、嘉文、致維、建緯、啟賢、文祥，特別是致維的大學同學們，讓我開心快樂地度過這兩年。感謝我大學時代的同學德筌總是能在我困惑的時候給予適當的意見及建議。還有要感謝祐寧、曲敏、宜誠等學妹們大力協助我的論文的完成，有了妳們讓我輕鬆多了。

最後感謝所有幫助過我的所有人，希望我將來也能成為幫助別人的人。

Contents

Chapter 1

Introduction

The theory of designs concerns itself with questions about subsets of a set possessing a high degree of regularity. By contrast, the large and amorphous area called "graph theory" is mainly concerned with questions about general relations on a set. There are some places where the two theories have interacted fruitfully. The unifying theme is provided by a class of graphs, the strongly regular graphs, introduced by Bose (1963), whose definition reflects the symmetry inherent in t-designs. There are some easy examples that the block graph of quasi-symmetric designs, and line graphs of 2-$(v, k, 1)$ designs are strongly regular graphs.

In addition to design theory, strongly regular graphs occur in many areas of computer science like digital logic, network security, and telecommunication networks. Since 0 and 1 are the only messages computer can recognized, Boolean function is used frequently. Spectral techniques have been widely used since the 70s in logic synthesis, testing, function classification, and other applications in logic circuits. Moreover, several authors have analyzed the *Walsh spectrum* of Boolean functions, and found links between properties of the spectrum and certain computational questions related to the functions.

There are many useful tools for analyzing strongly regular graphs since the existence of strongly regular graphs are not necessarily determined by their parameters. Some necessary conditions over v, k, λ, μ of $SRG(v, k, \lambda, \mu)$ are given in Chapter 2 including *Krein condition* and *Seidel's absolute bound*. A few families, such as $T(n)$, $L_2(n)$, *Payley graph*, etc., of *SRG* are also included in Chapter 2. Besides, the technique of matrix is another tool which associated algebra theory to graph theory. In analyzing a problem, decomposing a question into small pieces of easier questions is used frequently. The technique of *local eigenvalue* is a method discussing an introduced subgraph, with smaller order, of a strongly regular graph with known parameters, or constructing a graph from its introduced subgraphs. A common

feature among *SRG*, *BIBD* and *BGW* matrices is studied in Section 2.5.

Viewing a vertex as a person in a party, since we only discussing simple graphs, the edge with no direction means the relation between any pair of persons is symmetric. In Chapter 3, we review the history of friendship theorem and generalize it as a *SRG* with $\mu = \lambda$. We discuss the decomposition of λ, use the divisors of λ to find the formula of v and k which is a feasible parameters set, and give some feasible conditions from it. Finally, we present a family of $SRG(v, k, \lambda, \lambda)$, *symplectic graph*, to end this section.

As we consider a *Cayley graph* associated a Boolean function, *bent function* introduced in Section 4.1, a special case of Boolean function is related to a class of strongly regular graph with $\mu = \lambda$. Bent functions is often used to build the S-box in conventional encryption of network security. In the telecommunication network, strongly regular graphs with $|\mu - \lambda| \leq \frac{3k-4}{2\sqrt{k-1}}$ are all *Ramanujan graphs*, introduced in Section 4.2. Ramanujan graph is very interesting in telecommunication network because of its small absolute value, which implies small diameter, of the next to the largest eigenvalue. It means that a Ramanujan graph can be used to construct a good communication network which spreads information fast and costs less.

A survey of strongly regular graphs with small $|\mu - \lambda|$ will be given in Chapter 5, including the family of *Moore graphs* with $(\lambda, \mu) = (0, 1)$ and the family of *conference graphs* with $\mu - \lambda = 1$ in general. In addition to *symplectic graphs*and *bent functions*, mentioned in Chapters 3 and 4, symmetric 2-designs also provide some strongly regular graphs with $\mu - \lambda = 0$ or 2, some relations between them can be found in Section 5.2.

Chapter 2

Preliminaries

In this chapter, some basic properties of *SRG* and designs are given in Section 2.1, their matrix representations together with spectrums will be considered too. From these properties, some useful necessary conditions will be represented. In Section 2.2, we give some techniques which are useful in computing the eigenvalues of adjacency matrices and we can see some relations between the adjacency matrices of the *first and second subconstituents*.

Definition 1. *Let Γ be a k-regular graph of order v with the following properties that each pair of adjacent vertices has λ common neighbors and each pair of nonadjacent vertices has μ common neighbors. Then Γ is said to be strongly regular with parameters (v, k, λ, μ).*

Theorem 2.0.1 ([19]pp.218). *Assume that Γ is a $SRG(v, k, \lambda, \mu)$.*

1. *The complement graph $\overline{\Gamma}$ of Γ is also a strongly regular graph with parameters $(v, \overline{k}, \overline{\lambda}, \overline{\mu})$ where $\overline{k} = (v-1) - k$, $\overline{\lambda} = (v-2) - 2k + \mu$, $\overline{\mu} = (v-2) - (k-1) - (k-1) + \lambda$.*

2. *$k(k - \lambda - 1) = (v - k - 1)\mu$.*

	Parameters				Eigenvalues
Γ	v	k	λ	μ	$\frac{(\lambda-\mu)\pm\sqrt{(\lambda-\mu)^2+4(k-\mu)}}{2}$
$\overline{\Gamma}$	v	$v-k-1$	$v-2k-2+\mu$	$v-2k+\lambda$	$\frac{(\mu-\lambda-2)\pm\sqrt{(\mu-\lambda-2)^2+4(k-\lambda-1)}}{2}$

The second property can be obtained by counting the number of edges between $\Gamma_1(x)$ and $\Gamma_2(x)$ for arbitrary vertex x in two ways where $\Gamma_j(x)$ is defined as the set of vertex u satisfying $d(x, u) = j$. For the connectivity of Γ, a $SRG(v, k, \lambda, \mu)$, there are some statements are equivalent: Γ is not connected, $\mu = 0$, $\lambda = k - 1$, and $\Gamma = mK_{k+1}$ for some $m > 1$.

Definition 2. *A connected graph Γ is called distance-regular if there are integers $b_i, c_i, i = 0, 1, ..., d$ such that for any distinct vertices x, y with $d(x, y) = i$, then $\Gamma_{i-1}(x) \cap \Gamma_1(y) = b_i$ and $\Gamma_{i+1}(x) \cap \Gamma_1(y) = c_i$.*

2.1 Matrix interpretations of *SRG* and *BIBD*

Since the complete graphs are the trivial strongly regular graphs, we only consider those not complete and whose complement is also connected. Suppose A is the adjacency matrix of a connected strongly regular graph Γ. The entry uv of A^2 is the number of walks of length 2 from u to v. Therefore, from the definition of strongly regular graph we have

$$A^2 = kI + \lambda A + \mu(J - I - A)$$

which can be rewritten as

$$A^2 - (\lambda - \mu)A - (k - \mu)I = \mu J.$$

Since Γ is k-regular, k is an eigenvalue with all one vector as its eigenvector, other eigenvalues of A can be found explicitly.

The first part of the following theorem yields a powerful feasibility condition. Given a parameter set we can compute m_θ and m_τ using these formulas. If the results are not integers, then there is no such a strongly regular graph with these parameters. In practice this is a very useful condition, called the *Integrality Condition*, as we shall see in Theorem 3.2.1. The classical application of this idea is to determine the possible valencies for a Moore graph with diameter 2. The third part is another bound called *absolute bound*. Two methods are known to derive the final part of the following theorem, called *Krein bound*. The first one, consider a strongly regular graph as a *two-class association scheme*, see details in [27, pp.237-238]. The second one is more elementary, which uses *Cauchy-Schawrtz inequality* and the discriminant of a quadratic polynomial to get these two inequalities, but seems not easy to generalize to distance-regular graphs in general.

Theorem 2.1.1 ([19], pp.220-221). *Suppose Γ is a $SRG(v, k, \lambda, \mu)$ with $Spec(\Gamma) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$, then*

1. $\theta = \dfrac{(\lambda - \mu) + \sqrt{\Delta}}{2}$, $\tau = \dfrac{(\lambda - \mu) - \sqrt{\Delta}}{2}$, *with multiplicities*

$$m_\theta = \frac{1}{2}((v-1) - \frac{2k + (v-1)(\lambda - \mu)}{\sqrt{\Delta}}) \text{and}$$
$$m_\tau = \frac{1}{2}((v-1) + \frac{2k + (v-1)(\lambda - \mu)}{\sqrt{\Delta}})$$

respectively, where $\Delta = (\theta - \tau)^2 = (\lambda - \mu)^2 + 4(k - \lambda)$;

2. $\lambda = k + \theta + \tau + \theta\tau$, $\mu = k + \theta\tau$ *and* $m_\theta m_\tau(\theta - \tau)^2 = vk\overline{k}$;

3. *(the absolute bound)*
   $v \leq \frac{1}{2}m_\theta(m_\theta + 3)$ *and* $v \leq \frac{1}{2}m_\tau(m_\tau + 3)$;

4. *(the Krein bound)*

$$\theta\tau^2 - 2\theta^2\tau - \theta^2 - k\theta + k\tau^2 + 2k\tau \geq 0 \text{ and}$$
$$\theta^2\tau - 2\theta\tau^2 - \tau^2 - k\tau + k\theta^2 + 2k\theta \geq 0.$$

   If the first inequality is tight, then $k \geq m_\theta$, *and if the second is tight, then* $k \geq m_\tau$. *If either of the inequalities is tight, then one of the following is true:*

   (a) Γ *is the 5-cycle* C_5.

   (b) *Either* Γ *or* $\overline{\Gamma}$ *has all its induced subgraphs over* $\Gamma_1(x)$ *empty, and all its induced subgraphs over* $\Gamma_2(x)$ *strongly regular.*

   (c) *All subconstituents of* Γ *are strongly regular.*

Proof.

1. Since Γ is k-regular, the all one vector is the eigenvector of eigenvalue k and other eigenvectors are orthogonal to it. From $A^2 - (\lambda - \mu)A - (k - \mu)I = \mu J$, the remaining eigenvalues θ and τ which are represented as the theorem are the roots of the quadratic equation $x^2 - (\lambda - \mu)x - (k - \mu) = 0$. Because Γ is connected and the sum of the eigenvalues equals $trace(A) = 0$. It follows that the corresponding multiplicities are 1, $m_\theta = -\frac{(v-1)\tau+k}{\theta-\tau}$ and $m_\tau = \frac{(v-1)\theta+k}{\theta-\tau}$. Applying $\theta = \frac{(\lambda-\mu)+\sqrt{\Delta}}{2}$ and $\tau = \frac{(\lambda-\mu)-\sqrt{\Delta}}{2}$, $m_\theta = \frac{1}{2}((v-1) - \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{\Delta}})$ and $m_\tau = \frac{1}{2}((v-1) + \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{\Delta}})$.

2. We only prove the last equality.

$$m_\theta m_\tau = (-\frac{(v-1)\tau + k}{\theta - \tau})(\frac{(v-1)\theta + k}{\theta - \tau}) = \frac{-(v-1)^2\theta\tau - (v-1)(\theta+\tau)k - k^2}{(\theta-\tau)^2}$$

   Replace $\theta\tau$ by $\mu - k$, $\theta + \tau$ by $\lambda - \mu$ and k by $v - 1 - \overline{k}$, then

$$\begin{aligned} m_\theta m_\tau(\theta - \tau)^2 &= -(v-1)^2\theta\tau - (v-1)(\theta+\tau)k - k^2 \\ &= (v-1)^2(k-\mu) - (v-1)(\lambda-\mu)k - k(v-1-\overline{k}) \\ &= (v-1)((v-1-k)k - (v-1-k)\mu + k(k-\lambda-1)) + k\overline{k}. \end{aligned}$$

   Because $(v-1-k)\mu = k(k-\lambda-1)$, hence $m_\theta m_\tau(\theta-\tau)^2 = (v-1)k\overline{k} + k\overline{k} = vk\overline{k}$.

□

There is a theorem showing us that we can easily determine whether a graph is strongly regular or not by the number of distinct eigenvalues and their multiplicities, since it is a necessary and sufficient condition for an existent graph.

Theorem 2.1.2. *A graph is a strongly regular graph if and only if it has exactly three eigenvalues.*

Proof. Because A has exactly three distinct eigenvalues, the minimal polynomial of A is $f(x) = (x-k)(x-\theta)(x-\tau) = (x-k)g(x)$. Therefore, $f(A) = (A-kI)g(A) = 0$ and $Ag(A) = kg(A)$. Hence, $g(A) = tJ$ for some t, and J is a linear combination of A^2, A, and I. □

Definition 3. *Let v', k' and λ' be positive integers such that $v' > k' \geq 2$. A (v', k', λ')-balanced incomplete block design (which we abbreviate to (v', k', λ')-BIBD), which is also called a 2-(v', k', λ') design, is a pair $(X, \mathcal{B})$ such that the following properties are satisfied:*

1. *X is a set of v' elements called points,*
2. *$\mathcal{B}$ is a collection of subsets of X called blocks,*
3. *each block contains exactly k' points, and*
4. *every pair of distinct points is contained in exactly λ' blocks.*

It is often convenient to represent a *BIBD* by means of an incidence matrix. Let $X = \{x_1, x_2, ..., x_{v'}\}$ and $\mathcal{B} = \{B_1, B_2, ..., B_b\}$. The incidence matrix of $(X, \mathcal{B})$ is the $v' \times b$ 0-1 matrix $M = (m_{ij})$ where $m_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j \end{cases}$

From the definition, we have $JM = kJ$ and $MM^T = rI + \lambda(J - I)$ for any incidence matrix M of a 2-design. A 2-design in which $b = v$ is called *symmetric*. Here are some properties of symmetric 2-designs.

Theorem 2.1.3 ([32], pp.12). *Let $\Pi = (X, \mathcal{B})$ be a 2-(v', k', λ') design. The followings are equivalent.*

1. *$|B_i \cap B_j| = \lambda'$ for any pair B_i, $B_j \in \mathcal{B}$;*
2. *Π is a symmetric design.*

From the above theorem, a symmetric 2-design has the property that the intersection of each pair of distinct blocks has unique cardinality. If the number of cardinalities becomes two, then this 2-design is called a *quasi-symmetric design*. Let $x < y$ be the two cardinalities of block intersection in a quasi-symmetric design. The *block graph* of a quasi-symmetric design has as vertices the blocks, two vertices adjacent if they intersect y points.

As we know, a connected graph is a strongly regular graph if and only if its adjacency matrix has exactly three distinct eigenvalues. By the property, a block graph of a quasi-symmetric design is a strongly regular graph and we will represent the parameters of SRG by its eigenvalues, see details in Section 5.3.

Definition 4. *Let $\Pi = (X, \mathcal{B})$ be a 2-(v', k', λ') design. Π is called an affine resolvable design if the following properties are satisfied:*

1. *There is a partition $\{\pi_1, \pi_2, ..., \pi_r\}$ of $\mathcal{B}$ such that each π_i is a set of disjoint blocks whose union is X.(resolvable property)*
2. *$b = v' + k' + \lambda' - 1$ where $|\mathcal{B}| = b$.*

Since any two blocks from different π_i of an affine resolvable design intersect in exactly $\frac{k^2}{v}$ points [32, pp.36], it is a quasi-symmetric design with $x = 0$ and $y = \frac{k^2}{v}$.

In order to associated algebraic theory to the area of graph theory, we transfer a graph to an adjacency matrix or an incidence matrix. Similarly, design theory can be associated to algebraic theory by the incidence matrix of a design. The previous two classes of matrix are 0-1 matrices; there is another class of matrix whose entries are not just 0 and 1 but the elements of a finite group, called *balanced generalized weighing matrix*, having similar behavior as the adjacency matrix of a strongly regular graph and the incidence matrix of a symmetric 2-design.

Definition 5. *Let $(G, \cdot)$ be a finite group, $W = (\alpha_{ij})_{v\times v}$ a matrix over $G \cup \{0\}$. If each row of W contains exactly k nonzero entries and, for distinct $i, h \in \{1, 2, ..., v\}$, the multi-set $\{\alpha_{hj}^{-1}\alpha_{ij} : 1 \le j \le v, \alpha_{ij} \neq 0, \alpha_{hj} \neq 0\}$ contains exactly $\frac{\lambda}{|G|}$ copies of each element of G. Then W is called a balanced generalized weighing matrix with parameters (v, k, λ) over G or a $BGW(v, k, \lambda)$.*

Most of the known BGW belong to the family $(\frac{q^{d+1}-1}{q-1}, q^d, q^d - q^{d-1})$ over a cyclic group G, where q is a prime power, d is a positive integer, and the order of G divides $q - 1$. Suppose R is the group ring of a finite group G over the rationals. $W^* = (\alpha_{ij}^*)^T$, $\alpha_{ij}^* = \alpha_{ij}^{-1}$ if $\alpha_{ij} \in G$ and $\alpha_{ij}^* = 0$ if $\alpha_{ij} = 0$. Then W is a $BGW(v, k, \lambda)$ if and only if

$$WW^* = (ke)I + (\frac{\lambda}{|G|}G)(J - I)$$

where e is the identity of G, G stands for the sum of all elements of G in R, I is the identity matrix, and J is the matrix with all entries equal to e. The form is similar to the quadratic form of

$$NN^T = kI + \lambda(J - I)$$

where N is an incidence matrix of a symmetric 2-(v, k, λ) design. If N is also a symmetric matrix with all diagonal entries equal to 0, then N is an adjacency matrix of $SRG(v, k, \lambda, \lambda)$. Because

$$A^2 = kI + \lambda A + \mu(J - I - A)$$

for any adjacency matrix A of a strongly regular graph.

2.2 A technique in terms of local eigenvalues

If we have constructed a graph and want to know whether it is strongly regular or not, the previous section gives a sufficient and necessary condition by computing its eigenvalues. But given a feasible parameter set, it is still difficult to know the existence of the corresponding graph. There is much algebraic theory useful to analysis the adjacency matrix of graph. C. Godsil and G. Royle [19] discuss the properties of the eigenvalues of two special induced subgraphs, whose vertex sets are the vertices at distance one or two from an arbitrary vertex respectively, and use it to prove the uniqueness of *Clebsch graph*.

Definition 6. *Let* $A = \begin{bmatrix} 0 & 1^T & 0 \\ 1 & A_1 & B^T \\ 0 & B & A_2 \end{bmatrix}$ *be the adjacency matrix of a strongly regular graph* Γ *with a partition* $\{u\} \cup \Gamma_1(u) \cup \Gamma_2(u)$ *of* $V(\Gamma)$.

1. *A_1 and A_2 are called the first and second subconstituents of graph Γ relative to u respectively.*

2. *If an eigenvalues of A_i, $i = 1, 2$ is not an eigenvalue of A and orthogonal to the all one vector, then it is called a local eigenvalue.*

In discussing the subconstituents of a strongly regular graph, there is an interesting result that *5-cycle* is the only connected strong regular graph whose complement is connected, A_1 is empty, and A_2 is complete. And the *Clebsch graph*(see details in Section 2.4) provides an example where A_1 is empty and A_2 is *Petersen graph*. These two graphs approach the tight Krein bound as Theorem 2.1.1. in previous section.

Definition 7. *A partition $\pi = \{C_1, C_2, ..., C_r\}$ of $V(\Gamma)$ is called an equitable partition if the number of neighbors in C_i of a vertex u in C_j is a constant c_{ij}, which is independent of u.*

The first and second subconstituents of a strongly regular graph are regular graphs and the edges joining any two distinct cells forms a semiregular bipartite graph. The partition $\pi = \{u\} \cup \Gamma_1(u) \cup \Gamma_2(x)$ of $V(\Gamma)$ is an *equitable partition.*

For any adjacency matrix A as following, each diagonal cell is an adjacency matrix of an induced subgraph.

$$A = \begin{bmatrix} A_1 & B_1 & B_2 \\ B_3 & A_2 & B_4 \\ B_5 & B_6 & A_3 \end{bmatrix}$$

If the rowsums of each submatrix of A are the same, i.e., π is also an equitable partition, then we have a 3×3 matrix

$$A/\pi = \begin{bmatrix} rowsumofA_1 & rowsumofB_1 & rowsumofB_2 \\ rowsumofB_3 & rowsumofA_2 & rowsumofB_4 \\ rowsumofB_5 & rowsumofB_6 & rowsumofA_3 \end{bmatrix}$$

The three eigenvalues of A/π are identical with those of A, and we can see that every strongly regular graph has an equitable partition which make the rowsums of each submatrix are the same and

$$A/\pi = \begin{bmatrix} 0 & k & 0 \\ 1 & \lambda & k-\lambda-1 \\ 0 & \mu & k-\mu \end{bmatrix}$$

Here we introduce a technique used to compute the eigenvalues of adjacency matrices, and can be used in proving following lemmas. Suppose there is a quadratic equation of matrix A. Assume an eigenvalue of A is θ, and $Ax = \theta x, x \neq 0$. Multiply eigenvector x to both sides of the equation. Then, the equation can be transferred to an equation of θ. For example, $A^2 + aA + bI = B^T B$, and θ_1, θ_2 are the roots of $\theta^2 + a\theta + b = 0$ with $\theta_1 > \theta_2$;

1. if $Bx = 0$, then $(A^2 + aA + bI)x = B^T Bx = 0$, $\theta^2 + a\theta + b = 0$, hence $\theta_1 + \theta_2 = -a$, $\theta_1\theta_2 = b$.

2. if $Bx \neq 0$, then $(A^2 + aA + bI)x = B^T Bx$, $\theta^2 + a\theta + b > 0$ and we have $\theta_2 < \theta < \theta_1$.

Lemma 2.2.1 ([19], pp.228). *Let Γ be strongly regular with Spec$(\Gamma) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$, A_1 and A_2 be the first and second subconstituents respectively.*

1. *suppose $A_1x = \theta_1 x$ with $1^T x = 0$, then $\theta_1 \in \{\theta, \tau\}$ whenever $Bx = 0$, or otherwise $\tau < \theta_1 < \theta$;*

2. *suppose $A_2y = \theta_2 y$ with $1^T y = 0$, then $\theta_2 \in \{\theta, \tau\}$ whenever $B^T y = 0$, or otherwise $\tau < \theta_2 < \theta$.*

3. *σ is a local eigenvalue of one subconstituent of Γ if and only if $\lambda - \mu - \sigma$ is a local eigenvalue of the other, with equal multiplicities.*

Proof. We only prove the third part. $A_1x = \sigma_1 x$, applying $BA_1 + A_2B = (\lambda - \mu)B + \mu J$, $A_2(Bx) = (\lambda - \mu - \sigma_2)(Bx)$; $A_2y = \sigma_2 y$, $A_1(B^T y) = (\lambda - \mu - \sigma_2)(B^T y)$; the dimension of σ_1-eigenspace is not less than the dimension of $(\lambda - \mu - \sigma_1)$-eigenspace; and vice versa. □

2.3 Some feasible parameters of *SRG* based on $\mu - \lambda$

It is known [11] that there are only finite many feasible parameter sets (v, k, λ, λ) for a given λ. We also give some theorems in Section 3.2 to sieve the possible parameter sets of this class of strongly regular graphs from the value of λ. Berlekamp and van Lint proved that there are only finitely many feasible parameter sets $(v, k, \lambda, \lambda + 1)$ for each λ.

Strongly regular graphs with $\mu - \lambda = 2$ corresponding to symmetric 2-$(v', k+1, \mu)$ designs with $\mu \geq 2$ that have a polarity with all points absolute (see details in Section 5.2). The projective planes provide an infinitely family of symmetric 2-$(v', k+1, \mu)$ designs with $(v', k', \mu) = (k^2 + k + 1, k + 1, 1)$, but only finitely many symmetric 2-$(v', k + 1, \mu)$ designs are known for each $\mu \geq 2$. Thus it is currently unknown whether there are infinitely many $SRG(v, k, \mu - 2, \mu)$ for a given $\mu \geq 2$.

Strongly regular graphs with $\mu = 1$, $\lambda = 0$ are discussed by Kantor [24] and N. Biggs [8] respectively.

Lemma 2.3.1 ([24]).

1. *For each $\lambda \neq 3$, the parameter set $(v, k, \lambda, 1)$ is feasible if and only if k is one of a finite list of values.*

2. *The parameter set $(v, k, 3, 1)$ is feasible if and only if $k = r^2$ where $r \geq 4$ is even.*

Lemma 2.3.2 ([8], pp.102).

1. *The parameter set* $(v, k, 0, 2)$ *is feasible if and only if* $k = r^2 + 1$ *where* $r \neq 0 (mod\ 4)$, $r \geq 2$.

2. *The parameter set* $(v, k, 0, 4)$ *is feasible if and only if* $k = r^2$.

3. *The parameter set* $(v, k, 0, 6)$ *is feasible if and only if* $k = r^2 - 3$ *where* $r \geq 3$ *and* $r \neq 0\ (mod\ 4)$.

4. *For* $\mu \notin 2, 4, 6$, *the parameter set* $(v, k, 0, \mu)$ *is feasible if and only if* k *is one of a finite list of values.*

Elzinga [17] proved the following theorem.

Theorem 2.3.3 ([17]). *For fixed* λ *and* μ, *there are only finite many feasible parameter sets* (v, k, λ, μ), *unless* λ *and* μ *satisfy one of the following three relations:*

1. $(\mu - \lambda)^2 = 4\mu$;

2. $\mu - \lambda = 2$;

3. $(\mu - \lambda)^2 - 2(\mu - \lambda) = 4\mu$.

The parameter sets (v, k, λ, μ) for which λ and μ satisfy one of the above three equations are summarized in the following table for some integer t and nonnegative integer r.

Case	v	k	λ	μ	m_θ
1.	$\frac{(r^2+r-t)(r^2-r-t)}{t^2}$	r^2	t^2+2t	t^2	$\frac{r(r^2+r-t)(r-t-1)}{2t^2}$
2.	$\frac{(r^2+\mu)^2-r^2}{\mu}$	$r^2+\mu-1$	$\mu-2$	μ	$\frac{(r^2+r+\mu)(r^2+\mu-1)}{2\mu}$
3.	$\frac{r^2(r^2-1)}{t(t+1)}$	r^2+t	t^2+3t	t^2+t	$\frac{(r^2+t)(r-t-1)(r+1)}{2t(t+1)}$

Note that $\mu - \lambda$ is even in either of the above cases. If one of the relations in the previous theorem holds, then there may be infinitely many feasible (v, k, λ, μ) .

2.4 Some families of *SRG* with certain properties

A few families of *SRG* will be presented in this section. *Petersen graph*, *Clebsch graph* and *Schläfli graph*, are three graphs whose second subconstituent is the previous one and we only prove the uniqueness of Petersen graph which helps to construct the figure of the last two. $L_2(n)$, the *square lattice graph*, and $T(n)$, the *triangular graph*, are two families of unique *SRG* with their parameters as n is large enough. *Gewirtz graph* and *Payley graph* are two kinds of strongly regular graph which can be constructed from group theory. Finally, a family of strongly regular graph from

2-$(v', k', 1)$ design is presented. There are several kinds of graphs from symmetric 2-designs and quasi-symmetric designs will be introduced in Section 5.

The Payley graph $P(q)$ is defined on the finite field $GF(q)$ where $q \equiv 1(mod 4)$, such that $x, y \in GF(q)$ are adjacent if and only if $x - y = c$ for some nonzero square c in $GF(q)$.

Theorem 2.4.1 ([19], pp.221). *A Payley graph $P(q)$ is a SRG(q, $\frac{q-1}{2}$, $\frac{q-5}{4}$, $\frac{q-1}{4}$) and Spec($P(q)$) = ($\frac{q-1}{2}^1$, $\frac{-1+\sqrt{q}}{2}^{\frac{q-1}{2}}$, $\frac{-1-\sqrt{q}}{2}^{\frac{q-1}{2}}$).*

The family of Payley graph is another family of *Cayley graph* which will be introduced in Section 4.1. The Cayley set is the collection of x which can be represented as a square. Since -1 is a square in $GF(q)$, the graph is undirected. A Payley graph is a conference graph, which has the parameters set as the above theorem. Indeed, Payley graphs are self complementary. Here are some figures of Payley graph of small orders.

Definition 8. *The Gewirtz graph is defined on $\{\infty\} \cup P \cup Q$, where P is the set of Sylow 3-subgroups of the alternating group A_6, and Q the set of involutions in A_6. Join ∞ to all vertices in P; join $p \in P$ to $q \in Q$ whenever $q^{-1}pq = p$; join $q_1, q_2 \in Q$ whenever q_1q_2 has order 4. Combinatorially, we may identify $p \in P$ with a pair of disjoint 3-subsets of $\{1, ..., 6\}$ (its orbits). Then typical edges of the second and the third types join $\{\{1, 2, 3\}, \{4, 5, 6\}\}$ to (12)(45), and (12)(34) to (23)(56) respectively.*

Definition 9. *Let Y be a subset of $V(\Gamma)$, the vertex set of a graph Γ. The graph switching Γ with respect to Y arises from Γ by changing all the edges between Y and $V(\Gamma) \setminus Y$ to non-edges, and all the non-edges between Y and $V(\Gamma) \setminus Y$ to edges.*

Definition 10. *Let $[n]$ denote the set $\{1, 2, ..., n\}$.*

1. *The Petersen graph is defined on $\binom{[5]}{2}$, such that $A, B \in \binom{[5]}{2}$ are adjacent if and only if $|A \cap B| = 0$.*

2. *The Clebsch graph is defined on $\{A : A \in 2^{[5]}, |A| = 0 \text{ or } 2 \text{ or } 4\}$. A and B are adjacent if and only if $|A \cup B - A \cap B| = 4$.*

3. *The triangular graph $T(n)$ is defined on $\binom{[n]}{2}$, such that $A, B \in \binom{[n]}{2}$ are adjacent if and only if $|A \cap B| = 1$. Any vertex neighborhood subgraph of $T(n)$ is isomorphic to the product $K_n \times K_2$, where K_n is the complete graph on n vertices.*

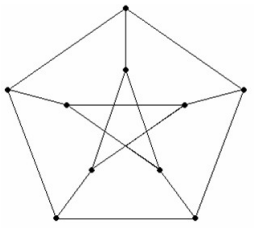


Figure 2.1: Petersen graph

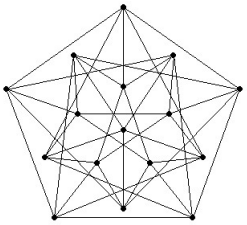


Figure 2.2: Clebcsh graph

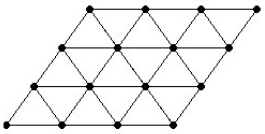


Figure 2.3: Shrikhande graph

4. *The square lattice graph $L_2(n)$ is defined on $[n] \times [n]$, and two vertices are adjacent if and only if they agree in one coordinate.*

5. *The Shrikhande graph is obtained from $L_2(4)$ by switching with respect to the set of vertices $\{(1,1),(2,2),(3,3),(4,4)\}$. It is strongly regular with the same parameters as $L_2(4)$.*

6. *The Schläfli graph is obtained from $T(8)$ by deleting $\{1,2\}$ and switching with respect to the set $\Omega = \{\{1,i\},\{2,i\} : i = 3,...,8\}$. i.e., it has the vertex set $\binom{[n]}{2} - \{\{1,2\}\}$, and any two vertices in Ω (or in Ω^C) are adjacent if and only if they are not disjoint, on the other hand, one vertex in Ω and another vertex in Ω^C are adjacent if and only if they are disjoint.*

7. *The cocktail party graph $CP(n)$ is the complement of nK_2. It models a cocktail party made up of n couples, at which each participant speaks to everybody except her/his partner.*

8. *The three Chang graphs are obtained by switching $T(8)$ with respect to*

   (a) *four disjoint edges;*

   (b) *an octagon;*

   (c) *the disjoint union of a pentagon and a triangle.*

The vertex neighborhood subgraphs of the three Chang graphs are no longer strongly regular graphs, but those of the first Chang graph still possess highly symmetric structure. The first Chang graph is obtained from $T(8)$ by switching with

respect to $\{\{1,2\}, \{3,4\}, \{5,6\}, \{7,8\}\}$, and independent set. Each maximal clique if the vertex neighborhood subgraph of $\{1,2\}$ consists of 4 vertices, and the intersection of any two of them is either empty or a singleton. If any two distinct maximal cliques are called adjacent whenever they are not adjacent, then the associated graph on the set of all maximal clique is isomorphic to the multipartite graph $K_{2,2,2}$.

Some interesting relations are among $T(5)$, Petersen graph, Clebsch graph, and Schläfli graph, related to the work of Cameron et al [14], and Noda [29]:

1. The vertex neighborhood subgraph $\Gamma^{(1)}$ of Γ at the vertex $\{1,3\}$ is isomorphic to the Clebsch graph, see also [13, pp.319], and

2. the vertex neighborhood subgraph $\Gamma^{(2)}$ of $\Gamma^{(1)}$ at the vertex $\{2,3\}$, i.e., the induced subgraph of Γ on $\Gamma_1(\{1,3\}) \cap \Gamma_1(\{2,3\})$, is isomorphic to the triangular graph $T(5)$, which is isomorphic to the complement of the Petersen graph.

Graph	(v,k,λ,μ)
Petersen graph	(10, 3, 0, 1)
Clebsch graph	(16, 5, 0, 2)
Shrikhande graph	(16, 6, 2, 2)
Schläfli graph	(27, 16, 10, 8)
Gewirtz graph	(56, 10, 0, 2)
$T(n)$	$(\frac{1}{2}n(n-1), 2(n-2), n-2, 4)$
$L_2(n)$	$(n^2, 2(n-1), n-2, 4)$
$CP(n)$	$(2n, 2(n-1), 2(n-2), 2)$
$P(q)$	$(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$

For strongly regular graphs Γ with $r = 0$. Under this case, $\mu = k$, the multiplicity of r is a positive integer $\frac{k}{k-\lambda}$, see [12], and $s = \lambda - k < 0$. Let $t = k - \lambda$, $k = lt$ for some positive integer l. Then $s = -t$, $v = (l+1)t$, and

$$(v,k,\lambda,\mu) = ((l+1)t, lt, (l-1)t, lt).$$

Straightforward combinatorial arguments show that Γ must be the complete multipartite graph $K_{t,t,\ldots,t}$ with $(l+1)$ equal parts of size t. Clearly any vertex neighborhood subgraph $\Gamma^{(1)}$ of Γ is again a strongly regular graph with parameters $(lt, (l-1)t, (l-2)t, (l-1)t)$. Furthermore, any vertex neighborhood subgraph $\Gamma^{(i)}$ of $\Gamma^{(i-1)}$ is still a strongly regular graph with parameters $((l-i+1)t, (l-1)t, (l-i-1)t, (l-i)t)$ for $i = 1, 2, \ldots, i-1$, where $\Gamma^{(0)} = \Gamma$. Each $\Gamma^{(i)}$ has distinct eigenvalues $(l-i)t > 0 > -t$. The complement of the ladder graph corresponds to the special case $t = 2$.

Definition 11.

1. *The line graph $L(\Gamma)$ of a graph $\Gamma = (V, E)$ is defined on $E \subseteq \binom{V}{2}$, such that $A, B \in E$ are adjacent if and only if $|A \cap B| = 1$.*

2. *The line graph of the 2-$(v', k', 1)$ design, $\Pi = (X, \mathcal{B})$, is defined on $\mathcal{B}$, such that $A, B \in \mathcal{B}$ are adjacent if and only if $|A \cap B| = 1$.*

Definition 12. *The Latin square graph is defined on n^2 columns of the orthogonal array $OA(k, n)$, which is a $k \times n^2$ array with entries from a set $[n]$ such that the n^2 ordered pairs defined by any two rows are all distinct, and two vertices adjacent if they have the same entries in one coordinate position.*

Graph	(v, k, λ, μ)
Latin square graph on $OA(k, n)$	$(n^2, k(n-1), n-2+(k-1)(k-2), k(k-1))$
Line graph of the 2-$(v, k, 1)$ design	$(\frac{v(v-1)}{k(k-1)}, \frac{k(v-k)}{k-1}, \frac{v-2k+1}{k-1} + (k-1)^2, k^2)$

Note that Petersen graph is the complement of $L(K_5)$, $T(n)$ is $L(K_n)$ and $L_2(n)$ is $L(K_{n,n})$; the Latin square graph on $OA(n-1, n)$ has the same parameters as the complement of $L_2(n)$.

Theorem 2.4.2 tells us that some families of strongly regular graphs are uniquely determined by their parameters.

Theorem 2.4.2.

1. *Petersen graph is the unique $SRG(10, 3, 0, 1)$;*

2. *Clebsch graph is the unique $SRG(16, 5, 0, 2)$ [[19], pp.230];*

3. *Schläfli is the unique $SRG(27, 16, 10, 8)$;*

4. *$T(n)$ is the unique $SRG(\binom{n}{2}, 2(n-2), n-2, 4)$ if $n > 8$;*

5. *$L_2(n)$ is the unique $SRG(n^2, 2(n-1), n-2, 2)$ if $n > 4$.*

Proof. We only proof the uniqueness of Petersen graph. Let Γ be a strongly regular graph with parameters (10, 3, 0, 1).

1. Because every pair of adjacent vertices has 0 common neighbor, there is no triangle in Γ.

2. Because every pair of nonadjacent vertices has a unique common neighbor, Γ has no diamond as its induced subgraph.

Let $\{1, 2, 3, ..., 10\}$ be the vertex set of Γ. Because Γ is 3-regular, there are three distinct vertices adjacent to vertex 1. Without loss of generality, let the neighborhood of vertex 1 be $\Gamma_1(1) = \{2, 3, 4\}$. Since there is no triangle in Γ, the vertices in $\Gamma_1(1)$ are pairwise nonadjacent. Since Γ has no diamond as its subgraph, each pair of vertices in $\Gamma_1(1)$ are nonadjacent and has no other common neighbor except 1. Therefore, each vertex in $\Gamma_1(1)$ is adjacent to two other vertices of $\Gamma \setminus (\Gamma_1(1) \cup \{1\})$.

Without loss of generality, let $\Gamma_1(2) = \{5, 6\}$, $\Gamma_1(3) = \{7, 8\}$, and $\Gamma_1(4) = \{9, 10\}$. By reason 1, the vertices in the same set are nonadjacent. Each vertex in $\Gamma_1(2) \cup \Gamma_1(3) \cup \Gamma_1(4)$ needs to be adjacent to two more vertices. If the neighbors of vertex 5 are in the same set, then we get a diamond, a contradiction. Hence, one of its neighbors must be in $\{7, 8\}$, and the other in $\{9, 10\}$.

Without loss of generality, we add edges $\{5, 7\}$ and $\{5, 9\}$. By reason 2, vertex 5 and 6 have no common neighbor except vertex 2. Hence joining $\{6, 8\}$ and $\{6, 10\}$ is the unique choice. Similarly, vertex 5 and 7 have no common neighbors. Therefore, joining $\{7, 10\}$ and $\{8, 9\}$ is the unique choice. The final graph Γ is a strongly regular graph with parameters $(10, 3, 0, 1)$, which is isomorphic to Petersen graph. □

For $n = 8$, there are three other graphs with same parameters of $T(8)$, $SRG(28, 12, 6, 4)$, known as the Chang graphs.

Theorem 2.4.3 ([11], pp.63). *A strongly regular graph with least eigenvalue -2 is one of the following:*

1. *$T(n)$ for $n \geq 5$, $L_2(n)$ for $n \geq 3$ or $CP(n)$ for $n \geq 2$;*
2. *the Petersen graph, the Shirkhande graph or the three Chang graphs;*
3. *the complement of the Clebsch graph or of the Schläfli graph.*

Chapter 3

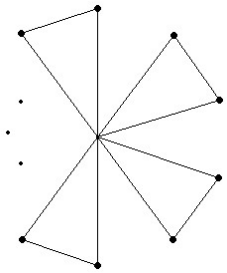
The Friendship Property and Strongly Regular graphs

In this chapter, graphs with the property that each pair of distinct vertices has the same number λ of common neighbors are introduced. The friendship theorem shows the graphs with $\lambda = 1$. And the k-regular graphs with $\lambda > 1$ are $SRG(v, k, \lambda, \lambda)$. Symplectic graphs and the Cayley graphs associated with bent functions, which will appear in Section 4.1, are the examples.

3.1 A review of friendship theorem

In a 1983 survey article [20] entitled "The Friendship Theorem and the Lover Problem", Hammersley assembled material appeared previously in separate contexts and diverse guises, such as the solubility of Diophantine quadratic matrix equations; the construction of block designs, the existence of finite geometries, etc. Moreover, in stressing the graph-theoretic aspects of the matter, he adopted a rather different line from traditional treatments. He began with a special case of the love problem, known as the friendship theorem. It is not known who first raised the following problem or who gave it its human touch. The earliest published paper [35] to Hammersley's knowledge was Wilf (1971), who cites an earlier unpublished account by Graham Higman in 1968. However, Van Lint [11, pp.45] referred this result to Erdös, Rényi and Sós (1966)[18].

Suppose in a group of at least three people we have the situation that any pair of persons have precisely one common friend. Then there is always a person (the "politician") who is everybody's friend. Before tackling the proof, let us rephrase the problem in graph-theoretic terms. We interpret the people as the set of vertices V with $|V| = n \geq 3$, and join two vertices by an edge if the corresponding people are friends. We tacitly assume that friendship is always two-ways, that is, if u is a friend of v, then v is also a friend of u, and further that nobody is his or her own friend. Note that there are graphs with this property as in the figure, where u is



the politician; in fact we will show that these "windmill graphs" are the only graphs with this property.

Theorem 3.1.1 (The Friendship Theorem). *If* Γ *is a graph in which any two distinct vertices have exactly one common neighbor, then* Γ *has a vertex joined to all others.*

Suppose that, in a finite community of n people, any two distinct individuals have exactly one mutual friend. Then n cannot be even, although any odd $n \geq 3$ is possible. Further, the people can be labeled $V_1, V_2, ..., V_n$ such that, whenever $2 \leq 2r < n$, V_{2r} and V_{2r+1} are friends of each other and of V_1 and of nobody else. Thus V_1, the Dale Carnegie (1953) of the community, is everybody's friend. By hypothesis, friendship is symmetric but not reflexive: if V_i is a friend of V_j, then V_j is a friend of V_i, but V_i cannot be friend himself. Love, on the other hand, may or may not be reciprocated, and may be narcissistic. The love problem is the generalization of the friendship theorem when the asymmetric and possibly reflexive relationship of love replaces the symmetric and non-reflexive relationship of friendship. Whereas the friendship theorem is completely solved, the love problem is largely unsolved. It is starting that such a combinatorial - sounding result seems to have no short combinatorial proof. There do exist proofs avoiding eigenvalues (see Hammersley [20, 1983]), but they require complicated *numerical arguments* to eliminate regular graphs. Wilf (1971) used the feasible condition of strongly regular graphs to eliminate regular graphs and combine the condition that unique common neighbor forbids 4-cycles to prove that there is a vertex joined to all others. Craig Huneke has a short proof to exclude regular graphs by counting walks and using *modular arithmetic*; it is no longer than the proof of the *Integrality Condition*. The resulting graph consists of some number of triangles sharing a vertex. If Γ is a regular graph, then it is a strongly regular graph with $\mu = \lambda = 1$. From the feasible condition about multiplicity of eigenvalue mentioned in Chapter 2, it is easy to see that triangle is the only choice.

It should be clear that in the presence of a politician only the windmill graphs are possible. Several proofs of the friendship theorem exist, but the first proof, given

by Paul Erdös, Alfred Rényi and Vera Sós, is still the most accomplished.

Proof. (by Paul Erdös,Alfred Rényi and Vera Sós)

Suppose the assertion is false, and Γ is a counterexample, that is no vertex of Γ is adjacent to all other vertices. To derive a contradiction we proceed in two steps. The first part is combinatorics, and the second part is linear algebra.

1. We claim that Γ is a regular graph, that is, $d(u) = d(v)$ for any $u, v \in V$. Note first that the condition of the theorem implies that there are no cycles of length 4 in Γ as in the figure. Let us call this the C_4-*condition*.

   We first prove that any two *non-adjacent* vertices u and v have equal degree $d(u) = d(v)$. Suppose $d(u) = k$, where $w_1, w_2, ..., w_k$ are the neighbors of u. Exactly one of the w_i, say w_2, is adjacent to v, and w_2 adjacent to exactly one of the other w_i's, say w_1, so that we have the situation of the figure to the left. The vertex v has with w_i the common neighbor w_2, and with w_i $(i \geq 2)$ a common neighbor z_i $(i \geq 2)$. By the C_4-condition, all these z_i must be distinct. We conclude $d(v) \geq k = d(u)$, and thus $d(u) = d(v)$ by symmetry.

   It remains to show that $d(u) = d(v)$ holds also for *adjacent* vertices u and v. Let $v = w_1, w_2, ..., w_k$ be the neighbors of u. If any of the neighbors z of u (and there must be at least one by our assumption) is also non-adjacent to v, then we infer $d(u) = d(z) = d(v)$ by what we just proved. Hence we may assume that v is adjacent to all $z \notin \{w_2, ..., w_k\}$.

   By our assumption $d(v) < n - 1$ there must be some w_i, say w_2, which is not adjacent to v. But z_1 and w_2 must have a common neighbor. It cannot be u since u and z_1 are not adjacent, nor can it be $v = w_1$ since v and w_2 are not adjacent. It cannot be any of the other w_j by the C_4-condition, and this has exhausted all the possibilities of a common neighbor of z_1 and w_2.

   In conclusion, $d(u) = k$ for all u, for some k between 2 and $n - 2$. Looking at the figure for the case of adjacent vertices again, we find $n = k^2 - k + 1$. Indeed, any of the w_i's have exactly $k - 2$ neighbors outside $\{w_1, w_2, ..., w_k\}$ has a common neighbor with u. Hence

   $$n = 1 + k + k(k - 2) = k^2 - k + 1. \tag{1}$$

2. The rest of the proof is a beautiful application of some standard results of linear algebra. Note first that k must be greater than 2, since $k = 2$, only $\Gamma = K_3$ is possible by (1), which is a windmill graph. Consider the adjacency matrix $A = (a_{ij})$. By part 1, any row has exactly k 1's, and by the condition

of the theorem, for any two rows there is exactly one column where they both have a 1. Note further that the main diagonal consists of 0's. Hence we have

$$A^2 = \begin{pmatrix} k & 1 & \dots & 1 \\ 1 & k & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \dots & 1 & k \end{pmatrix} = (k-1)I + J$$

where I is the identity matrix, and J the matrix of all 1's. It is immediately checked that J has the eigenvalues n (of multiplicity 1) and 0 (of multiplicity $n-1$). It follows that A^2 has the eigenvalues $k-1+n = k^2$ (of multiplicity 1) and $k-1$ (of multiplicity $n-1$).

Since A is symmetric and hence diagonalizable, we conclude that A has the eigenvalue k (of multiplicity 1) and $\pm\sqrt{k-1}$. Suppose r of the eigenvalues are equal to $\sqrt{k-1}$ and s of them are equal to $-\sqrt{k-1}$, with $r+s = n-1$. Now we are at most home. Since the sum of the eigenvalues of A equals the trace (which is 0), we find $k + r\sqrt{k-1} - s\sqrt{k-1} = 0$, and, in particular, $r \neq s$, and $\sqrt{k-1} = \frac{k}{s-r}$. It follows that $\sqrt{k-1}$ is an integer h (if $\sqrt{m}$ is rational, then it is an integer!), and we obtain

$$h(s-r) = k = h^2 + 1.$$

Since h divides h^2+1 and h^2, we find that h must be equal to 1, and thus $k = 2$, which we have already excluded. So we have arrived at a contradiction, and the proof is complete.

□

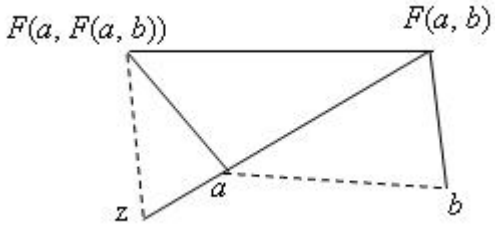
A proof was given by D. G. Higman [22]. Another quite elementary proof, though not wholly elementary, was given by Wilf. Wilf assumed the conclusion is false and defined an incidence structure which is a projective plane. Finally, he used the Integrality Condition, which West used to eliminate the regularity of the graph, to get the nonexistence of the structure.

Proof. ([35], Wilf 1971)

We assume that the conclusion is false. Then for our graph we have the hypotheses

1. Each pair of different x, y has a unique common neighbor $F(x, y)$.

2. Each point x, there exists a y different from x and y not adjacent to x.



We then define an incidence structure $\Pi = (X, L)$ associated with the graph under consideration with X the vertex set $V(\Gamma)$ of the graph Γ, and $L = \{l(x) : x \in X\}$ where $l(x) = \{y : y \in X \text{ is adjacent with } x\}$. We shall claim that $\Pi = (X, L)$ is a finite projective plane, indeed, it suffices to show that there is a set of four points of Π, no three of which lie on a line.

We may assume that $n \geq 4$ by hypotheses 1 and 2. By 1, every pair of points lies on exactly one line, indeed $\{x, y\} \in l(F(x, y))$, and every pair of lines of Π have exactly one point in common, namely $l(x) \cap l(y) = \{F(x, y)\}$.

Choose four distinct points of Π. If no three lie on a line we are finished. Otherwise, some three have a common neighbor a. By 2, there is a b such that a and b are not adjacent. If $F(a, b)$ is the common neighbor of a and b, let z be any neighbor of a other than $F(a, b)$ and $F(F(a, b), a)$. Then we have the figure 3.1.

In the picture, a solid line denotes "adjacency" and a dotted line "non-adjacency". We claim that four distinct points $F(a, b), a, z, b$ satisfy the condition that no three of them lie on a line.

1. If $F(a, b), a, z$ have a common neighbor, it is $F(a,\ F(a,\ b))$. But z and $F(a, F(a, b))$ are not adjacent for otherwise z and $F(a, b)$ would have two common neighbors.

2. If $F(a, b), a, b$ have a common neighbor, it is $F(a, b)$, a contradiction.

3. If $F(a, b), z, b$ have a common neighbor, since $a = F(z, F(a, b))$, and a, b are not adjacent, we have a contradiction.

4. If a, z, b have a common neighbor, it is $F(a, b)$. But z and $F(a, b)$ are not adjacent because otherwise $F(a, b)$ and a have two common neighbors, namely z and $F(a, F(a, b))$.

It follows that the structure Π is a finite projective plane of order m for some positive integer m. Hence Π has $m^2 + m + 1$ points and $m^2 + m + 1$ lines, that each line of Π contains $m + 1$ points and that each point of Π is on $m + 1$ lines. Let A denote the incidence matrix of the points and lines of Π. Then A has the properties

that A is symmetric with $trace(A) = 0$, A^2 is the matrix with entry $m+1$ in all diagonal positions and 1 in all off-diagonal positions, a contradiction, since that, there exists no projective plane of order $m > 1$ whose incidence matrix is symmetric with trace zero, is proved as follow. The spectrum of A^2 is $((m^2+m+1)^1, m^{m^2+m})$, and hence the spectrum of A is $(m+1^1, \sqrt{m}^{\mu_1}, -\sqrt{m}^{\mu_2})$. Clearly, $\mu_1+\mu_2 = m^2+m$, $trace(A) = (m+1)+\mu_1\sqrt{m}-\mu_2\sqrt{m} = 0$, and then $\mu_2 = \frac{1}{2}(m^2+m+\sqrt{m}+\frac{1}{\sqrt{m}})$ is not an integer. □

Proof. [34, pp.467]

The symmetry of the condition suggests that Γ might be regular. If Γ is a regular graph, then it is strongly regular with $\lambda = \mu = 1$. By the Integrality Condition, this requires that $\frac{1}{2}((n-1) \pm \frac{k}{\sqrt{k-1}})$ is an integer. Hence $\frac{k}{\sqrt{k-1}}$ is an integer, which happens only when $k = 2$. However, K_3 is the only 2-regular graph satisfying the condition, and it does have vertices of degree $n-1$.

Now suppose Γ is not regular. We show that any two non-adjacent vertices have the same degree. Insistence on unique common neighbors forbids 4-cycles. Suppose v and w are not adjacent, and let u be their common neighbor. Let a be the common neighbor of u, v and b the common neighbor of u, w. We want to show w has as many neighbors as v. Any $x \in S = \Gamma_1(v) - u - a$ has a common neighbor $f(x)$ with w. If $f(x) = b$ for any $x \in S$, then x, b, u, v is a 4-cycle. If $f(x) = f(x')$ for distinct $x, x' \in S$, then $x, v, x', f(x)$ is a 4-cycle. Hence w has distinct neighbors for each neighbor of v, and $d(w) \geq d(v)$. By symmetry, $d(v) \geq d(w)$.

Since Γ is not regular, it has two vertices v, w with $d(v) \neq d(w)$. By the preceding argument, we know $v \leftrightarrow w$. Let u be their common neighbor. Since u cannot have the same degrees each of them, we may assume $d(u) \neq d(v)$. Now suppose Γ has a vertex x not adjacent to v. Then $d(x) = d(v)$, but this requires $x \leftrightarrow w$ and $x \leftrightarrow u$. This creates the 4-cycle v, u, x, w. Hence $d(v) = n-1$. □

Let us rephrase our theorem in the following way: Suppose Γ is a graph with the property that between any two vertices there is exactly one path of length 2. Clearly, this is an equivalent formulation of the friendship condition. Our theorem then says that the only such graphs are the windmill graphs. But what if we consider paths of length more than 2? A conjecture of Anton Kotzig asserts that the analogous situation is impossible. Kotzig's conjecture has been verified for some l, but the general case remains open.

Kotzig's Conjecture. *Let $l \geq 2$. Then there are no graphs with the property that between any two vertices there is precisely one path of length l.*

3.2 *SRG* with $\mu = \lambda$

We now consider $SRG(v, k, \lambda, \lambda)$. When $\lambda = 1$, K_3 is the only choice for regular graphs which has been proved in friendship theorem. And there are finitely many graphs with $\lambda > 1$ which can be known in Theorem 3.2.1. The symplectic graphs $Sp(2m)$ in Section 3.3 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 in Section 4.1 provide another family of such graphs. Some necessary conditions among v, k, λ and their spectrums are given in the following theorem.

Theorem 3.2.1. *Suppose there exists a* $SRG(v, k, \lambda, \lambda)$ *with* $\lambda > 1$, *and with* $Spec(\Gamma) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$, *then*

1. $\theta = -\tau = \sqrt{k-\lambda}$, $\theta\tau = -(k-\lambda)$ *are integers with multiplicities* $m_\theta = \frac{1}{2}((v-1) - \frac{k}{\sqrt{k-\lambda}})$, *and* $m_\tau = \frac{1}{2}((v-1) + \frac{k}{\sqrt{k-\lambda}})$ *respectively.*
2. $\theta \mid \lambda$ *and* $(v, k) = (\frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}, \theta^2+\lambda)$.
3. *for each* λ, *there are only finitely many feasible parameter sets.*
4. *if* $\theta = \lambda$ *then* $(v, k, \lambda) = (\lambda^2(\lambda+2), \lambda(\lambda+1), \lambda)$.

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 $\lambda = h_1h_2$, 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 $v = \frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}$ in either case as required. □

Since $\theta = -\tau$ as shown in Theorem 3.2.1, $\theta^2 = k - \lambda < k - 1$ and $\theta < 2\sqrt{k-1}$, a $SRG(v, k, \lambda, \lambda)$ turns out to be a Ramanujan graph, see details in Section 4.2. Indeed, the above theorem 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

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

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

$$\begin{aligned}(v, k, \lambda) &= (2^2(2^m+1)^2, (2^m+1)(2^{m+1}+1), 2^m(2^m+1)) \text{ or} \\ &\quad (2^m(2^{m+2}), 2^m(2^{m+1}+1), 2^m(2^m+1));\end{aligned}$$

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

Graphs	Parameters
Symplectic graphs $Sp(2m+1)$	$(2^{2m+2}-1, 2^{2m+1}, 2^{2m})$
Cayley graphs associated with bent functions over Z_2^{2m+2}	$(2^m(2^{m+2}), 2^m(2^{m+1}+1), 2^m(2^m+1))$
Latin square graphs	$(2^2(2^m+1)^2, (2^m+1)(2^{m+1}+1), 2^m(2^m+1))$

Since $v = \frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}$ is an integer, $\frac{\lambda}{\theta}$ is a divisor of $\theta(\theta^2-1)$. In the previous theorem, there are too many methods to factor λ as the product of two positive integers if λ is not a prime. For each (θ, λ) with $\theta|\lambda$, $(v, k, \lambda) = (\frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda}, \theta^2+\lambda, \lambda)$ needs not to be a feasible parameter set for $SRG(v, k, \lambda, \lambda)$; for example $(\theta, \lambda) = (3, 15)$. $\frac{(\theta^2+\theta+\lambda)(\theta^2-\theta+\lambda)}{\lambda} = \frac{27 \cdot 21}{15}$ is not an integer. However, if $\theta = 2$ is an eigenvalue of a SRG, and $\lambda = 2 \cdot p$ for some prime p, then $v = 16$ is the unique choice and $(v, k, \lambda) = (16, 6, 2)$.

Corollary 3.2.2. *If Γ is a $SRG(v, k, \lambda, \lambda)$ with $Spec(\Gamma) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$ and $\lambda = \theta \cdot q$, then $q|\theta(\theta^2-1)$. Moreover, $\theta = \sqrt{cq+1}$ for some integer c if $gcd(\theta, q) = 1$, and in general $\frac{q}{d}|\theta^2 - 1$ where $d = gcd(\theta, q)$.*

Proof. It is easy to be proved by checking the integrality condition of v. □

Theorem 3.2.3. *Suppose there exists a $SRG(v, k, \lambda, \lambda)$ with $Spec(\Gamma) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$ and $\lambda = p \cdot q$ for distinct primes $p > q$.*

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 $(v, \theta) = (16, 2)$ or $(\frac{p(p+1)(p+3)}{2}, p)$.*

Proof. Let $v = \frac{q(p+q-1)(p+q+1)}{p}$ by Theorem 3.2.1. 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 $(v, \theta) = (16, 2)$. □

In Theorem 3.2.2, we know that a $SRG(v, k, \lambda, \lambda)$ with $\tau = -2$, then $(v, k, \lambda) = (16, 6, 2)$. In general case for any λ and μ, we have a theorem which decides all the possible strongly regular graphs with at least eigenvalue -2 in Section 2.4, see details in [11].

3.3 Symplectic graphs

Let N be a block diagonal matrix with m blocks of the form $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Definition 13. *The symplectic graph has vertex set* $V(Sp(2m)) = GF(2)^{2m} - \{0\}$, *and* u *and* v *are adjacent if and only if* $u^T N v = 1$.

The binary rank of $Sp(2m)$ is $2m$ from the order of N. The name "symplectic graph" arises because the function $f(u, v) = u^T N v$ is known as a symplectic form. Two vertices u and v are orthogonal with respect to f if $f(u, v) = 0$. Therefore, $Sp(2m)$ is the non-orthogonality graph of $GF(2)^{2m} - \{0\}$ with respect to the symplectic form f. Actually every graph ,which has no isolated vertices with the property that the neighborhoods of distinct vertices are distinct, has the adjacency defined as above by relabelling the vertices, and we can compute their binary ranks. Here are some properties between $Sp(2m)$ and its induced subgraphs.

Theorem 3.3.1 ([19], pp.184-185).

1. *Suppose* Γ *has no isolated vertices and the neighborhoods of distinct vertices are distinct. Then* Γ *has binary rank at most* $2m$ *if and only if it is an induced subgraph of* $Sp(2m)$.

2. *Every graph on* $2m-1$ *vertices occurs as an induced subgraph of* $Sp(2m)$.

This implies that studying the properties of the universal graph $Sp(2m)$ can yield information that applies to all graphs with binary rank $2m$. A trivial observation of this kind is that a reduced graph with binary rank $2m$ has at most $2m-1$ vertices. Since the chromatic number of an induced subgraph is less then the chromatic number of the origin graph, we have a theorem as follow.

Theorem 3.3.2 ([19], pp.243-244).

1. *The chromatic number of* $Sp(2m)$ *is* $2^m + 1$.

2. *For any graph* Γ *with binary rank* $2m$, $\chi(\Gamma) \leq 2^m + 1$.

Finally, the $Sp(2m)$ is a strongly regular graph with $\mu = \lambda$, and the parameter set, which can be proved from the theory of linear algebra, and its spectrum are as follow theorem.

Theorem 3.3.3 ([19], pp.243). *The graph* $Sp(2m)$ *is* $SR(2^{2m}-1,\ 2^{2m-1},\ 2^{2m-2},\ 2^{2m-2})$ *and with* $Spec(Sp(2m)) = ((2^{2m-1})^1,\ (2^{m-1})^{2^{2m-1}-2^{m-1}-1},\ (-2^{m-1})^{2^{2m-1}+2^{m-1}-1})$.

Proof. Because the rank of $y^T N$ is 1, applying $rank(y^T N) + nullity(y^T N) = 2m$ to get $nullity(y^T N) = 2m-1$; the number of nonzero vector x satisfying $y^T N x = 1$ is $2^{2m} - 2^{2m-1} = 2^{2m-1}$. The other two parameters of SRG are both 2^{2m-2}. □

Chapter 4

Bent Functions, Ramanujan graphs and *SRG*

Motivated from Ramanujan graphs and the spectra of Cayley graphs associated with bent functions, the Cayley graphs associated with bent functions are all SRG with $\mu = \lambda$, we then show that all SRG with $\mu = \lambda$ are Ramanujan graphs, providing a practical model for communication.

4.1 *SRG* associated with bent functions

From design theory, there are many methods used to associated a 2-design with a graph, like block graph, line graph, and viewing the incidence matrix of a symmetric 2-design as an adjacency matrix of a graph. In group theory, there is also a method used to construct a graph, called Cayley graph, from a finite group.

Definition 14. *Given a finite group G and a subset C of nonidentity elements of G such that $\alpha \in C$ implies that $\alpha^{-1} \in C$, the Cayley graph is the simple graph with vertex set G and where vertices α and β are adjacent if and only if $\beta\alpha^{-1} \in C$.*

A complete graph K_n is a Cayley graph with respect to any group of order n, where C consists of all nonidentity elements. Often it is required that C generates the group; this ensures that the corresponding Cayley graph is connected.

We will introduce a Cayley graph associated to a Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. Whose vertices, elements of $\mathbb{Z}_2^n$, are assigned the elements of $\mathbb{Z}_2$ by f and the Cayley set C is chosen as the collection of $x \in \mathbb{Z}_2^n$ which is assigned 1.

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 [5, 6] is a successful example. It was shown in [5] 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 [6]. 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.

The Fourier transform of a Boolean function $f(x) : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is defined to be

$$f^*(w) = \frac{1}{2^n} \sum_{\forall x \in \mathbb{Z}_2^n} f(x) \cdot (-1)^{\langle w,x \rangle}$$

which satisfies the property that

$$f(x) = \frac{1}{2^n} \sum_{\forall w \in \mathbb{Z}_2^n} f^*(w) \cdot (-1)^{\langle w,x \rangle}.$$

The Cayley graph Γ_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 Γ_f is usually denoted by $Spec(\Gamma_f) = (|\Omega_f|, \theta_1, ..., \theta_{2^n-1})$ where

$$\theta_i = \sum_{\forall x \in \mathbb{Z}_2^n} f(x) \cdot (-1)^{\langle b(i),x \rangle} = 2^n \cdot f^*(b(i))$$

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 Γ_f is $|\Omega_f|$-regular with $2^{n-dim\langle \Omega_f \rangle}$ connected components and the graph Γ_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 $d \leq m - 1$.

A Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called a *bent function* if

$$((-1)^{f(x)})^*(w) = \pm \frac{1}{\sqrt{2^n}}$$

for any $w \in \mathbb{Z}_2^n$. It is equivalent to say that f is a bent function if

$$2^n \cdot f^*(0) = 2^{n-1} - 2^{\frac{n}{2}-1} \text{ or } 2^{n-1} + 2^{\frac{n}{2}-1} \text{ and}$$
$$2^n \cdot |f^*(w)| = 2^{\frac{n}{2}-1} \text{ for any } w \neq 0,$$

the term of bent was coined by Rothaus [30]. If $f(x)$ is a bent function on $\mathbb{Z}_2^n$, $n \geq 3$, then $n = 2k$ must be even, and the degree of $f(x)$ is at most k; moreover $f(x)$ is irreducible whenever $deg(f(x)) = k \geq 3$, see [30] 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 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. 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 $(k-\theta)(k-\tau) = 2^n(k+\theta\tau)$ where $k = |\Omega_f|$, and n must be replaced by $dim\langle\Omega_f\rangle$ if Γ_f is not connected. If Γ_f is a $SRG(v, k, \lambda, \mu)$, 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.

If f is a Boolean function on $\mathbb{Z}_2^n$ with connected strongly regular graph Γ_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 $y \in \mathbb{Z}_2^n$. 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 [6] 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 4.1.1 ([5, 6]). *The associated Caley graph Γ_f of a bent function f is a $SRG(v, k, \lambda, \lambda)$; moreover, the bent functions are the only Boolean functions f whose associated graph Γ_f is a $SRG(v, k, \lambda, \lambda)$*

Those graphs Γ_f with small numbers of distinct eigenvalues are considered: if Γ_f has a single eigenvalue, then $\Gamma_f = \overline{K_{2^n-1}}$; if Γ_f has two distinct eigenvalues, then Γ_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 Γ_f has three eigenvalues, then $(k, \theta, \tau) = (|\Omega_f|, 0, -|\Omega_f|)$ if and only if Γ_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 Γ_f is a complete multipartite graph with $\overline{\Gamma_f} = (-\frac{|\Omega_f|}{\tau} + 1)K_{-\tau}$. If Γ_f is connected, then Γ_f is a $SRG(2^n, |\Omega_f|, \lambda, \mu)$ with

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

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

Theorem 4.1.2. *If f is a bent function with connected Γ_f, then Γ_f is a $SRG(v,$ $k,$*

λ, λ) *with* (v, k, λ) *is either*

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

and with spectrum $Spec(\Gamma_f)$ *either*

$$\begin{aligned} & ((2^{n-1} + 2^{\frac{n}{2}-1})^{(1)}, (2^{\frac{n}{2}-1})^{(2^{n-1}-2^{\frac{n}{2}-1}-1)}, (-2^{\frac{n}{2}-1})^{(2^{n-1}+2^{\frac{n}{2}-1})}) \\ \text{or} \quad & ((2^{n-1} - 2^{\frac{n}{2}-1})^{(1)}, (2^{\frac{n}{2}-1})^{(2^{n-1}-2^{\frac{n}{2}-1})}, (-2^{\frac{n}{2}-1})^{(2^{n-1}+2^{\frac{n}{2}-1}-1)}) \end{aligned}$$

respectively.

It has been shown that certain Boolean functions, depending on say, k variables, may be classified as equivalent under the set of *affine transformations*. The number of equivalent classes is much smaller than the total number of functions depending on k variables. For instance, the total number of Boolean functions depending on 4 variables is 65,536, while the number of canonic functions on four variables under affine transformations is only eight, while only the 8th one represents a bent function.

1. The first canonic function is simply the constant function. Hence its associated graph has only one eigenvalue 0, and is *totally disconnected graph.*

2. The second canonic function coincides with the AND function. The spectrum of its associated graph is (1^8, -1^8), which has eight connected components, is simply a *matching.*

3. The graph associated to the third canonic function has spectrum (2^4, 0^8, -2^4), it follows that each connected components is a complete bipartite graph, i.e., $4K_{2,2}$.

4. The graph associated the fourth canonic function has spectrum (3^2, 1^6, -1^6, -3^2), it follows that it has two connected components and each corresponding to a *three dimensional cube.*

5. The graph associated the fifth canonic function has spectrum (4^2, 0^{12}, -4^2), it follows that it has two connected components and each component is a complete bipartite graph, i.e., $2K_{4,4}$.

6. The graph associated the sixth canonic function has spectrum (4^1, 2^4, 0^6, -2^4, -4^1) and is a connected bipartite graph with valency 4 and diameter 4.

7. The graph associated the seventh canonic function has spectrum (5^1, 1^{10}, -3^5), which is the *Clebsch graph*, the unique $SRG(16, 5, 0, 2)$.(See figure **??**)

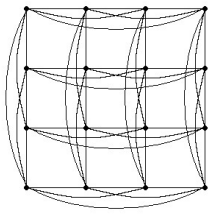


Figure 4.1: $L_2(4)$

8. The graph associated the eight canonic function is a bent function and has spectrum $(6^1, 2^6, -2^9)$. It follows that the associated graph is a $SRG(16, 6, 2, 2)$ which is isomorphic to $L_2(4)$.

4.2 *SRG* which are Ramanujan graphs

Telecommunications networks are frequently modeled using graph theory. Such networks have to transmit information quickly, so the question of how long it takes news to spread through the network is a central one. News spreads rapidly through the network if, for each subset X of the vertex set, there are many neighbors of the vertices of X that are not themselves in X. Let Γ be a k-regular graph of order n, and consider the eigenvalue of its adjacency matrix. The largest eigenvalue of Γ is k; let $\theta(\Gamma)$ be the absolute value of the next to largest eigenvalue. An asymptotic lower bound for θ, due to Alon and Boppana, states that $\liminf_{n\to\infty} \theta(\Gamma) \geq 2\sqrt{k-1}$. This lower bound gives rise to the following definition.

Definition 15. *A k-regular graph Γ is a Ramanujan graph if $\theta(\Gamma) \leq 2\sqrt{k-1}$.*

Theorem 4.2.1 ([15]). *The diameter $d(\Gamma)$ of a k-regular graph Γ of order n satisfies the inequality $d(\Gamma) \leq \lceil \frac{log(n-1)}{log(\frac{k}{\theta})} \rceil$.*

Since, for fix k, θ is asymptotically minimal for Ramanujan graphs, these graphs also minimize the diameter. Since the diameter of a graph corresponds to the worst-case transmission time in the corresponding telecommunications networks, the Ramanujan graphs provide models of communications networks that are extremely good for both average and worst-case transmission times.

We will see in the following theorem that Moore graphs and strongly regular graphs with $\mu = \lambda$ are Ramanujan graphs.

Theorem 4.2.2. *Suppose Γ is a $SRG(v, k, \lambda, \mu)$ with $Spec(\Gamma) = (k^1, \theta^{m_\theta}, \tau^{m_\tau})$, $k \geq 2$ and $|\lambda - \mu| \leq \frac{3k-4}{2\sqrt{k-1}}$. Then Γ is a Ramanujan graph.*

Proof. If $\lambda > \mu$, which implies $\theta > |\tau|$, implies $(\lambda - \mu) + \sqrt{(\lambda-\mu)^2 + 4(k-\mu)} < 4\sqrt{k-1}$ or $\lambda < \mu$, which implies $\theta < |\tau|$, implies $\sqrt{(\lambda-\mu)^2 + 4(k-\mu)} - (\lambda - \mu) < 4\sqrt{k-1}$, then we can say that Γ is also a Ramanujan graph.

Let $\lambda - \mu = t \geq 0$. Suppose a contradictory, $\sqrt{t^2 + 4(k-\mu)} > 4\sqrt{k-1} - t$. $t^2 + 4(k-\mu) > 16(k-1) + t^2 - 8t\sqrt{k-1}$, since $0 \leq t \leq \frac{3k-4}{2\sqrt{k-1}}$ implies $4\sqrt{k-1} - t > 0$. Hence $0 < \mu < -3k + 4 + 2t\sqrt{k-1}$ and $t > \frac{3k-4}{2\sqrt{k-1}}$, a contradiction. It is similar as $t < 0$. □

Chapter 5

SRG with Small $\mu - \lambda$

There are several interesting properties among small $\mu - \lambda$ known. For $\mu - \lambda = 0$, we have introduced in Chapter 4 that there are finitely many feasible parameter sets for a given λ (see Theorem 4.1.1) and two special classes of strongly regular graphs, symplectic graphs and Cayley graphs associated with bent functions. Moreover symmetric 2-designs can be obtained from SRG with $\mu - \lambda = 0,\ 2$. Conference graph is the known strongly regular graph with $\mu - \lambda = 1$.

5.1 *SRG* with $\mu = \lambda + 1$ and conference graphs

There are some families of $SRG(v, k, \lambda, \lambda + 1)$ which has been constructed. The existence of Moore graphs with valency 2, 3, 7 and Payley graph, which is mentioned in Section 2.4 and also a conference graph, which vertex size a prime power have been determined. Conference graph is a class of strongly regular graphs whose parameters satisfy the feasible condition and $\mu = \lambda + 1$, but we are not sure that all the parameter sets have corresponding graphs.

Definition 16. *A Moore graph is a graph with diameter d and girth $2d + 1$.*

Complete graphs are trivial examples with $d = 1$, and odd cycles of order v form another class with $d = \frac{v-1}{2}$.

Theorem 5.1.1 ([19], pp.91). *A Moore graph is distance-regular.*

Bannai and Ito (1973) and Damerell (1973) proved independently that the only Moore graph with diameter $d > 2$ is the cycle of odd length $2d + 1$. We now consider Moore graphs with diameters 2. Because the girth is 5, the triangle is forbidden. Therefore for any vertex x, $|\Gamma_1(x)| = k$ and $|\Gamma_2(x)| = k - 1$. Then the necessary condition of Moore graphs with diameter two is that it is $SR(k^2+1, k, 0, 1)$. Since $v = k^2 + 1$, the multiplicities $m_\theta = \frac{1}{2}(k^2 - \frac{2k-k^2}{\sqrt{4k-3}})$, $m_\tau = \frac{1}{2}(k^2 + \frac{2k-k^2}{\sqrt{4k-3}})$ are functions of k. Since m_θ, m_τ are integers, $k \in \{2, 3, 7, 57\}$. Moreover, the following theorem shows that for any SRG with $\lambda = 0$ and $\mu = 1$, Moore graph is the only

choice. To prove the theorem, we rewrite v and k as functions of its eigenvalue θ. Similarly, using the Integrality Condition, $(v,k) = (5,2)$ or θ is necessarily belongs to $\{0,1,2,7\}$, where 0 is not feasible, which implies k belongs to $\{3,7,57\}$.

Theorem 5.1.2 ([21]). *A $SRG(v,k,0,1)$ is a Moore graph with diameter 2, and it is either C_5, Petersen graph, Hoffman-Singleton graph, or otherwise $(v,k,\lambda,\mu) = (3250,57,0,1)$.*

Moore graphs of valency $2,3,7$ are already known, but the existence of a Moore graph of valency 57 is still an open problem. Since the absolute value of the next to largest eigenvalue is $\frac{1+\sqrt{4k-3}}{2} < \frac{1+2\sqrt{k-1}}{2} < 2\sqrt{k-1}$ for $k \geq 2$, the following theorem is obtained.

Theorem 5.1.3. *A Moore graph is a Ramanujan graph.*

Definition 17. *Conference graphs are $SRG(v,k,\lambda,\mu)$ with $m_\theta = m_\tau$.*

Payley graphs are $SRG(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$, and hence they form a class of conference graphs.

Theorem 5.1.4 ([17]). *A $SRG(v,k,\lambda,\mu)$ is a conference graph if and only if $(v,k,\lambda,\mu) = (v, \frac{1}{2}(v-1), \frac{1}{4}(v-5), \frac{1}{4}(v-1))$; moreover v is the sum of two squares.*

Proof. From Theorem 2.1.1, it is easy to check that $m_\theta = \frac{v-1}{2} = m_\tau$.

Let $m = m_\theta = m_\tau = \frac{v-1}{2}$. Note that $gcd(m,v) = 1$, Since $m^2(\theta-\tau)^2 = vk\overline{k}$, $gcd(m^2,v) = 1$ and $m^2 > v$. Hence $m^2 | k\overline{k}$ and $k\overline{k} \geq m^2$. Because $\frac{k+\overline{k}}{2} \geq \sqrt{k\overline{k}}$ and $k + \overline{k} = v-1$, $k\overline{k} \leq \frac{(v-1)^2}{4} = m^2$. The equality holds if and only if $k = \overline{k} = m$. Because Γ is connected and the sum of the eigenvalues equals $trace(A) = 0$, $m\theta + m\tau + k = 0$ and $\lambda - \mu = \theta + \tau = -1$. With $\lambda + \mu = k - 1$ from the feasible condition $(v-1-k)\mu = k(k-\lambda-1)$, $\lambda = \frac{1}{4}(v-5)$ and $\mu = \frac{1}{4}(v-1)$. □

Note that the set of parameters $(21,10,4,5)$ satisfy all known necessary conditions for SRG, but such a graph does not exist because 21 is not the sum of two squares.

5.2 Symmetric 2-designs from *SRG* with $\mu = \lambda, \lambda+2$

Let A be the adjacency matrix of a strongly regular graph with parameters (v,k,λ,λ). Then $AA^T = A^2 = (k-\lambda)I + \lambda J$, which shows that A is the incidence matrix of some symmetric 2-(v',k',λ') designs.

Theorem 5.2.1 ([21]). *For a $SRG(v,k,\lambda,\mu)$ with adjacency matrix A,*

1. *if $\mu = \lambda$, then A is the incidence matrix of a symmetric 2-(v,k,λ) design;*

2. *if $\mu = \lambda+2$, then $A+I$ is the incidence matrix of a symmetric 2-$(v, k+1, \lambda+2)$ design.*

For instance, the triangular graph $T(6)$ is a $SRG(15, 8, 4, 4)$, providing a symmetric 2-(15, 8, 4) design; the complement of Clebsch graph is a $SRG(16, 10, 6, 6)$, providing a symmetric 2-(16, 10, 6) design; the Gewirtz graph is a $SRG(56, 10, 0, 2)$ provides a symmetric 2-(56, 10, 2) design. Actually we have the following sufficient and necessary conditions between strongly regular graphs and symmetric 2-designs.

Graph	Parameters	Designs
$T(6)$	$SRG(15, 8, 4, 4)$	2-(15, 8, 4) design
the complement of Clebsch graph	$SRG(16, 10, 6, 6)$	2-(16, 10 ,6) design
Gewirtz graph	$SRG(56, 10, 0, 2)$	2-(56, 10, 2) design

Definition 18. *Let $\Pi = (X, \mathcal{B})$ be a symmetric 2-design.*

1. *A duality of a design Π is an isomorphism from Π to its dual; i.e., a pair of bijections $\sigma : X \mapsto \mathcal{B}$ and $\tau : B \mapsto X$ such that $x \in B$ if and only if $B^\tau \in x^\sigma$.*

2. *A duality is called polarity if the automorphisms $\sigma\tau : X \mapsto X$ and $\tau\sigma : B \mapsto B$ are trivial, i.e., τ and σ are inverse of each other.*

3. *A point x is absolute with a polarity σ if $x \in x^\sigma$.*

Theorem 5.2.2 ([11], pp.43). *Let Γ be a graph. Then*

1. *Γ is associated with a polarity of a symmetric 2-design with no absolute points if and only if Γ is strongly regular with $\mu = \lambda$.*

2. *Γ is associated with a polarity of a symmetric 2-design with every point absolute if and only if Γ is strongly regular with $\mu = \lambda + 2$.*

As considering a strongly regular graph with $\mu = \lambda$ in Section 3.2, the extremal case $(v, k) = (\lambda^2(\lambda + 2), \lambda(\lambda + 1))$ (see Theorem 3.2.1) occurs for all prime power λ. Note that $L_2(4)$ and the Shrikhande graph are the only $SRG(16, 6, 2, 2)$ up to isomorphic, associated with different polarities of the same symmetric 2-(16, 6, 2) design.

Suppose the blocks of a 2-(16, 6, 2) design are

$B_1 = \{2, 3, 4, 5, 9, 13\}$, $B_2 = \{1, 3, 4, 6, 10, 14\}$, $B_3 = \{1, 2, 4, 7, 11, 15\}$,
$B_4 = \{1, 2, 3, 8, 12, 16\}$, $B_5 = \{1, 6, 7, 8, 9, 13\}$, $B_6 = \{2, 5, 7, 8, 10, 14\}$,
$B_7 = \{3, 5, 6, 8, 11, 15\}$, $B_8 = \{4, 5, 6, 7, 12, 16\}$, $B_9 = \{1, 5, 10, 11, 12, 13\}$,
$B_{10} = \{2, 6, 9, 11, 12, 14\}$, $B_{11} = \{3, 7, 9, 10, 12, 15\}$, $B_{12} = \{4, 8, 9, 10, 11, 16\}$,
$B_{13} = \{1, 5, 9, 14, 15, 16\}$, $B_{14} = \{2, 6, 10, 13, 15, 16\}$, $B_{15} = \{3, 7, 11, 13, 14, 16\}$,
$B_{16} = \{4, 8, 12, 13, 14, 15\}$.

The polarity associated to $L_2(4)$ is the pair of bijections $i^\sigma = B_i$ and $B_i^\tau = i$ for all i.

In the other case of strongly regular graphs associated with polarities, viz. those with $\mu = \lambda + 2$, similar finiteness theorem is known for $SRG(v, k, \lambda, \lambda + 2)$ associate, even for $(\lambda, \mu) = (0, 2)$. Three such graphs are known:

1. $CP(2)$ with parameters $(4, 2, 0, 2)$;
2. the Clebsch graph with the parameters $(16, 5, 0, 2)$;
3. the Gewirtz graph with parameters $(56, 10, 0, 2)$.

Note that these graphs are known uniquely determined by their parameters. They are associated with polarities of the trivial 2-(4, 3, 2) design, a 2-(16, 6, 2) design, and a 2-(56, 11, 2) design respectively. It is known that there are exactly three non-isomorphic 2-(56, 11, 2) designs; but other designs with these parameters do not admit polarities with every point absolute.

Bruck-Ryser-Chowla Theorem gives a necessary condition for the existence of symmetric 2-designs, and hence it also provides some constraints over (v, k, λ) for $SRG(v, k, \lambda, \lambda + 2)$. Since we can construct a symmetric 2-design from a SRG with $\mu = \lambda$ and $\mu = \lambda + 2$, it may decide the existence of such SRG from the existence of its corresponding symmetric 2-design.

Bruck-Ryser-Chowla Theorem ([11], pp.7). *For the existence of a symmetric* $2 - (v', k', \lambda')$ *design, it is necessary that:*

1. *if* v' *is even then* $k' - \lambda'$ *is a square;*
2. *if* v' *is odd, then the equation* $z^2 = (k' - \lambda')x^2 + (-1)^{\frac{v'-1}{2}}\lambda' y^2$ *has a solution in integers* x, y, z *not all zero.*

From Bruck-Ryser-Chowla Theorem, $SRG(v, k, \lambda, \lambda)$ will not exist if $k - \lambda$ is not a square and $SRG(v, k, \lambda, \lambda + 2)$ will not exist if $k - \lambda - 1$ is not a square whenever v is even.

5.3 *SRG* associated with quasi-symmetric designs

As we know, a connected graph is a strongly regular graph if and only if its adjacency matrix has exactly three distinct eigenvalues. By the property, a block graph of a quasi-symmetric design is a strongly regular graph and we will represent the parameters of SRG by its eigenvalues.

Theorem 5.3.1. *Let $\Pi = (X, \mathcal{B})$ be a quasi-symmetric $2-(v,k,\lambda)$ design and $x < y$ the cardinalities of intersections among a pair of blocks. Then the block graph of Π is a $SRG(v', k', \lambda', \mu')$ with spectrum $(k^1, \theta^{m_\theta}, \tau^{m_\tau})$ where*

$$v' = \frac{\lambda v(v-1)}{k(k-1)}, k' = \frac{\lambda(v-1)(k^2-xv)}{k(k-1)(y-x)} - \frac{2}{y-x}, \lambda' = k' + \theta + \tau + \theta\tau, \mu' = k' + \theta\tau,$$

$$\theta = \frac{(x-k)(k-1)+\lambda(v-k)}{(k-1)(y-x)}, \tau = \frac{x-k}{y-x}, m_\theta = v-1, \text{ and } m_\tau = \frac{\lambda v(v-1)}{k(k-1)} - v.$$

Proof. Let N be the incidence matrix of Π, and A the adjacency matrix of its block graph. Therefore $NN^T = (r-\lambda)I + \lambda J$ and $N^TN = kI + yA + x(J - I - A)$. From the definition of 2-design, NN^T has an eigenvalue kr with all one vector as its eigenvector and so does N^TN. Besides, NN^T has another eigenvalue $r - \lambda$ with multiplicity $v - 1$. Therefore, the spectrum of NN^T and N^TN are

$$((\frac{\lambda k(v-1)}{k-1})^1, (\frac{\lambda(v-k)}{k-1})^{v-1}) \text{ and } ((\frac{\lambda k(v-1)}{k-1})^1, (\frac{\lambda(v-k)}{k-1})^{v-1}, 0^{\frac{\lambda v(v-1)}{k(k-1)}-v})$$

respectively. Since

$$\frac{x-k}{y-x} - \frac{x}{y-x} \cdot \frac{\lambda v(v-1)}{k(k-1)} + \frac{k}{y-x} \cdot \frac{\lambda(v-k)}{k-1}$$

is an eigenvalue of

$$A = \frac{x-k}{y-x} I - \frac{x}{y-x} J + \frac{1}{y-x} N^TN$$

with all one vector as its eigenvector. The spectrum of A is

$$((\frac{\lambda(v-1)(k^2-xv)}{k(y-x)(k-1)})^1, (\frac{(x-k-\lambda)(k-1)+\lambda(v-1)}{(y-x)(k-1)})^{v-1}, (\frac{x-k}{y-x})^{\frac{\lambda v(v-1)}{k(k-1)}v})$$

which implies A is a strongly regular graph. By the property that $\lambda' = k' + \theta + \tau + \theta\tau$ and $\mu' = k' + \theta\tau$, the parameters of SRG are obtained. □

Note that $\mu' - \lambda' = \frac{2(x-k)(k-1)+\lambda(v-k)}{(k-1)(y-x)}$ in the above theorem. For instance, an affine resolvable $(v,k,\lambda) - BIBD$ is a quasi-symmetric design with $x = 0$ and $y = \frac{k^2}{v}$. Its block graph is a $SRG(\frac{\lambda v(v-1)}{k(k-1)}, \frac{\lambda v(v-1)}{k(k-1)} - \frac{v}{k}, \frac{\lambda v(vk+v-2k)}{k^2(k-1)} - \frac{2vk-k-v}{k^2} - \frac{\lambda v^2(v-k)}{k^3(k-1)}, \frac{\lambda vk(v-1)}{k^2(k-1)} - \frac{v}{k}(\frac{\lambda v(v-k)}{k^2(k-1)} - \frac{1}{k} - 1))$ with spectrum $((\frac{\lambda v(v-1)}{k(k-1)} - \frac{v}{k})^1, (\frac{\lambda v(v-k)}{k^2(k-1)} - \frac{1}{k})^{v-1}, (\frac{-v}{k})^{\frac{\lambda v(v-1)}{k(k-1)}-v})$.

Bibliography

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer 1999.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin-Cummings Lecture Note Series, 1984.

[3] L. W. Beineke and R. J. Wilson, *Graph connections Relationships between Graph Theory and other Area of Mathematics*, Clarendon Press, Oxford, pp. 46-47, 1997.

[4] E. R. Berlekamp, J. H. van Lint, and J. J. Seidel. "A Strongly Regular Graph Derived from the Perfect Golay Code", *A Survey of Combinatorial Theory* (J. N. Srivastava et al., eds.) North Holland, Amsterdam, 1973.

[5] 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.

[6] 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, pp. 984-985, September 2001.

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

[8] N. Biggs. *Finite groups of Automorphisms*, Number 6 in London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1971.

[9] B. Bollobás, *Modern Graph Theory*, Graduated Texts in Mathematics 184, Spriger-Verlag, New York, 1998.

[10] F. C. Bussemaker, D. M. Cvetkovic and J. J. Seidel, "Graphs related to exceptional root systems", T. H. -Report 76WKS- 05, Technolog. Univ. Eindhown, 1976.

[11] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, London Math. Society Student Texts 22, Cambridge University Press, Cambridge, 1991.

[12] P. J. Cameron, J. H. van Lint, *Graphs, Codes, and Designs*, London Mathematical Society Lecture Note Series 43.

[13] P. J. Cameron, J. M. Goethals, J. J. Seidel and E. Shult, "Line graphs, root systems, and elliptic geometry", *J. of Algebra* 43, pp. 305-327, 1976.

[14] P. J. Cameron, J. M. Goethals, J. J. Seidel, "Strongly regular graphs having strongly regular subconstituents", *J. of Algebra* 55, pp. 257-280, 1978.

[15] F. R. K. Chung, "Diameters and Eigenvalues", *J. Amer. Math. Soc.*, 2, pp. 187-196, 1989.

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

[17] R. J. Elzinga, "Strongly Regular Graphs: Values of λ and μ for Which There Are Only Finitely Many Feasible (v, k, λ, μ)",*Electronic Journal of Linear Algebra*, Vol.10, , pp. 232-239, Oct. 2003.

[18] P. Erdös, A. Rényi, and V. T. Sós, "On a Problem in Graph Theory", *Studies Math. Hungar.*, 1, pp. 215-235, 1966.

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

[20] J. Hammersley , "The friendship theorem and the love problem". *Surveys in Combinatorics* (ed. E.K. Lloyd), Lond. Math. Soc. Lec. Notes Combridge Univ. Press, pp. 31-54, 1983.

[21] W. H. Haemers, "Matrix techniques for strongly regular graphs and related geometries", Lecture notes for the Intensive Course on Finite geometry and its Applications, 2000.

[22] G. Higman, *Lecture given at Conference on Combinatorial Analysis*, Oxford University, 1969.

[23] T. Huang and K. H. You, "Strongly Regular Graphs associated with Bent Functions", Proceeding of 2004 International Symposium on Parallel Architectures Algorithms and Networks, Hong- Kong, pp. 380-383, May 10-12, 2004.

[24] W. M. Kantor, "Moore geometries and rank 3 groups having μ=1", *The Quarterly Journal of Mathematics*, Oxford Series, 1:309-328, 1977.

[25] A. Kotzig, "Regularly k-path connected graphs". *Congressus Numerantium* 40, 137-141, 1983.

[26] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized Bent Functions and Their Properties", *J. Combinatorial Theory* (A), Vol. 40, pp. 90-107, 1985.

[27] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992.

[28] M. R. Murty, "Ramanujan Graphs", *J. Ramanujan Math. Soc.*, 18, No. 1, pp. 1-20, 2003.

[29] R. Noda, "Partitioning strongly regular graphs", *Osaka J. Math.* 22, pp. 379-389, 1985.

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

[31] J. J. Seidel, "Strongly regular graphs", *Survey in Combinatorics*, ed. B. Bollabas, London Mathematics Society Lecture Note Series 38, pp. 157-180.

[32] D. R. Stinson, *Combinatorial Designs with Selected Applications Lecture Notes*, 1996.

[33] P. Terwilliger, "A new feasibility conditions for distance regular graphs", *Discrete Math.* 61, pp. 311-315, 1986.

[34] Douglas B.West, *Introduction to Graph Theory*, Prentice Hall, 1996.

[35] H. S. Wilf, "The Friendship Theorem". *Combinatorial Mathematics and Its Applications*, Proc. Conf. Oxford 1969 Academic Press, pp. 307-309, 1971

Appendix A

Tables of *SRG* on at most 280 vertices

These tables are taken from *The CRC Handbook of Combinatorial Designs*.

1. $\lambda = \mu$

Existence	v	k	λ	μ	Comments
!	15	8	4	4	two-graph-*; Sp(4)
!	16	10	6	6	Clebsch graph; two-graph
2!	16	6	2	2	Shrikhande graph; two-graph
+	35	18	9	9	S(2,3,15); two-graph-*
+	36	15	6	6	OA(3,6); two-graph
+	36	21	12	12	two-graph
+	40	27	18	18	
+	45	12	3	3	
!	56	45	36	36	
+	63	32	16	16	S(2,4,28); two-graph-*; Sp(6)
+	64	28	12	12	OA(4,8); two-graph
+	64	36	20	20	two-graph
+	85	64	48	48	
+	96	20	4	4	
+	96	76	60	60	
+	99	50	25	25	S(2,5,45); two-graph-*
+	100	45	20	20	OA(5,10)?; two-graph
+	143	72	36	36	S(2,6,66); two-graph-*
+	144	66	30	30	OA(6,12); two-graph
+	144	78	42	42	two-graph
+	156	125	100	100	
+	175	30	5	5	
+	176	126	90	90	
+	195	98	49	49	S(2,7,91); two-graph
+	196	91	42	42	OA(7,14)?; two-graph
+	255	128	64	64	S(2,8,120); two-graph-*; Sp(8)
+	256	120	56	56	OA(8,16); two-graph
+	256	136	72	72	two-graph

$\lambda = \mu$ feasible but not known example

v	k	λ	μ
100	55	30	30
105	40	15	15
112	75	50	50
115	96	80	80
120	35	10	10
120	85	60	60
133	100	75	75
153	96	60	60
160	54	18	18
171	120	84	84
189	48	12	12
196	105	56	56
204	175	150	150
208	162	126	126
210	77	28	28
210	133	84	84
220	147	98	98
231	70	21	21
259	216	180	180
261	196	147	147
280	63	14	14
280	217	168	168

2. $\mu = \lambda + 1$

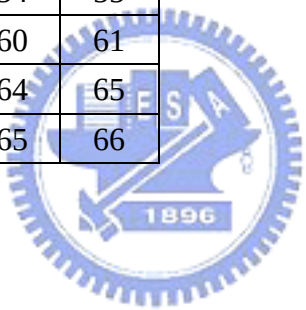
Existence	v	k	λ	μ	Comments
!	5	2	0	1	pentagon; Paley(5); two-graph-*
!	9	4	1	2	Payley(9); two-graph-*
!	10	3	0	1	Petersen graph
!	10	6	3	4	two-graph
!	13	6	2	3	Payley(13); two-graph-*
!	17	8	3	4	Payley(17); two-graph-*
-	21	10	4	5	Conf
15!	25	12	5	6	Payley(25); OA(3,5); two-graph-*
10!	26	10	3	4	two-graph
10!	26	15	8	9	S(2,3,13); two-graph
41!	29	14	6	7	Payley(29); two-graph-*
-	33	16	7	8	Conf
+	37	18	8	9	Payley(37); two-graph-*
+	41	20	9	10	Payley(41); two-graph-*
+	45	22	10	11	two-graph-*
+	49	24	11	12	Payley(49); OA(4,7); two-graph-*
!	50	7	0	1	
!	50	42	35	36	
+	50	21	8	9	two-graph
+	50	28	15	16	S(2,4,25); two-graph
+	53	26	12	13	Payley(53); two-graph-*
-	57	28	13	14	Conf
+	61	30	14	15	Payley(61); two-graph-*
-	69	34	16	17	Conf
+	73	36	17	18	Payley(73); two-graph-*
-	77	38	18	19	Conf
+	81	40	19	20	Payley(81); OA(5,9); two-graph-*
+	82	36	15	16	two-graph
+	82	45	24	25	S(2,5,41); two-graph
+	89	44	21	22	Payley(89); two-graph-*
-	93	46	22	23	Conf
+	97	48	23	24	Payley(97); two-graph-*
+	101	50	24	25	Payley(101); two-graph-*
-	105	52	25	26	Conf
+	109	54	26	27	Payley(109); two-graph-*

+	113	56	27	28	Payley(113); two-graph-*
+	121	60	29	30	Payley(121); two-graph-*
+	122	55	24	25	two-graph
+	122	66	35	36	S(2,6,61)?; two-graph
+	125	62	30	31	Payley(125); two-graph-*
-	129	64	31	32	Conf
-	133	66	32	33	Conf
+	137	68	33	34	Payley(137); two-graph-*
-	141	70	34	35	Conf
+	149	74	36	37	Payley(149); two-graph-*
+	157	78	38	39	Payley(157); two-graph-*
-	161	80	39	40	Conf
-	165	82	40	41	Conf
+	169	84	41	42	Payley(169); OA(7,13); two-graph-*
+	170	78	35	36	two-graph
+	170	91	48	49	S(2,7,85)?; two-graph
+	173	86	42	43	Payley(173); two-graph
-	177	88	43	44	Conf
+	181	90	44	45	Payley(181); two-graph-*
-	189	94	46	47	Conf
+	193	96	47	48	Payley(193); two-graph-*
+	197	98	48	49	Payley(197); two-graph-*
-	201	100	49	50	Conf
-	209	104	51	52	Conf
-	213	106	52	53	Conf
-	217	108	53	54	Conf
+	225	112	55	56	OA(8,15)?; two-graph-*
+	226	105	48	49	two-graph
+	226	120	63	64	S(2,8,113)?; two-graph
+	229	114	56	57	Payley(229); two-graph-*
+	233	116	57	58	Payley(233); two-graph-*
-	237	118	58	59	Conf
+	241	120	59	60	Payley(241); two-graph-*
+	243	22	1	2	
+	243	220	199	200	
-	249	124	61	62	Conf
-	253	126	62	63	Conf

+	257	128	63	64	Payley(257); two-graph-*
+	269	134	66	67	Payley(269); two-graph-*
-	273	136	67	68	Conf

$\mu = \lambda + 1$ feasible but not known example

v	k	λ	μ
65	32	15	16
85	42	20	21
99	14	1	2
99	84	71	72
117	58	28	29
145	72	35	36
153	76	37	38
185	92	45	46
205	102	50	51
221	110	54	55
245	122	60	61
261	130	64	65
265	132	65	66



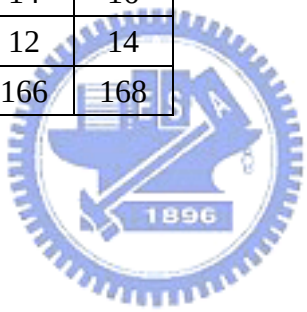
3. $\mu = \lambda + 2$

Existence	v	k	λ	μ	Comments
!	15	6	1	3	two-graph-*
!	16	5	0	2	two-graph
2!	16	9	4	6	OA(3,4); two-graph
+	35	16	6	8	two-graph-*
+	36	14	4	6	two-graph
+	36	20	10	12	two-graph
+	40	12	2	4	
+	45	32	22	24	
!	56	10	0	2	Sims-Gewirtz graph
+	63	30	13	15	two-graph-*
+	64	27	10	12	two-graph
+	64	35	18	20	OA(5,8); two-graph
+	85	20	3	5	
+	96	19	2	4	
+	96	75	58	60	
+	99	48	22	24	two-graph-*
+	100	44	18	20	
+	100	54	28	30	OA(6,10)?; two-graph
+	143	70	33	35	two-graph-*
+	144	65	28	30	two-graph
+	144	77	40	42	OA(7,12); two-graph
+	156	30	4	6	
+	175	144	118	120	
+	176	49	12	14	
+	195	96	46	48	two-graph-*
+	196	104	54	56	OA(8,14)?; two-graph-*
+	255	126	61	63	two-graph-*
+	256	119	54	56	two-graph
+	256	135	70	72	OA(9,16); two-graph

$\mu = \lambda + 2$ feasible but not known example

v	k	λ	μ
105	64	38	40
112	36	10	12
115	18	1	3

120	34	8	10
120	84	58	60
133	32	6	8
153	56	19	21
160	105	68	70
171	50	13	15
189	140	103	105
196	90	40	42
204	28	2	4
208	45	8	10
210	76	26	28
210	132	82	84
220	72	22	24
231	160	110	112
259	42	5	7
261	64	14	16
280	62	12	14
280	216	166	168



4. Unique Existence

v	k	λ	μ	Comments
5	2	0	1	pentagon; Paley(5); two-graph-*
9	4	1	2	3^2; Payley(9); two-graph-*
10	3	0	1	Petersen graph / $T(5)$; two-graph
13	6	2	3	Payley(13); two-graph-*
15	6	1	3	two-graph-* / $T(6)$; two-graph-*; $Sp(4)$
16	5	0	2	two-graph / Clebsch graph; two-graph
17	8	3	4	Payley(17); two-graph-*
21	10	3	6	/ $T(7)$
25	8	3	2	$L_2(5)$ / OA(4, 5)
27	10	1	5	two graph-* / Schläfli graph; two graph-*
36	10	4	2	$L_2(6)$
36	14	7	4	$T(9)$
45	16	8	4	$T(10)$
49	12	5	2	$L_2(7)$ / OA(6, 7)
50	7	0	1	Hoffman-Singleton graph
55	18	9	4	$T(11)$
56	10	0	2	Sims-Gewirtz graph
64	14	6	2	$L_2(8)$ / OA(7, 8)
66	20	10	4	$T(12)$
77	16	0	4	S(3, 6, 22); subconstituent of Higman-Sims graph/Witt 3-(22, 6, 1)
78	22	11	4	$T(13)$
81	16	7	2	$L_2(9)$ / OA(8, 9)
81	20	1	6	
91	24	12	4	$T(14)$
100	18	8	2	$L_2(10)$
100	22	0	6	Higman-Sims graph
105	26	13	4	$T(15)$
112	30	2	10	Subconstituent of McLaughlin graph
120	28	14	4	$T(16)$
121	20	9	2	$L_2(11)$ / OA(10, 11)
136	30	15	4	$T(17)$
144	22	10	2	$L_2(12)$ / OA(11, 12)?
153	32	16	4	$T(18)$
162	56	10	24	/ subconstituent of McLaughlin graph
169	24	11	2	$L_2(13)$ / OA(12, 13)

171	34	17	4	$T(19)$
190	36	18	4	$T(20)$
196	26	12	2	$L_2(14)$ / OA(13, 14)?
210	38	19	4	$T(21)$
225	28	13	2	$L_2(15)$ / OA(14, 15)?
231	40	20	4	$T(22)$
253	42	21	4	$T(23)$
256	30	14	2	$L_2(16)$ / OA(15, 16)
275	112	30	56	two graph-* / McLaughlin graph; two graph-*
276	44	22	4	$T(24)$

5. *SRG* but not *Ramanujan graph*

Existence	v	k	λ	μ	Comments
-	56	22	3	12	Krein; Abs
-	63	22	1	11	Krein; Abs
-	64	21	0	10	Krein; Abs
-	81	40	13	26	Abs
!	91	24	12	4	C(14, 2)
-	100	33	18	7	Abs
!	105	26	13	4	C(15, 2)
!	120	28	14	4	C(16, 2)
!	121	20	9	2	*T*(11)
-	121	56	15	35	Abs
-	125	48	28	12	Abs
-	125	76	39	57	Abs
!	136	30	15	4	C(17, 2)
!	144	22	10	2	*T*(12)
-	144	65	16	40	Krein; Abs
-	144	78	52	30	Krein; Abs
!	153	32	16	4	C(18, 2)
-	154	51	8	21	Krein
!	162	56	10	24	
!	169	24	11	2	*T*(13)
!	171	34	17	4	C(19, 2)
+	175	72	20	36	edges of Hoffman-Singleton graph; two-graph-*
+	176	70	18	34	S(4, 7, 23)\S(3, 6, 22); two-graph
-	176	70	42	18	Abs
-	176	105	52	78	Abs
-	184	48	2	16	Krein
!	190	36	18	4	C(20, 2)
!	196	26	12	2	*T*(14)
?	196	81	42	27	
-	196	85	18	51	Krein; Abs
-	196	110	75	44	Krein; Abs
!	210	38	19	4	C(21, 2)
-	216	70	40	14	Abs
-	216	145	88	116	Abs

!	225	28	13	2	*T*(15)
-	225	56	1	18	Krein
-	225	96	19	57	Krein; Abs
-	225	128	88	52	Krein; Abs
?	225	96	51	33	
!	231	40	20	4	C(22, 2)
?	232	77	36	20	
-	243	88	52	20	Abs
-	243	154	85	119	Abs
!	256	30	14	2	*T*(16)
-	256	66	2	22	Krein
?	261	84	39	21	
!	275	112	30	56	two-graph-*
!	275	162	105	81	McLaughlin graph
!	276	44	22	4	C(24, 2)
-	276	110	28	54	Krein; Abs
-	276	165	108	84	Krein; Abs
+	276	135	78	54	two-graph