Colouring Cayley Graphs

by
Lei Chu

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2004

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We will discuss three ways to bound the chromatic number on a Cayley graph.

(a) If the connection set contains information about a smaller graph, then these two graphs are related. Using this information, we will show that Cayley graphs cannot have chromatic number three.

(b) We will prove a general statement that all vertex-transitive maximal triangle-free graphs on n vertices with valency greater than $n/3$ are 3-colourable. Since Cayley graphs are vertex-transitive, the bound of general graphs also applies to Cayley graphs.

(c) Since Cayley graphs for abelian groups arise from vector spaces, we can view the connection set as a set of points in a projective geometry. We will give a characterization of all large complete caps, from which we derive that all maximal triangle-free cubelike graphs on 2^n vertices and valency greater than $2^n/4$ are either bipartite or 4-colourable.

Acknowledgements

I would like to give my special thanks to my supervisor, Chris Godsil, who inspired me throughout the whole year, and who gave me tremendous help in writing this thesis. It is a great pleasure to work with him.

Contents

Chapter 1

Introduction

Let G be a group and let C be a subset of G. A *Cayley graph* $X(G, C)$ is the graph with vertex set G, and the vertex g is adjacent to the vertex h if and only if $hg^{-1} \in C$. The subset C is called the connection set of X. Sometimes we write $X(G, C)$ as $X(C)$ for convenience, if it is clear what group we are talking about.

If $X(G, C)$ is undirected and loopless then C is inverse-closed and does not contain the identity of G. We are only interested in undirected and loopless Cayley graphs for finite abelian groups.

Cayley graphs play a significant role in the theory of graph homomorphisms. It can be shown that every vertex-transitive graph is a retract of a Cayley graph. Naserasr and Tardif also showed that if there is a graph homomorphism from a graph X to a Cayley graph Y for an abelian group with exponent d, then there is a map from the free Cayley graph $\mathbb{Z}_d[X]$ to Y that is both a graph homomorphism and a group homomorphism (see Theorem 4.1.1). Thus we can obtain bounds on the chromatic number of X or $\mathbb{Z}_p[X]$. This method will be discussed in Section 4.

An interesting class of Cayley graphs is the class of *cubelike graphs*, which are Cayley graphs on $\mathbb{Z}_2^n$. Cubelike graphs are closely related to binary codes and subsets in projective geometry. Let M be a matrix whose columns are the vectors in the connection set C. Then we can view M as the generator matrix of a binary linear code, or the check matrix of its dual code. We can show that if the code of M has a codeword of weight n then the cubelike graph $X(C)$ is bipartite. On the other hand, we can view C as a set of points in a projective geometry. If C corresponds to a complete binary cap then the graph $X(C)$ is maximal triangle-free. Geometric operations, such as doubling, deletion, projection, also correspond to graphical operations on $X(C)$.

In this thesis we will focus on describing the connections among graphs, codes, and finite geometry. We first present a result from Brandt that all regular maximal triangle-free graphs with valency more than $|V|/3$ are 4-colourable. Payan showed that no cubelike graph has chromatic number three. These two results imply that all maximal triangle-free cubelike graphs on 2^n vertices with valency more than $2^n/3$ are bipartite. If we consider the vectors in C as points in the projective space of dimension $n-1$, then "triangle-free" translates to the fact that C is a cap. Davydov and Tombak proved that if a complete cap is of size greater than $2^{n-2}+2$, then it arises from doubling, and there exists a subspace of codimension two skew to it. The arguments include lengthy calculations that are hard to understand. Here we will present the proof in a simpler way. In addition to the result of Davydov and Tombak, we will also show that if the size of a complete cap is $2^{n-2}+1$, then there exists a subspace of codimension two skew to it. Based on the characterization of complete caps, we can conclude that any maximal triangle-free cubelike graph on 2^n vertices with valency at least $2^n/4$ is either bipartite, or has chromatic number four.

Chapter 2

The Basics

Cayley graphs play a significant role in the study of graph homomorphisms. It can be shown that every vertex-transitive graph is a retract of a Cayley graph. In this chapter we will discuss the basic properties of Cayley graphs and provide some examples. The content is mostly taken from *Algebraic Graph Theory*, by Chris Godsil and Gordon Royle [7].

2.1 Definitions

We will introduce Cayley graphs and cubelike graphs, and prove some standard results on Cayley graphs.

Let G be a group and let C be a subset of G. The *Cayley graph* $X(G, C)$ is the graph with vertex set G, and the vertex g is adjacent to the vertex h if and only if $hg^{-1} \in C$. The subset C is called the *connection set* of X.

The complete graph K_n is a Cayley graph for the additive group $\mathbb{Z}_n$ whose connection set is the set of all non-zero elements of $\mathbb{Z}_n$.

The Andrásfai graph $\text{And}(k)$ is another example. It is defined as follows: for any integer $k \geq 1$, let $G = \mathbb{Z}_{3k-1}$ denote the additive group of integers modulo $3k - 1$, and let C be the subset of $\mathbb{Z}_{3k-1}$ consisting of the elements congruent to 1 modulo 3. We denote the Cayley graph $X(G, C)$ by $\text{And}(k)$.

The graph And(2) is isomorphic to the 5-cycle, and And(3) is known as the Möbius ladder. The graph And(k) is triangle-free and of diameter two, and the neighbourhoods of any two vertices are distinct. The diameter of a graph is the maximum distance between two distinct vertices. (It is usually taken to be infinite if the graph is not connected.)

It is easy to show that Cayley graphs are vertex-transitive.

2.1.1 Theorem. *The Cayley graph $X(G, C)$ is vertex transitive.*

Proof. For each $g \in G$ define the mapping

$$\rho_g : x \mapsto xg.$$

This mapping defines a permutation of the vertices of $X(G, C)$. It is also a graph automorphism. To see this, note that

$$(yg)(xg)^{-1} = ygg^{-1}x^{-1} = yx^{-1},$$

and so xg is adjacent to yg if and only if x is adjacent to y.

Thus $X(G, C)$ is vertex transitive, since for any two vertices x and y, the automorphism $\rho_{x^{-1}y}$ maps x to y. □

Cayley graphs are important because every connected vertex-transitive graph is a retract of a Cayley graph (see Godsil and Royle [7]).

The following lemma is from Chris Godsil's colouring notes.

2.1.2 Lemma. *Let $X(G, C)$ be a Cayley graph for a group G, and let S be an independent set of X. If x is adjacent to y, then $S^{-1}x \cap S^{-1}y = \emptyset$.*

Proof. Suppose, on the contrary, that s is an element in $S^{-1}x \cap S^{-1}y$, then

$$s = a^{-1}x = b^{-1}y,$$

for some $a, b \in S$, and so

$$ba^{-1} = yx^{-1} \in C,$$

but ba^{-1} is not in C, since S is an independent set. A contradiction. □

The size of the largest clique in a graph X is denoted by $\omega(X)$, and the size of the largest independent set by $\alpha(X)$. The following corollary is an easy consequence of Lemma 2.1.2

2.1.3 Corollary. *Let $X(G, C)$ be a Cayley graph for an Abelian group G. Then $\alpha(X)\omega(X) \leq |V(X)|$.* □

A Cayley graph is *normal* if its connection set is closed under conjugation. The chromatic number of a graph X is denoted by $\chi(X)$. The following observation is due to Chris Godsil.

2.1.4 Theorem. *Let $X(G, C)$ be a normal Cayley graph. If $\alpha(X)\omega(X) = |V(X)|$, then $\chi(X) = \omega(X)$.*

Proof. Clearly $\chi(X) \geq \omega(X)$. Let $\omega(X) = \omega$. We will prove that there exists an ω-colouring of X.

Since X is undirected and normal, it follows that the vertex g is adjacent to h if and only if g^{-1} is adjacent to h^{-1}. To see this, suppose that g is adjacent to h. Then

$$h^{-1}g = h^{-1}(gh^{-1})h.$$

Since C is inverse-closed, it follows that $gh^{-1} \in C$, and since X is normal, it follows that $h^{-1}Ch = C$. Thus $h^{-1}g \in C$, and g^{-1} is adjacent to h^{-1}.

Let S be an independent set of size α. It follows from the above fact that the set S^{-1} is also an independent set.

Let u, v be two adjacent vertices. We have showed in Lemma 2.1.2 that $S^{-1}u \cap S^{-1}v = \emptyset$. We will show that for every $u \in X \setminus S^{-1}$, $S^{-1}u$ is an independent set.

Suppose, on the contrary, that $S^{-1}u$ is not an independent set. Then there exists $p, q \in S^{-1}$ such that pu is adjacent to qu. Thus

$$(qu)(pu)^{-1} = quu^{-1}p^{-1} \in C.$$

It follows that $qp^{-1} \in C$, and so p is adjacent to q. But S^{-1} is an independent set, a contradiction.

Let C be a clique of size ω. Since X is vertex-transitive, we can assume that C contains a vertex $v \in S^{-1}$. Then the set S^{-1}, together with the sets of the form $S^{-1}u$ where $u \in C \setminus \{v\}$, form a partition of the vertices in X of size ω. This partition gives us an ω-colouring of X. □

A *cubelike graph* is a Cayley graph on $\mathbb{Z}_2^n$. More specifically, it is defined as follows.

A cubelike graph $X_n(C)$ is the graph whose vertices are the binary vectors in $\mathbb{Z}_2^n$, and two vertices u and v are adjacent if and only if $u + v$ is an element in C.

Cubelike graphs are normal, and so Theorem 2.1.4 holds. In fact, all abelian Cayley graphs are normal. We will show that a cubelike graph is either complete, in which case the chromatic number is $2^n - 1$, or else it has chromatic number at most 2^{n-1}.

2.1.5 Theorem. *Let $X_n(C)$ be a cubelike graph on 2^n vertices. If it is not complete, then $\chi(X_n) \leq 2^{n-1}$.*

Proof. Since X_n is not complete, there exists a non-zero vector $v \notin C$. This vector induces a perfect matching in $\bar{X_n}$, in which each matching edge is of the form $x(x + v)$, where x is a vertex in X_n. The two ends of each edge in this matching form an independent set of size two in X_n. Hence $\chi(X_n) \leq |V|/2 = 2^{n-1}$.

2.2 An Example

The *Clebsch graph* is a cubelike graph $X_4(C)$ where

$$C = \{0001,\ 0010,\ 0100,\ 1000,\ 1111\}.$$

The Clebsch graph is vertex-transitive by Theorem 2.1.1.

The Clebsch graph is important because it is the unique strongly regular graph with parameters $[16, 5, 0, 4]$ (see Godsil and Royle [7]).

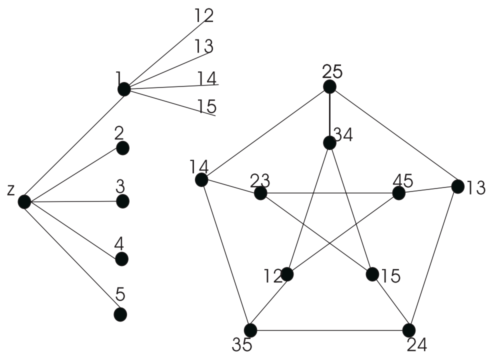

Figure 2.1: The Clebsch Graph

Another description of the Clebsch graph X is as follows (see Figure 2.1). The vertices are

$$V(X) = \{z\} \cup S_1 \cup S_2,$$

where the vertices in S_1, labelled $1, 2, 3, 4, 5$, form an independent set, and the vertices in S_2 induce a copy of the Petersen graph, in which the vertices are the subsets of the set $\{1, 2, 3, 4, 5\}$ of size two, and two subsets are adjacent if they are disjoint.

The special vertex z is adjacent to all vertices in S_1. The vertex in S_1 labeled $\{i\}$ is adjacent to all vertices in S_2 whose label contains i.

2.2.1 Lemma. *Let X be the Clebsch graph. Then $\alpha(X) = 5$, and every independent set of size five is the neighbourhood of a vertex.*

Proof. Let S be a maximum-size independent set. Since X is vertex-transitive, we can assume that $z \in S$. The set $S \setminus \{z\}$ contains vertices of distance two from z, and these vertices form an independent set in S_2. A maximum-size independent set in the Petersen graph consists of four vertices whose label contains a common element, say i. And by the description of X, this independent set is adjacent to the vertex in S_1 labeled i. Thus S is of size five and is in the neighbourhood of the vertex i. □

2.2.2 Theorem. *Let X be the Clebsch graph. Then $\chi(X) = 4$.*

Proof. Since X has 16 vertices, and $\alpha(X) = 5$, it follows that

$$\chi(X) \geq \lceil \frac{16}{5} \rceil = 4.$$

The Petersen graph induced by the vertices in S_2 has a 3-colouring $\mathcal{C}$. The colours are labeled $1, 2, 3$. Since the vertices in S_1 form an independent set, they can all be assigned the colour 4. The special vertex z is of distance two from any vertex in S_2, and so we assign colour 1 to z. □

2.3 Lexicographic Product

The *lexicographic product* $X[Y]$ of two graphs X and Y has vertex set $V(X) \times V(Y)$ where (x, y) is adjacent to (x', y') if and only if

(a) x is adjacent to x' in X, or

(b) $x = x'$ and y is adjacent to y' in Y.

The lexicographic product of any two cubelike graphs is cubelike.

2.3.1 Theorem. *Let X be the Clebsch graph. Then $\chi(X[K_4]) = 14$.*

Proof. We will first describe a 14-colouring of $X[K_4]$. The graph $X[K_4]$ can be constructed from X by replacing each vertex x by a 4-clique C_x, and if two vertices x and y are adjacent in X, then all vertices in C_x are adjacent to all vertices in C_y. Thus any colouring of $X[K_4]$ corresponds to a colouring of X where each vertex has four different colours.

We first colour the vertices in the Petersen graph induced by S_2. These vertices are the subsets of the set {1,2,3,4,5} of size two, and two vertices are adjacent if the subsets are disjoint. The labels of these vertices give us a colouring of the Petersen graph in which each vertex is coloured two distinct colours. We can extend this colouring so that each vertex is coloured four colours as follows. For each vertex $\{i, j\}$ in S_2 we colour it $\{i, j, i', j'\}$. For the vertices in S_1, we assign four colours different from the ones we used in the vertices in S_2. Since the special vertex z is not adjacent to the vertices in S_2, we can assign any four colours used in S_2 to z. Thus we obtain a 14-colouring of $X[K_4]$.

We will prove that $X[K_4]$ is not 13-colourable using linear programming. The idea originated with Alastair Farrugia. Suppose, for contradiction, that $X[K_4]$ has a 13-colouring. Since $\alpha(X[K_4]) = 5$, there must be 12 colour classes of size 5 and one colour class of size 4. We can view this as 13 independent sets that cover each vertex of X four times.

Every independent set of size 5 in X is the neighbourhood of a vertex, and so we only need to consider the independent set of size 4, denoted S. Since X is vertex-transitive, we can assume that z is a vertex in S. Then S contains three vertices that are of distance two from z, and so they are from the Petersen graph whose vertices are the subsets of size two of $\{1, 2, 3, 4, 5\}$. An independent set of size three in the Petersen

graphs consists either three subsets whose labels contain a common element i, or three subsets of the form $\{i, j\}$, $\{j, k\}$ and $\{k, i\}$.

Let x be the sum of characteristic vector of the 12 independent sets of size 5 in X. Since each vertex in X is coloured four different colours, each entry of x is at most 4. Let y be the characteristic vector of the independent set of size 4. If A is the adjacent matrix of X then it follows that

$$\frac{1}{4}(Ax + y) = \mathbf{1} \tag{2.1}$$

where $\mathbf{1}$ is the all-ones vector. If there exists a 13-colouring, then there exists an integer solution to (2.1).

The computation for y was carried out by the author, who found that there is no integer solution for x. □

Chapter 3

Eigenvalue Bound

A Cayley graph $X(G, C)$ is *linear* if the connection set C is closed under scalar multiplication. Lovász [9] derived a simple expression for all eigenvalues of linear Cayley graphs. We will use this information to bound the independence number of a Cayley graph, and thus bound its chromatic number.

3.1 Characters of Abelian Group

Let G be an abelian group of order n. A character of G is a homomorphism from G into the non-zero complex numbers, viewed as a multiplicative groups. The set of all characters of G will be denoted by G^*. The trivial character is the homomorphism which maps each element of G to 1. If $g \in G$ then $g^n = 1$ and so if $\phi \in G^*$ then

$$1 = \phi(g^n) = \phi(g)^n.$$

Thus $\phi(g)$ is an n-th root of unity for all elements g of G and all characters ϕ. If $\phi \in G^*$ then $\bar{\phi}$ is the character which maps an element $g \in G$ onto the complex conjugate of $\phi(g)$. As $\phi(g)\bar{\phi}(g) = 1$, we deduce that $\bar{\phi}(g) = \phi^{-1}(g)$. If ϕ and ψ are characters of G then the product $\phi\psi$ maps g in G onto $\phi(g)\psi(g)$. It follows from these observations that G^* is itself a group, with the trivial character as the identity element, and ϕ^{-1} equals to $\bar{\phi}$.

3.1.1 Lemma. *Let G be an abelian group of order n and let ϕ be a non-trivial character of G. Then*

$$\sum_{g \in G} \phi(g) = 0.$$

Proof. This follows from an observation that, for any non-zero element $a \in G$, we have

$$\sum_{g \in G} \phi(g) = \sum_{g \in G} \phi(ag) = \sum_{g \in G} \phi(a)\phi(g) = \phi(a) \sum_{g \in G} \phi(g).$$

Since ϕ is non-trivial, it follows that $\phi(a) \neq 1$ for some $a \in G$, and so $\sum_{g \in G} \phi(g) = 0$. □

3.1.2 Lemma. *Let $V = (\mathbb{Z}_q)^n$ be a space of column vectors over the field $\mathbb{Z}_q$, where q is a prime power. If $a \in V$ and ϕ is a non-trivial character of the additive group of $\mathbb{Z}_q$ then the mapping*

$$\phi_a : x \mapsto \phi(a^T x)$$

is a character of V, viewed as an abelian group. If $a \neq b$ then $\phi_a \neq \phi_b$, and so all characters of V arise in this way.

Proof. It is routine to check that ϕ_a is a character of V. If a and b are elements of V then

$$\sum_{u \in V} \phi_a(u)\bar{\phi_b}(u) = \sum_{u \in V} \phi_{a-b}(u).$$

from which it follows that ϕ_a and ϕ_b are orthogonal if $a \neq b$. □

3.2 Eigenvalues of Cayley Graphs

The *character table* of G is the complex matrix with rows and columns indexed respectively by the characters and elements of G, and ij-th entry of the character table equals to the value of the i-th character on the j-th element of G.

Let ϕ be a character of the group G and let C be a subset of G. Define

$$\phi(C) = \sum_{v \in C} \phi(v).$$

The following is due to Lovász [9].

3.2.1 Lemma. *Let G be a finite abelian group, and let C be a subset of $G \backslash 0$. Let A be the adjacency matrix of the Cayley graph $X(G, C)$. Then the rows of the character table H of G are a complete set of eigenvectors for A, and the eigenvector belonging to the character ψ has the eigenvalue $\psi(C)$.*

Proof. For every vertex $v \in G$, we observe that

$$A\phi(v) = \sum_{vw \in E(X)} \phi(w) = \sum_{c \in C} \phi(cv) = \sum_{c \in C} \phi(c)\phi(v) = \phi(v)\phi(C),$$

Thus ϕ is an eigenvector with eigenvalue $\phi(C)$. By Lemma 3.1.2, the rows of H are orthogonal, and so they are distinct eigenvectors. □

3.2.2 Lemma. *Let V be an n-dimensional vector space over the field $\mathbb{Z}_q$ where q is a prime power, and let $\mathcal{P}$ be the projective space where the points are the 1-dimensional subspaces of V. Let S be a subset of $\mathcal{P}$, and let X be the Cayley graph with vectors in V as vertices, and two vertices are adjacent if their difference is a coordinate vector of a point in S. Then each hyperplane H of $\mathcal{P}$ corresponds to $q-1$ linearly independent eigenvectors of $A(X)$, each with eigenvalue*

$$q|H \cap S| - |S|.$$

The eigenvectors determined by distinct hyperplanes are linearly independent.

Proof. Let C be a set of coordinate vectors of the points in S. Then $|C| = (q-1)|S|$. By Lemma 3.2.1, it follows that every character ψ gives rise to a eigenvector. By Lemma 3.1.2, $\psi = \phi_a$ where ϕ is a non-trivial character of $\mathbb{Z}_q$, and $a \in V$. If $\lambda \in \mathbb{Z}_q \setminus 0$ then the characters $\phi_{\lambda a}$ are orthogonal and have the same kernel. This kernel determines a hyperplane $a^{\perp}$.

The eigenvalue of $\phi_{\lambda a}$ is given by the following formula,

$$\phi_{\lambda a}(C) = \sum_{c \in C} \phi(\lambda a^T c).$$

Let R be a point in $S \cap H$ (a 1-dimensional subspace of V). Then $\phi_{\lambda a}(x) = \phi(\lambda a^T x) = 1$ for all $x \in R$, and so

$$\sum_{x \in R \backslash 0} \phi_{\lambda a}(x) = q - 1.$$

Let P be a point in $S \setminus H$. Then by Lemma 3.1.1

$$\sum_{y \in P \backslash 0} \phi_{\lambda a}(y) = -1.$$

It follows that

$$\begin{aligned} \phi_{\lambda a}(C) &= (q-1)|S \cap H| - |S \setminus H| \\ &= q|S \cap H| - |S|. \end{aligned}$$

Linear independence follows from Lemma 3.2.1 □

3.3 Ratio Bound

We will develop the ratio bound on the independence number of regular graphs, which we will use in subsequent chapters. This bound is due to Hoffmann.

3.3.1 Lemma. *Let X be a k-regular graph with v vertices and least eigenvalue τ. Then*

$$\alpha(X) \leq \frac{v}{1 + \frac{k}{-\tau}}. \tag{3.1}$$

Proof. Let S be an independent set in X with characteristic vector z. Let A be the adjacency matrix of X, and let the matrix M be given by

$$M := A - \tau I - \frac{k-\tau}{v} J.$$

The eigenvalues of M are non-negative, and therefore $M \succeq 0$. Consequently

$$0 \leq z^T M z = z^T A z - \tau z^T z - \frac{k-\tau}{v} z^T J z = z^T A z - \tau |S| - \frac{k-\tau}{v} |S|^2.$$

Since S is independent, it follows that $z^T A z = 0$ and hence we have

$$\frac{k-\tau}{v} |S|^2 \leq -\tau |S|.$$

This yields the bound of the theorem. □

The bound (3.1) is called the *ratio bound* on the independence number of X. Since $\chi(X)\alpha(X) \geq |V(X)|$ for any graph X, we see that for k-regular graphs the previous lemma implies that

$$\chi(X) \geq 1 + \frac{k}{-\tau}.$$

Chapter 4

Free Cayley Graphs

Free Cayley graphs are introduced by Naserasr and Tardif [11]. Let $Y = (V, E)$ be a graph with vertex set V and edge set E. Suppose that there is a graph homomorphism from Y to a Cayley graph $X(G, C)$. Let d be the exponent of G. The *free Cayley graph* $\mathbb{Z}_d[Y]$ is defined to be the Cayley graph with vertex set $G_F = \mathbb{Z}_d^{|V|}$ and connection set

$$C_F = \{e_v - e_w : \ vw \in E(Y)\}$$

Here e_v denotes the vector in $\mathbb{Z}_d^{|V|}$ with 1 in the v-th position and 0 in all the other positions. We will only deal with simple undirected graphs, so we can assume that Y is simple and undirected, and so is $\mathbb{Z}_d[Y]$.

Free Cayley graphs are interesting because they embed information about smaller graphs. Suppose that Y is a graph and $\mathbb{Z}_d[Y]$ is the free Cayley graph defined on Y. We can view the connection set of $\mathbb{Z}_d[Y]$ as the set of columns of the incidence matrix of Y. In this section we will discuss the relationship between Y and $\mathbb{Z}_d[Y]$, and derive bounds on the chromatic number of Cayley graphs.

4.1 Free Cayley Graphs

The following observations are due to Naserasr and Tardif [11].

4.1.1 Theorem. *Let Y be a graph and let G be a group with exponent d. Suppose that there is a graph homomorphism ψ from Y to a Cayley graph $X(G, C)$. Then there is a map $\widehat{\psi}$ from $\mathbb{Z}_d[Y]$ to X which is both a graph and a group homomorphism.*

Proof. Suppose that ψ is a graph homomorphism from Y to $X(G, C)$. If the vertex v is adjacent to the vertex w in Y, then $\psi(v)$ is adjacent to $\psi(w)$. In other words, if $e_w - e_v \in C_F$ then $\psi(e_w)\psi(e_v)^{-1} \in C$.

We extend ψ to a group homomorphism $\widehat{\psi}$ from $\mathbb{Z}_d[Y]$ to X. For any an element of $a \in \mathbb{Z}_d^{|V|}$, we have

$$a = a_1 e_1 + \ldots + a_n e_n$$

where $e_1, \ldots, e_n$ are the canonical embedding of the vertices of Y. These vectors form a set of generators of the group $\mathbb{Z}_d^{|V|}$.

We define the function $\widehat{\psi}$ on the element a as follows,

$$\widehat{\psi}(a) = a_1\psi(e_1) + \ldots + a_n\psi(e_n).$$

The function $\widehat{\psi}$ is well defined and is a group homomorphism from $\mathbb{Z}_d^{|V|}$ to G. We will show that it is also a graph homomorphism.

Let a, b be two adjacent vertices in the graph $\mathbb{Z}_d[Y]$. Then $b - a \in C$. Thus $b - a = e_w - e_v$ for some e_v and e_w. We have

$$\widehat{\psi}(b)\widehat{\psi}(a)^{-1} = \widehat{\psi}(b - a) = \widehat{\psi}(e_w - e_v) = \psi(e_w)\psi(e_v)^{-1} \in C.$$

Hence $\widehat{\psi}(a)$ is adjacent to $\widehat{\psi}(b)$, and so $\widehat{\psi}$ is a graph homomorphism. □

4.1.2 Corollary. *Let X be a Cayley graph of a group with exponent d. Then $\chi(X) = \chi(\mathbb{Z}_d[X])$.*

Proof. Since X is a subgraph of $\mathbb{Z}_d[X]$, it follows that $\chi(X) \leq \chi(\mathbb{Z}_d[X])$. Moreover, since there is a graph homomorphism from the Cayley graph X to itself, there is a graph homomorphism from $\mathbb{Z}_d[X]$ to X, and hence $\chi(\mathbb{Z}_d[X]) \leq \chi(X)$. □

4.1.3 Corollary. *Suppose there is a graph homomorphism $X \mapsto Y$. Then there is a graph homomorphism $\mathbb{Z}_r(X) \mapsto \mathbb{Z}_r(Y)$.*

Proof. Since Y is a subgraph of $\mathbb{Z}_r[Y]$, there is a graph homomorphism $X \mapsto \mathbb{Z}_r[Y]$, and so there is a graph homomorphism $\mathbb{Z}_r[X] \mapsto \mathbb{Z}_r[Y]$. □

4.2 Halved Cubes

Let X denote the n-cube, and let Y denote the graph with vertex set $V(X)$ where two vertices are adjacent in Y if and only if they are at distance two in X. The graph Y is not connected, but has two isomorphic components on 2^{n-1} vertices. The graph induced by one component is called the *halved n-cube*. We can also define the halved n-cube to be the graph on the binary vectors of length n with even weight, where two such vectors are adjacent if and only if their sum has weight two. We denote the halved n-cube by $\frac{1}{2}Q_n$.

Another description of $\frac{1}{2}Q_n$ is the graph obtained from the vertices of $(n-1)$-cube, by joining two vertices if they lie at distance one or two in the $(n-1)$-cube. To see this, delete the last coordinate from each binary vector of length n with even weight. Two of these truncated vectors are adjacent if and ony if their sum has weight one or two.

The eigenvalues of $\frac{1}{2}Q_n$ can be computed easily. Let A_1 be the adjacency matrix of the n-cube X, and let A_2 be the distance two graph Y of the n-cube. We have

$$A_1^2 - nI = 2A_2,$$

from which we can determine the eigenvalues of Y. The eigenvalues of X are the integers $n - 2i$ for $i = 1, \dots, n$, and therefore the eigenvalues of Y are the integers

$$\frac{1}{2}[(n-2i)^2 - n] = \binom{n}{2} - 2i(n-i).$$

The following lemma provides one reason why we are interested in the halved cubes.

4.2.1 Lemma. *Each of the two components of the graph $\mathbb{Z}_2(K_n)$ is isomorphic to $\frac{1}{2}Q_n$.*

Proof. The connection set of $\mathbb{Z}_2(K_n)$ consists of the columns of the adjacency matrix of K_n, which is the set of all binary n-bit vectors of weight two. Thus each of the two (isomorphic) components of $\mathbb{Z}_2(K_n)$ is isomorphic to $\frac{1}{2}Q_n$ according to the first definition of $\frac{1}{2}Q_n$. □

Linial, Meshulam and Tarsi proved that the following theorem is true for $0 \leq i \leq 3$. Chris Godsil proved two cases using the ratio bound. Here we will present Godsil's proof.

4.2.2 Theorem.

$$\chi(\mathbb{Z}_2(K_n)) \leq 2^{\lceil \log_2(n) \rceil}$$

equality holds if $n = 2^r - i$, where $i \in \{0, 1\}$.

Proof. If $n = 2^r$ then K_n is a cubelike graph on $\mathbb{Z}_2^r$. Since $K_n \mapsto K_n$, it follows that $\mathbb{Z}_2(K_n) \mapsto K_n$. Since $\mathbb{Z}_2(K_n)$ contains the even vectors in $\mathbb{Z}_2^r$ and that each fibre of this map is an independent set, it follows that the fibres of this map are the cosets of a linear even binary code with minimum distance at least four; this must be the extended binary Hamming code.

The halved n-cube has valency $\binom{n}{2}$. If $n = 2m$ or $2m + 1$, then its least eigenvalue is $-m$. So if $n = 2^r$, the ratio bounds (see Lemma 3.3.1) on $\alpha(X)$ is

$$\frac{2^{n-1}}{1 + \frac{\binom{n}{2}}{\frac{n}{2}}} = \frac{2^{n-1}}{2^r} = 2^{n-1-r}$$

and therefore $\chi(X) \geq 2^r$. Since the halved 2^r-cube has a 2^r-colouring, it follows that its chromatic number is 2^r.

If $n = 2^r - 1$, the ratio bound is still 2^{n-1-r}, and therefore $\chi(X) \geq 2^r$. Since the halved $(n-1)$-cube is a subgraph of $\frac{1}{2}Q_n$, it follows that the halved $(2^r - 1)$-cube has chromatic number 2^r. □

4.3 Folded Cubes

We will introduce folded cubes and show that they have chromatic number four. If a cubelike graph is not bipartite, then it contains a folded cube and hence is not 3-colourable.

Folded cubes can be obtained from the n-cubes. Let Q_n be an n-cube. We can view Q_n as a graph with the subsets of $\{1, \ldots, n\}$ as its vertices, where subsets S and T are adjacent if and only if $|S \triangle T| = 1$. Each subset S determines a partition $(S, \bar{S})$ of $\{1, \ldots, n\}$ with two cells. The folded cube is the graph with these partitions as its vertices, where two partitions are adjacent if a cell of one is adjacent to a cell of the other in Q_n. The folded 3-cube is K_4 and the folded 5-cube is the Clebsch graph.

We are interested in two alternative descriptions. Assume n is odd. We construct a graph on the subsets of $\{1, \ldots, n\}$ with size at most $(n-1)/2$. Two such subsets are adjacent if either:

(a) They differ in size by 1, and one is contained in the other, or

(b) They both have size $(n-1)/2$, and they are disjoint.

The folded n-cube can also be described as follows. Take the $(n-1)$-cube Q_{n-1}. We can construct the folded n-cube by adding edges to pairs of vertices with distance n.

The following observation is due to Chris Godsil.

4.3.1 Theorem. *If C is a cycle of $2k+1$ vertices, then each of the two components of $\mathbb{Z}_2[C]$ is isomorphic to the folded $(2k+1)$-cube.*

Proof. Let $c_1, \ldots, c_{2k+1}$ be the characteristic vectors of the edges of C. Consider the matrix A whose columns are the c_i's,

$$A = [c_1 \ c_2 \ \ldots \ c_{2k+1}].$$

The first $2k$ columns are linearly independent and the last column is the sum of all the other columns.

There is a linear mapping from the column space of the matrix A to the column space of the following matrix B,

$$B = [e_1\ e_2\ \ldots\ e_{2k}\ (e_1 + e_2 + \ldots + e_{2k})].$$

where e_i is the i-th standard basis vector (with one in the i-th position and zeros everywhere else). The cubelike graph whose connection set is B is a folded n-cube according to the last description of the folded cubes.

□

4.3.2 Theorem. *Let $X(C)$ be a cubelike graph with connection set C. If $X(C)$ is not bipartite then it contains a folded cube.*

Proof. If $X(C)$ is not bipartite, then it contains an odd cycle C_{2k+1}. This cycle corresponds to $2k + 1$ vectors in the connection set C. Denote these vectors $v_1, v_2, \ldots v_{2k+1}$ where $v_1 + v_2 + \ldots + v_{2k+1} = 0$. Let

$$C' = \{v_1,\ v_2,\ \ldots,\ v_{2k+1}\}$$

Then the Cayley graph with connection set C', which is a subgraph of X, is isomorphic to a folded cube. □

In the next section we will show that the chromatic number of folded cubes is four. Thus if a cubelike graph is not bipartite, its chromatic number is at least four.

4.4 Chromatic Number of Folded Cubes

We will show that the chromatic number of $\mathbb{Z}_2[C_{2k+1}]$ is four. First of all, since there is a graph homomorphism from C_{2k+1} to C_3, there is a graph homomorphism from C_{2k+1} to $\mathbb{Z}_2[C_3]$, and by Theorem 4.1.1, there is a graph and group homomorphism from $\mathbb{Z}_2[C_{2k+1}]$ to $\mathbb{Z}_2[C_3] = 2K_4$ (here I mean two vertex-disjoint copies of K_4). Thus $\mathbb{Z}_2[C_{2k+1}]$ is 4-colourable. We will show that it is not 3-colourable.

We proceed by showing that any folded cube contains a copy of *generalized Mycielski graph* whose chromatic number is four.

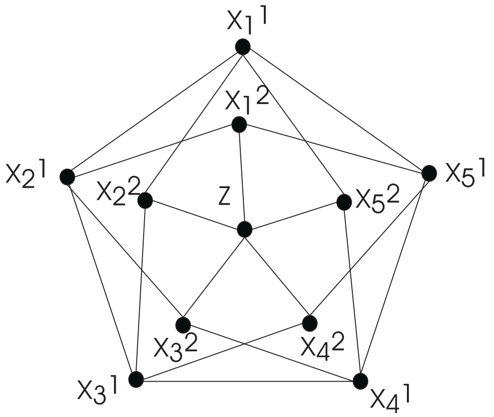

Figure 4.1: The Mycielski Graph $M_2(C_5)$

We are only interested in the generalized Mycielski graph of odd cycles. We define it as follows (see Figure 4.1).

Let $C_{2k+1} = \{v_1, v_2, \ldots, v_{2k+1}\}$ be an odd cycle of $2k+1$ vertices, and let d be an integer. The generalized Mycielski graph of C_{2k+1}, denoted $M_d(C_{2k+1})$, is the graph with vertex set

$$V = S_1 \cup S_2 \ldots \cup S_d \cup \{z\}$$

where

$$S_i = \{x^i_1, x^i_2 \ldots, x^i_{2k+1}\}$$

for $1 \leq i \leq d$.

The edges are defined as follows. The subgraph induced by S_1 is C_{2k+1}. For $2 \leq i \leq d$, the vertex v^i_j is connected to the vertices $v^{i-1}_{(j-1)}$ and $v^{i-1}_{(j+1)}$, where addition and substraction of the subscripts are taken modula $2k+1$. The special vertex z is connected to all vertices in S_d.

Payan [12] proved that the chromatic number of $M_d(C_{2k+1})$ is four. We will present a new version of his proof.

4.4.1 Theorem. $\chi(M_d(C_{2k+1})) = 4$.

Proof. We will develop some tools first.

Let $C = \{v_1, v_2, \ldots, v_{2k+1}\}$ be a directed cycle of $(2k+1)$ vertices which are labeled $1, 2, 3$. This labeling may or may not be a proper colouring. We construct a directed graph $T(C)$ with three vertices 1,2,3 by identifying the vertices of C labeled by $i \in \{1, 2, 3\}$ into the vertex i. The number of directed $\{1, 2, 3\}$-cycles in $T(C)$ is called the *index* of the cycle C, denoted $t(C)$. Clearly $t(C) \geq 0$. If $t(C) > 0$ we know that all three labels $1, 2, 3$ are used.

Let $C = \{v_1, \ldots, v_{2k+1}\}$ be a directed cycle of $(2k+1)$ vertices. Consider the subdivision of C obtained by adding a vertex v'_i on each arc $v_i v_{i+1}$ where the addition of the subscripts are taken modula $2k+1$. Let D be the set of vertices on the arcs of C, i.e., $D = \{v'_i : 1 \leq i \leq 2k+1\}$. For any colouring of D with three colours $1, 2, 3$ we have $t(D) = t(C)$.

To see this, consider the reduced graph obtained from C by identifying the vertices of the same colour, let us colour each arc $v_i v_{i+1}$ by the colour given to the vertex v'_i. Note that if v_i and v_{i+1} are coloured differently, then the arc $v_i v_{i+1}$ is coloured uniquely. So every directed $\{1, 2, 3\}$-cycle on the vertices in $T(C)$ corresponds to a directed $\{1, 2, 3\}$-cycle on the edges. Hence $t(C) = t(D)$.

Consider an odd cycle $C = \{v_1, \ldots, v_{2k+1}\}$ and a colouring of C with three colours $1, 2, 3$. Let P be the distance-two graph of C, i.e.,

$$P = \{v_1, v_3, \ldots, v_{2k+1}, v_2, v_4, \ldots, v_{2k}\}.$$

Then $t(P) > 0$.

We prove the above by induction on k. The property is true for the cycle of length 3. When $k > 1$ we have two cases.

(a) If C is coloured $1, 2, 3, 1, 2, 3, \ldots, 1, 2, 3$ then $t(P) = (2k+1)/3$.

(b) C contains three vertices v_i, v_{i+1}, v_{i+2} such that v_i and v_{i+2} have the same colour. We can assume, without loss of generality, that v_1, v_2, v_3 are coloured $1, 2, 1$. Let C' be obtained from C by deleting v_2 and identifying v_1, v_3. Since C has a colouring, so does C'. Let P' be the distance-two graph of C'. Then P' is obtained from P by deleting v_1

and v_2 and adding the arc $v_{2k}v_3$ and $v_{2k+1}v_4$. By induction hypothesis, $t(P') > 0$. Adding back the vertex v_1 on the arc $v_{2k}v_3$ and the vertex v_2 on the arc $v_{2k+1}v_4$ does not decrease the index of the cycle. Hence $t(P) \geq t(P') > 0$.

Now we are ready to prove that the chromatic number of $M_d(C_{2k+1})$ is four.

The subgraph induced by S_1 is C_{2k+1} and is 3-colourable. Suppose that we have a 3-colouring of the vertices in any S_i, where $1 \leq i \leq d-1$. Since each vertex in S_{i+1} is adjacent to exactly two vertices in S_i, we can extend this colouring to a 3-colouring of the vertices in S_{i+1}. Thus we obtain a 3-colouring of the vertices in $S_1 \cup \ldots \cup S_d$. We assign the fourth colour to the vertex z to get a 4-colouring of $M_d(C_{2k+1})$.

We will also show that $M_d(C_{2k+1})$ does not have a 3-colouring. Consider any 3-colouring of $M_d(C_{2k+1})$. Since the vertices in S_1 form an odd cycle, we need to use three colours. Thus $t(S_1) > 0$. Let S_1' be the distance two graph of S_1. Then $t(S_1') > 0$. Consider the subdivision graph of S_1' obtained by adding vertices on the arcs of S_1'. The vertices on the arcs are exactly the vertices in S_2, and so $t(S_2) > 0$. Similarly we can show that $t(S_3) > 0$ and eventually $t(S_d) > 0$. Thus the vertices of S_d must use three colours, and the vertex z must use the forth colour. □

The following theorem shows why we are interested in the generalized Mycielski graph. It was originally proved by Naserasr and Tardif [11], and was proved again by Gordon Royle in a simpler way. Here we will present the simpler proof by Gordon Royle.

4.4.2 Theorem. *The folded cube $\mathbb{Z}_2[C_{2k+1}]$ contains $M_k(C_{2k+1})$.*

Proof. Consider the $k \times (2k+1)$ matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & \ldots \\ & & & \ldots & & & & & & \end{pmatrix}$$

The i-th row contains i ones in columns $1, 3, \ldots, 2i$, for $1 \leq i \leq k$. The rows of M and their cyclic shifts, together with the zero vector, induce a copy of $M_k(C_{2k+1})$, where z is the zero vector, and S_i is the cyclic shifts of the i-th row. It is easy to check that the conditions in the construction of $M_k(C_{2k+1})$ are satisfied. □

In conclusion, if a cubelike graph is not bipartite then it contains a copy of $\mathbb{Z}_2[C_{2k+1}]$ whose chromatic number is four, and therefore no cubelike graph has chromatic number three.

Chapter 5

Triangle-free Graphs

Let X be a regular maximal triangle-free graph. We will show that if X has valency greater than $|V(X)|/3$ then it is 4-colourable. We will also show that if X is vertex-transitive then it is 3-colourable. Our discussion is based on a paper by Brandt [2]. Applying this result to Cayley graphs, we conclude that if X is a maximal triangle-free Cayley graph on 2^n vertices with valency greater than $2^n/3$, then X is bipartite.

5.1 Regular Graphs

We will present a version of Brandt's proof with corrections.

We consider only finite, simple and undirected graphs. If G is a maximal triangle-free graph, then G has the following properties,

(a) every adjacent pair of vertices has no common neighbour,

(b) every non-adjacent pair of vertices has a common neighbour, and

(c) G has diameter two.

A *feasible weight function* is a function $\phi : V \mapsto R$, such that, for every vertex v,

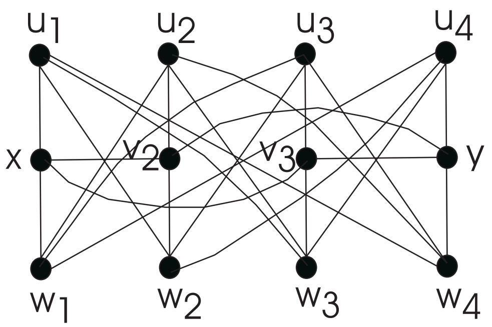

Figure 5.1: The subgraph H_{12}

(a) $\phi(v) \geq 0$, and

(b) $\phi(N(v)) \geq 1$,

where $N(v)$ denotes the neighbourhood of the vertex v.

The 3-cube Q_3 can be obtained from complete bipartite graph $K_{4,4}$ by deleting a perfect matching.

The main result of Brandt's paper is based on the following important lemma.

5.1.1 Lemma. *Let G be a maximal triangle-free graph and let ϕ be a feasible weight function. If the total weight is less than 3 then G does not contain the Q_3 as an induced subgraph.*

Proof. Suppose, for contradiction, that G has the Q_3 as an induced subgraph. Let u_1, u_2, u_3, u_4 be four vertices on one side of the bipartition of Q_3. Let w_1, w_2, w_3, w_4 be four other vertices such that $w_iu_i \notin E(G)$ and $w_iu_j \in E(G)$ for all $j \neq i$. Since G has diameter 2, for every pair of vertices u_i, w_i, there is a common neighbour v_i, which cannot be adjacent to any further vertex u_j, w_j $(j \neq i)$. Since $\phi(V(G)) < 3$ and $\phi(N(v)) \geq 1$ for every $v \in V(G)$, there must be a vertex x that is adjacent to more than four vertices in

$$V' = \cup_{1 \leq i \leq 4}\{u_i, v_i, w_i\}.$$

To see this, suppose that every vertex in G is adjacent to at most four vertices of V'. Let T_i be the set of vertices that has i neighbours in V',

$0 \leq i \leq 4$. In other words, the vertices in T_i are in i neighbourhoods of the vertices of V'. If we count the total value of ϕ on the neighbourhoods of the vertices in V', we count i times the value of $\phi(T_i)$. Thus

$$\phi(T_1) + 2\phi(T_2) + 3\phi(T_3) + 4\phi(T_4) \geq 12.$$

However, since the total weight is less than three, we have

$$\phi(T_1) + \phi(T_2) + \phi(T_3) + \phi(T_4) < 3,$$

which gives us a contradiction.

We have shown that there exists a vertex x in G adjacent to at least five vertices in V'. The indices may be chosen such that u_1, w_1, v_2, v_3, v_4 are the neighbours of x.

Consider the subgraph H spanned by the 9 vertices $\bigcup_{2\leq i\leq 4}\{u_i, v_i, w_i\}$. Since $\phi(V(G) < 3$ and $\phi(N(v)) \geq 1$ for every $v \in V(G)$, there must be a vertex y of G being adjacent to four vertices of H which we may assume to be v_2, v_3, u_4, w_4. Since G is triangle-free, no vertex of G can be adjacent to more than four vertices in the subgraph H_{12} induced by $\{x, v_2, v_3, y\} \cup \bigcup_{1\leq i\leq 4}\{u_i, w_i\}$ (see Figure 5.1), and hence

$$\phi(V(G)) \geq \frac{1}{4} \sum_{v\in H_{12}} \phi(N(v)) \geq 3.$$

A contradiction. □

5.1.2 Theorem. *Let G be a maximal triangle-free graph and let ϕ be a feasible weight function. If the total weight is less than 3 then every independent set of maximum weight of G is contained in the neighbourhood of a vertex.*

Proof. Suppose that S is an independent set of maximum weight that is not contained in the neighbourhood of a vertex. Let S' be a minimal subset of S that is not contained in the neighbourhood of a vertex. Since G has diameter two we get $|S'| \geq 3$ and, by the minimality of S', for every vertex u_i of S' ($1 \leq i \leq |S'|$) there is a vertex $w_i \in V(G)$ that is adjacent to all vertices of S' except u_i. If $|S'| \geq 4$ then we have an induced Q_3, which is impossible by Lemma 5.1.1.

Suppose that $|S'| = 3$. Let T_0 be the set of vertices of G having no neighbour in S'. Clearly $S \subseteq T_0$. Let T_2 be the vertices of G having exactly two neighbours in S'. Since $\phi(V(G)) < 3$ we have

$$\phi(T_1) + 2\phi(T_2) \geq 3,$$

and

$$\phi(T_0) + \phi(T_1) + \phi(T_2) < 3.$$

Thus $\phi(T_0) < \phi(T_2)$.

Since $|S'| = 3$, any two vertices in T_2 have a common neighbour in S'. Thus the set T_2 is an independent set of larger weight than S, a contradiction. □

Let G be a maximal triangle-free graph on n vertices with minimum valency greater than $n/3$. Let ϕ be the weight function assigning to each vertex weight $(\delta(G))^{-1}$. Then G and ϕ satisfy the hypothesis of Theorem 5.1.2 and hence every maximum-weight independent set belongs to the neighbourhood of a vertex. Since ϕ is constant this implies that every maximum-size independent set is contained in the neighbourhood of a vertex.

Two vertices are *similar* if they have the same neighbourhood. Denote the similarity class of a vertex v by $S(v)$.

5.1.3 Lemma. *Let G be a maximal triangle-free graph of n vertices and minimum valency more than $n/3$. Let S be a class of similar vertices of G. Then there is a set $T \subseteq N(S)$ with $|T| \leq 3$ such that $\cap_{v \in T} N(v) = S$.*

Proof. Choose a minimal subset $T \subseteq N(S)$ with $\cap_{v \in T} N(v) = S$. By the minimality of T for every vertex $v_i \in T$ there is a vertex $w_i \notin S$, being adjacent to every vertex of T, except v_i. If $|T| \geq 4$ then $\cup_{1 \leq i \leq 4}\{v_i, w_i\}$ induces a Q_3. By Lemma 5.1.1, we know that the induced Q_3 does not exist. So $|T| \leq 3$. □

A set $S \subseteq V(G)$ is *dominating* if $S \cup N(S) = V(G)$. Brandt proved the following theorem.

5.1.4 Theorem. *Let G be a regular maximal triangle-free graph of order n with degree $d > n/3$. Then G contains a dominating star $K_{1,t}$ with $t \leq 3$.*

Proof. Choose a vertex v for which $|S(v)|$ is minimal and let $S = S(v)$. By Lemma 5.1.3, there must be a minimal subset $T = \{w_1, \ldots, w_t\} \subseteq N(v)$ of cardinality $t \leq 3$ such that $\cap_{w \in T} N(w) = S$. We claim that $T' = \{v\} \cup T$ is a dominating set of G.

Assume, for contradiction, that there exists a set of vertices R which are not dominated by T'. If $t = 1$ then all neighbours of v are similar, since G is regular. Suppose $t = 2$. Since $d \geq n/3$, we have

$$n < d(v) + d(w_1) + d(w_2) \leq n - |R| + |S|,$$

which implies that $|R| < |S|$ and hence $R = \emptyset$ by the minimality of S.

Finally assume that $t = 3$. Since G is d-regular with $d > n/3$, we have

$$d + n < 4d \leq d(v) + d(w_1) + d(w_2) + d(w_3) \leq n - |R| + |S| + |U|.$$

where U is the set of vertices that have at least two neighbours in T. Thus

$$d + n < n - |R| + |S| + |U|$$

Since every vertex in U has at least two neighbours in T, and T has three vertices, every pair of vertices in U have a common neighbour in T. Thus U is an independent set. By Theorem 5.1.2, $|U| \leq d$. We have

$$|R| < |S|$$

By the minimality of S, we have $R = \emptyset$ □

5.1.5 Corollary. *Let G be a d-regular maximal triangle-free graph with n vertices and valency $d > n/3$ then G is 4-colourable.*

Proof. We have shown that G has a dominating star $K_{1,t}$ with $t \leq 3$. Suppose that $t = 3$, and the vertices in the dominating star are denoted r, a, b, c with r being the root. Removing the star, we get four neighbourhoods $N(r), N(a), N(b), N(c)$. Since G is triangle free, each neighbourhood is an independent set, and so we can assign the same colour to all vertices in a neighbourhood. Let the colours assigned to the vertices in $N(r), N(a), N(b), N(c)$ be $1, 2, 3, 4$, respectively. Then we can colour the vertices r, a, b, c with $2, 1, 1, 1$. It is easy to check that this is a valid colouring. □

5.2 Vertex-Transitive Graphs

Let X be a maximal triangle-free graph with n vertices and valency greater than $n/3$. We have shown that it is 4-colourable. In this section we will show that if it is vertex-transitive then it is 3-colourable. The result is due to Brandt [2].

5.2.1 Lemma. *Let G be a maximal triangle-free graph with n vertices and minimum valency greater than $n/3$. If a, b are non-adjacent, non-similar vertices for which $|N(a) \cap N(b)|$ is as large as possible, then G contains an edge xy such that $xa, yb \in E(G)$ and all vertices in $N(a) \setminus N(b)$ are similar with x and all vertices in $N(b) \setminus N(a)$ are similar with y.*

Proof. Since a and b are not similar, there must be a vertex $x \in N(a) \backslash N(b)$. Since G has diameter two, x must have a neighbour $y \in N(b) \setminus N(a)$. We will first show that all vertices in $N(x) \cap N(b)$ are similar.

Suppose, for contradiction, that x has a neighbour $y' \in N(b) \backslash N(a)$ that is not similar to y. Then

$$\begin{aligned} d(x) + d(b) + d(y') + d(y) &\leq n + |N(x) \cap N(b)| + |N(y) \cap N(y')| \\ &\leq n + |N(x) \cap N(b)| + |N(a) \cap N(b)| \\ &\leq n + d(b). \end{aligned}$$

which implies that $\delta(G) \leq n/3$. A contradiction. Thus all vertices in $N(x) \cap N(b)$ are similar. Similarly we can show that all vertices in $N(y) \cap N(a)$ are similar.

Now we will prove that all vertices in $N(b) \setminus N(a)$ are adjacent to x. Suppose, for contradiction, that there exists a vertex $y' \in N(b) \setminus N(a)$ that is not adjacent to x. Since G has diameter two, y' is adjacent to a vertex $x' \in N(a) \setminus N(b)$, and x' is not adjacent to y (otherwise, x' is similar to x). Thus the vertices $\{a, x, y, b, y', x', a\}$ form a 6-cycle C. Moreover, no vertex is adjacent to three vertices of C. To see this, suppose that there is a vertex z adjacent to a, y', y, then $z \in N(y) \cap N(a)$, and so is similar to x, but x is not adjacent to y', a contradiction. Hence all vertices are adjacent to at most two vertices of the 6-cycle, and so

$$6\delta(G) \leq \sum_{v \in V(C)} d(v) \leq 2n$$

which implies that $\delta(G) \leq n/3$. A contradiction. □

5.2.2 Theorem. *Let G be a d-regular maximal triangle-free graph with n vertices and valency $d > n/3$. If G has chromatic number at least four, then there are two vertices $y, z \in V(G)$ with $|S(y)| \neq |S(z)|$.*

Proof. First observe that if G does not have two non-adjacent non-similar vertices, then G is the complete multi-partite graph. Suppose that a, b are two non-adjacent non-similar vertices such that $|N(a) \cap N(b)|$ is maximal. Then by Lemma 5.2.1, there is an edge xy where $x \in N(a)$ and $y \in N(b)$ such that all vertices in $N(a) \setminus N(b)$ are similar to x, and all vertices in $N(b) \setminus N(a)$ are similar to y. If all vertices in G are adjacent to a, x, y then G is 3-colourable. Thus there exists a vertex z that is not adjacent to a, x, y. The vertex z is also not adjacent to b, since $N(b) \subseteq N(a) \cup N(x)$. Let

$$R = V(G) \setminus (N(a) \cup N(b) \cup N(x) \cup N(y))$$

Then

$$\begin{aligned} n - |R| &= |(N(a) \cup N(b) \cup N(x) \cup N(y)| \\ &= d(a) + d(b) + d(x) + d(y) \\ &- |N(a) \cap N(b)| - |N(a) \cap N(y)| - |N(b) \cap N(x)| \\ &\geq d(b) + d(x) + d(y) - |S(y)| \\ &> n - |S(y)|. \end{aligned}$$

It follows that $|S(y)| > |R| \geq |S(z)|$ □

5.2.3 Corollary. *Let G be a vertex-transitive maximal triangle-free graph with n vertices and valency $d > n/3$. Then G is 3-colourable.*

Proof. In a vertex-transitive graph, all similarity classes have the same size, but by Theorem 5.2.2, if G is not 3-colourable then there are two colour classes of different sizes. □

5.3 Cubelike Graphs

Let X be a maximal triangle-free cubelike graph on 2^n vertices with valency $2^n/3$. Since cubelike graphs are vertex-transitive, by Corollary 5.2.3, the graph X is 3-colourable. We have shown in Section 4 that X cannot have chromatic number three, and so X is bipartite.

Chapter 6

Codes and Cayley Graphs

We have shown that if a cubelike graph X is maximal triangle-free with valency greater than $|V(X)|/3$, then it is bipartite, but this is an easy consequence of a general graphical result. Since cubelike graphs arise from vector spaces, we can use information of codes and finite geometry to obtain a better bound.

In this chapter we will discuss the connections between codes, Cayley graphs, and projective geometry. We will first introduce linear q^k-colourings of a Cayley graph, and then describe the connections between binary caps and cubelike graphs, and after that we will discuss three geometric operations: doubling, deletion, and projection. All these operations have implications in Cayley graphs and codes.

6.1 Codes

The following discussions in the next two sections are based on Chris Godsil's colouring notes.

Let M be an $r \times n$ matrix over $\mathbb{Z}_q$, where q is a prime power. If the columns of M are non-zero and pairwise linearly independent, then M is called a *projective code.* The columns of M are the coordinate vectors of the points in the projective geometry $PG(r-1,q)$, with 1-dimensional subspaces as points, and 2-dimensional subspaces as lines. The row space of M determines a linear $[n,r]$-code C, and the kernel of M determines a linear $[n,n-r]$-code, denote $C^{\perp}$. Any codeword in C is of the form h^TM for some $h \in \mathbb{Z}_q^r$. The weight of this codeword is the number of non-zero entries in h^TM, which is determined by the number of columns of M that lies in the hyperplane $h^{\perp}$. We denote this hyperplane by $h^{\perp}$, since it is the kernel of the vector h^T.

Let $X(M)$ be a Cayley graph defined on the column space of M such that the vertices are the vectors in $\mathbb{Z}_q^r$, and two vectors v and w are adjacent if and only if their difference is a multiple of a column of M. This graph is undirected, and we can assume that the columns of M spans $\mathbb{Z}_q^r$, in which case X is connected. The vertices in the subspace whose coordinate vector is a column of M form a clique of size q, and the vertices in a coset of this subspace also form a clique of size q.

Let ϕ be a character of $\mathbb{Z}_q$. We showed in Section 3 that for any vector $a \in \mathbb{Z}_q^r$, the map

$$\phi_a(x) = \phi(a^Tx)$$

is also a character, and that the characters ϕ_a completely determine the eigenvalues of X. The eigenvalue associated with ϕ_0 is $(q-1)n$. When $a \in \mathbb{Z}_q^r \setminus 0$, the eigenvalue associated with ϕ_a is

$$q|a^{\perp} \cap S)| - |S| = q|a^{\perp} \cap S| - n,$$

where S be the set of points in $PG(r-1,q)$ corresponding to the columns of M, and $a^{\perp}$ denotes a hyperplane in $PG(r-1,n)$. The following lemma is true.

6.1.1 Lemma. *Let M be an $r \times n$ matrix. Then the least eigenvalue of the Cayley graph $X(M)$ is at least $-n$. The least eigenvalue is $-n$ if and only if the code of M has a codeword of weight n.* □

6.1.2 Theorem. *Let M be an $r \times n$ matrix, and let $X(M)$ be the Cayley graph defined on the column space of M. Then X is q-colourable if and only if there is a codeword of weight n in the code generated by M.*

Proof. If the code of M does not have a codeword of weight n then the least eigenvalue of X is greater than $-n$. We know that the valency of X is $n(q-1)$, and by the ratio bound, it follows that

$$\alpha(X) < \frac{|V(X)|}{1+\frac{n(q-1)}{n}} = \frac{|V(X)|}{q}.$$

and so $\chi(X) > q$.

On the other hand, let $h^T M$ be a codeword of weight n. For any two vertices v and w, if $h^T v = h^T w$ then $h^T(v-w) = 0$, and so $v-w$ is not the scalar multiple of a column of M. Thus the vector h determines a q-colouring of X. □

6.2 Linear q^k-Colourings

We will introduce and describe linear q^k-colourings of a Cayley graph.

Let S be a set of n points in $PG(r-1, q)$, where q is a prime power. The points in S can be represented by a set of non-zero vectors of length r over $\mathbb{Z}_q$, and no two vectors are scalar multiples of each other. Let $X(S)$ be a Cayley graph whose vertices are the vectors in $\mathbb{Z}_q^r$, and two vertices are adjacent if and only if their difference is a scalar multiple of a vector in S.

The set S is *affine* if there is a hyperplane that does not intersect S. Let M be an $r \times n$ matrix whose columns are the coordinate vectors of the points in S. We call M the matrix of S for convenience. If S is affine then there is a vector $h \in \mathbb{Z}_q^r$ such that $h^T M$ has weight n, and as we have showed in Section 6.1, the graph X is q-colourable. Hence we have the following lemma.

6.2.1 Lemma. *The following three statements are equivalent.*

(a) the set S is affine,

(b) the code of M has a codeword of weight n, and

(c) the graph $X(S)$ (or $X(M)$) is q-colourable.

□

Let $\mathbb{E}$ be an extension field of $\mathbb{Z}_q$ of order q^k. Since M is a matrix in $\mathbb{Z}_q$ it is also a matrix in $\mathbb{E}$. The projective geometry $PG(r-1, q^k)$ has more hyperplanes than $PG(r-1, q)$, and so if S is not affine in $PG(r-1, q)$ it may be affine in $PG(r-1, q^k)$ for some k. The smallest such k is called the *critical exponent.*

A hyperplane in $PG(r-1, q^k)$ is the kernel of a $k \times r$ matrix H. Hence if S is affine in $\mathbb{E}$, then each column of HM is non-zero. Let v and w be two vertices of X, if $Hv = Hw$ then $H(v - w) = \mathbf{0}$, and so $v - w$ is not a multiple of a column of M. Thus H determines a q^k-colouring of X. In general, the colouring of X determined by a $k \times r$ matrix over $\mathbb{Z}_q$ is called a *linear q^k colouring.*

If S is affine in $PG(r-1, q^k)$, then there exits hyperplanes $H_1, H_2, \ldots, H_k$ in $PG(r-1, q)$ such that

$$S \cap H_1 \cap H_2 \ldots \cap H_k = \emptyset.$$

In coding theory terms, S is affine over $\mathbb{E}$ if and only if there exists a set of k codewords such that the union of their supports has size n. Equivalently, the set S is affine over $\mathbb{E}$ if and only if the Cayley graph $X(S)$ is the union of k subgraphs, each of which has a linear q-colouring.

6.3 Caps, Codes, and Cubelike Graphs

We will describe the connections among caps, codes, and cubelike graphs.

A *cap* in $PG(r-1, q)$, where q is a prime power, is a set of points such that no three are collinear. A cap S is *complete* if and only if every point in

$PG(r-1,q)\setminus S$ lies in a secant of S. In other words, if a cap S is complete then it cannot be lengthened, in a sense that no point can be added to S. When $q=2$, a cap in $PG(r-1,2)$ is called a *binary cap.*

We will describe a connection between a coding theory parameter and complete caps.

Let C be a binary code of length n. The *covering radius* of C is the smallest integer r such that every binary vector of length n is within distance r from at least one codeword.

6.3.1 Theorem. *Let S be a binary cap in $PG(r-1,2)$ of size n, and let $C^{\perp}$ be its dual code. Then S is complete if and only if $C^{\perp}$ has covering radius two.*

Proof. Let M be the matrix of S. (Since S is a binary cap, each point has a unique coordinate vector.) If S is complete then every nonzero vector in $\mathbb{Z}_2^r$ is either a column of M or is the sum of two columns of M. Let x be a binary vector of length n that is not in $C^{\perp}$. Then either $Mx = m_i$ where m_i is a column of M, or $Mx = m_i + m_j$ where m_i, m_j are two columns of M. In the first case x is obtained from some codeword by flipping the bit in the i-th position, and in the second case x is obtained from some codeword by flipping the bits in both the i-th and the j-th positions.

If $C^{\perp}$ has covering radius two, then every vector x in Z_2^n is within distance two of some codeword c. If x is of distance one from c then Mx is a column of M, and if x is of distance two from c then Mx is the sum of two columns of M. □

Now we will describe the connections between caps and cubelike graphs. Let S be a binary cap in $PG(r-1,2)$ of size n, and let $X(S)$ be the cubelike graph with 2^r vertices and connection set S. Then $X(S)$ is triangle-free. To see this, suppose that X contains a triangle. Since X is vertex-transitive, we can assume that the three vertices in the triangle are $\mathbf{0}$, a, and b, where $a, b \in S$, but since ab is an edge $(a+b) \in S$. However S is a cap and so $(a+b) \notin S$.

If S is complete, then $X(S)$ is maximal triangle-free. Brandt proved that all maximal triangle-free vertex-transitive graphs with n vertices and valency greater than $n/3$ are 3-colourable (see Section 4). Naserasr and Tardif proved that a cubelike graph cannot have chromatic number three (see Section 5). These results imply that if the cubelike graph $X(S)$ (defined above) has valency greater than $2^r/3$ then it is bipartite. If we look at graph colouring from geometric point of view and study binary caps in $PG(r-1,2)$, we can characterize all maximal triangle-free cubelike graphs with 2^r vertices and valency greater than $2^r/4$, and show that the chromatic number of these graphs are either two or four (see Section 7).

6.4 Doubling Construction

Let S be a cap in $PG(r-1,2)$ of size n. We can extend S to a cap in $PG(r,2)$ of size $2n$ as follows. Embed $PG(r-1,2)$ into $PG(r,2)$, and let x be a point in $PG(r,2) \setminus S$. If we join x to a point $v \in S$, we obtain a third point on the line xv. The set of all third points on the lines xv, for all $v \in S$, together with the points in S, form a cap in $PG(r,2)$ of size $2n$. This process is called the *doubling construction.*

Let M be the matrix of a cap S in $PG(r-1,2)$, and let M' be the matrix of the cap in $PG(r,2)$ obtained by doubling S. Then M' is of the following form.

$$M' = \left(\begin{array}{c|c} 0\dots0 & 1\dots1 \\ \hline M & M \end{array}\right) \tag{6.1}$$

Let C be the code generated by M, and let C' be the code generated by M'. Then we call that C' is obtained by *doubling* the code C. It is easy to see that the distance of C' is four.

6.4.1 Lemma. *Let S be a binary cap in $PG(r-1,2)$. Suppose that S' is obtained by doubling S and C' is the code of S'. Then the minimum distance of C' is four.*

Proof. Let H be the matrix of S. Then the generator matrix M' of the code C' is of the form 6.1. The following four columns

$$\begin{pmatrix}0\\x\end{pmatrix},\ \begin{pmatrix}0\\y\end{pmatrix},\ \begin{pmatrix}1\\x\end{pmatrix},\ \begin{pmatrix}1\\y\end{pmatrix}$$

where x, y are columns of M, are linearly dependent. It is easy to verify that any three columns of M' are linearly independent, since S is a cap. □

We will introduce an equivalent concept. Let S be a binary cap in $PG(r-1,2)$ of size n, and let x be a point in $PG(r-1,2)\setminus S$. We call S *periodic* with respect to x if x lies in no tangent of S. In other words, for every point $v \in S$, the line xv is a secant of S.

6.4.2 Theorem. *Let S be a cap in $PG(r-1,2)$. Then S is obtained by doubling if and only if the set S is periodic.*

Proof. If S is obtained by doubling, then S is periodic by definition. Suppose that S is periodic with respect to x. Let H be a hyperplane such that $x \notin H$. Then S is obtained by doubling the cap $H \cap S$. To see this, consider any point $v \in H \cap S$. The third point on the line vx is in S but is not in H. □

This definition of periodic set agrees with the definition of periodic sets for abelian groups introduced by Kemperman [8], since every binary cap in $PG(r-1,2)$ can be viewed as a subset of an abelian group Z_2^r. The following proposition is important (Kemperman [8]).

6.4.3 Proposition. *Let F and E be subsets of the additive abelian group G and*

$$F + E = \{f + e : f \in F,\ e \in E\}.$$

If $|F+E| \leq |F| + |E| - 2$, then the set $F+E$ is a periodic subset. □

The following three lemmas are due to Davydov and Tombak [6]. In their paper the matrix H is the check matrix of some $[n, n-r, 4]$ code of covering radius two. However, the restriction on the distance ($d = 4$) does not play an role in the proof. Here we restate the lemmas in geometric language and prove them geometrically, so the notion of distance does not apply.

6.4.4 Lemma. *Let S be a complete cap in $PG(r-1,2)$. Let H be a hyperplane of $PG(r-1,2)$. If $H \cap S$ is periodic with respect to a point $x \in H \backslash S$, then S is periodic with respect to x.*

Proof. Suppose, for contradiction, that S is not periodic with respect to x. Then there exists a point $b_1 \in S \setminus H$ such that $x + b_1 \notin S$. This point $x + b_1$ does not lie in H, since $b_1 \notin H$. Since S is complete, it follows that $x + b_1 = a_1 + b_2$, where $a_1, b_2 \in S$. Note that if both a_1 and b_2 lies in $S \cap H$ then $a_1 + b_2$ lies in H, but it is not the case. Moreover, if a_1, b_2 lies in $S \backslash H$, then $a_1 + b_2$ lies in H, since H is a hyperplane that intersects every line. Thus we can assume that $a_1 \in S \cap H$ and $b_2 \in S \setminus H$.

Consider the plane $xb_1 \vee xb_2$. The lines xa_1 and b_1b_2 intersect in a point z. Since $S \cap H$ is periodic with respect to x, the point z lies in S. However, $b_1 + b_2$ does not lie in S, since S is a cap in $PG(r-1,2)$, a contradiction. □

6.4.5 Lemma. *Let S be a subset of $AG(r-1,2)$. If S is a cap constructed by doubling, then $AG(r-1,2) \setminus S$ is also a cap constructed by doubling.*

Proof. Since S is constructed by doubling, there is a vertex x such that the third point of every line xv, where $v \in S$, is also in S. It is easy to show that the third point of every line xw, where $w \in AG(r-1,2) \setminus S$, is also in $AG(r-1,2) \setminus S$. □

The following lemma is very important.

6.4.6 Lemma. *Let S be a complete cap in $PG(r-1,2)$ of size at least $2^{r-2}+2$. If there is a subspace of codimension two skew to S, then S is periodic, and equivalently, it is constructed by doubling.*

Proof. Suppose that H_2 be a subspace of codimension two skew to S. Let A, B, C be the three hyperplanes on H_2, and let S_A, S_B, S_C denote the points of S in A, B, C, respectively. Thus

$$|S_A| + |S_B| + |S_C| = |S| \geq 2^{r-2} + 2. \tag{6.2}$$

Consider any two points $x \in S_B$ and $y \in S_C$, then the point $x + y$ lies in $A \backslash H_2$ and $x + y \notin S$. Let $\bar{S_A}$ be the set of points in $A \backslash H_2$ but not in S. Since S is complete, it follows that $S_B + S_C = \bar{S_A}$. Thus

$$|S_B + S_C| = |\bar{S_A}| = 2^{r-2} - |S_A|. \tag{6.3}$$

Combing Equations 6.2 and 6.3 we obtain

$$|S_B + S_C| \leq |S_B| + |S_C| - 2,$$

and so the set $\bar{S_A} = S_B + S_C$ is periodic. By Lemma 6.4.5, the set S_A is also periodic, and by Lemma 6.4.4, the set S is periodic. Equivalently, the cap S is constructed by doubling. □

6.5 Doubling a Graph

Let S be a cap in $PG(r-1, 2)$ and let $X(S)$ be the cubelike graph defined on S. Let S' be the cap in $PG(r, 2)$ obtained by doubling S. Then the cubelike graph $Y(S')$ is isomorphic to $X[\bar{K_2}]$, the lexicographic product of X with $\bar{K_2}$. The vertices of Y are of the form (v, i) where $i \in \{1, 2\}$ and v is a vertex of X. Two vertices (v, i) and (w, j) are adjacent if v is adjacent to w in X. The set $\{(v, 1) \ : \ v \in X\}$ induces a copy of S.

Let A be the adjacency matrix of X. Then the adjacency matrix of Y is of the following form,

$$\begin{pmatrix} A & A \\ A & A \end{pmatrix}$$

6.5.1 Theorem. *Let S be a binary cap in $PG(r-1, 2)$ and let $X(S)$ be the cubelike graph defined on S. Let S' be the cap in $PG(r, 2)$ obtained by doubling S and let $Y(S')$ be the cubelike graph defined on S'. Then $\chi(X) = \chi(Y)$.*

Proof. Since X is a subgraph of Y, it follows that $\chi(X) \leq \chi(Y)$. Suppose that we have a colouring of X. For each vertex (v, i) in Y, where $i \in \{1, 2\}$, we assign the same colour of v in X. It is easy to verify that no adjacent vertices get the same colour. □

In general, $\chi(G[\bar{K_2}]) = \chi(G)$ for any graph G.

6.6 Deletion and Projection

There are three geometric operations: doubling, deletion, and projection. We have already described doubling. Here we will describe deletion and projection.

Let S be a cap of $PG(r-1,q)$, and let $X(S)$ be the Cayley graph defined on the points in S. Let M be the matrix of S and let C be the code generated by M.

Deleting a point from S corresponds to deleting a column x from M. In coding theory terms, this operation is called *puncturing* the code C. In terms of the Cayley graph $X(S)$, this operation corresponds to deleting all generators from the connection set that are the scalar multiplies of the column x.

Projection is described as follows: Suppose that $T \subset S$ and let K be the projective span of T. Assume that $\dim(K) = k$ and let H be a subspace with codimension k. If $x \in S \setminus K$, then $x \vee K$ spans a space of dimension $k+1$, and this space intersects H in a unique point. The map

$$\phi : x \mapsto (x \vee K) \cap H$$

is called the *projection* of S from T.

In the language of matroid theory, projection corresponds to contraction. Here we require that the subset T be a *flat*, that is,

$$span(T) \cap S = T \cap S.$$

We will only consider projections from a point in S, which is a flat of dimension 0. Let x be the coordinate vector of this point, and let H be a hyperplane not on x, denote $h^{\perp}$. Let v be the coordinate vector of a point in $S \setminus \{x\}$. Then the line $x \vee v$ meets H in a unique point. We can take the coordinate vector of this point to be $v - \lambda x$, and so

$$h^T(v - \lambda x) = 0.$$

It is easy to compute that

$$\lambda = \frac{h^T v}{h^T x}.$$

We can assume, without loss of generality, that $x = [10\ldots0]^T$, and the hyperplane H is the kernel of the vector $[10\ldots0]$. Then each point $v \in S \setminus x$ is mapped to $v - [v_1 0 \ldots 0]^T$ where v_1 is the first coordinate of v.

In the language of coding theory, projection corresponds to *shortening*. This process is described as follows. We first find a generator matrix of C that has a column $[10\ldots0]^T$. Then delete that column and the first row, leaving a generator matrix for a linear $[n-1, k-1]$-code C'. We say that the code C' is obtained by shortening the code C.

We can also describe projection in terms of the Cayley graph $X(S)$ (same as $X(M)$). The vertices in the point x (1-dimensional subspace) form a clique of size q. The cosets of this point also form cliques of size q. Projection from x corresponds to contracting all the edges in each clique, i.e, shrinking each clique to one vertex. The resulting graph is called the *coset graph* of $X(M)$ with respect to a generator x. If the matrix M is the adjacency matrix of a smaller graph Y, then projection corresponds to deleting one vertex from Y.

6.7 Summary

The following table summarizes the connection among a set of points S in $PG(r-1, q)$, the Cayley graph $X(S)$, and the code C (or the dual code $C^{\perp}$) of S.

S	$X(S)$	C or $C^{\perp}$
There is a subspace of codimension k skew to S	linear q^k-colouring	C contains a codeword of weight n in a field of order q^k
S is a complete binary cap	$X(S)$ is a maximal triangle-free cubelike graph	$C^{\perp}$ has distance at least four and covering radius two.
doubling	lexicographic product	doubling C
deletion	deleting a generator	puncturing C
projection	coset graph	shortening C

Chapter 7

Caps

Recall that a cap in $PG(r-1,q)$, where q is a prime power, is a set of points that does not contain a line. As we have noted before, complete binary caps give rise to maximal triangle-free cubelike graphs. In this chapter, we will prove that all complete large caps are either affine or skew to a subspace of codimension two, which implies that the corresponding cubelike graphs are either bipartite or have chromatic number four. A cap in $PG(r-1,2)$ is *large* if its size is at least $2^{r-1}+1$.

7.1 Overview

Let S be a binary cap in $PG(r-1,2)$ of size n. Then by the definition of caps, every line intersects $\bar{S}$, the complement of S. If $\bar{S}$ is a hyperplane then S is isomorphic to the affine geometry $AG(r-1,2)$ and the size of S is 2^{r-1}. The following result is not difficult to prove.

7.1.1 Theorem. *Let S be a complete cap in $PG(r-1,2)$. Then $|S| \leq 2^{r-1}$. Moreover, $|S| = 2^{r-1}$ if and only if S is isomorphic to the affine geometry $AG(r-1,2)$.*

Proof. Let x be a point in $PG(r-1,2)\backslash S$. There are $2^{r-1}-1$ lines through x. These lines partition the points in $PG(r-1,2)\backslash x$ into $2^{r-1}-1$ pairs. If S is a cap of maximum size, it must contain two points from one line through

x, and one point from all the other lines through x. This accounts for 2^{r-1} points.

We will show that the structure described above is isomorphic to $AG(r-1,2)$. We only need to show that $\bar{S}$ is a subspace. Let v, w be any two points in $PG(r-1,2)\setminus S$. We can assume, without loss of generality that $v, w \neq x$. Then $v+w=(v+x)+(w+x)$. Since $v,w,x \notin S$, it follows that $(v+x),(w+x) \in S$ and hence $(v+x)+(w+x) \notin S$, since S is a cap. Therefore, $\bar{S}$ is a hyperplane of size $2^{r-1}-1$, and S is isomorphic to $AG(r-1,2)$. □

Recall that S is affine if there exists a hyperplane skew to it. We have showed in Section 6 that S is affine if and only if the code of S contains a codeword of weight n, and if and only if the Cayley graph $X(S)$ has a linear q-colouring. All binary affine caps are subsets of $AG(r-1,2)$, and so they are not very interesting. The interesting case is when S is not affine.

Segre [13] derived an upper bound on the size of caps that are not affine. Here we will present his proof. We will first state the following lemma, whose proof includes lengthy calculations and requires non-trivial knowledge in algebraic geometry.

7.1.2 Lemma. *Suppose that we are given a cap S and a point $o \notin S$. Let t be the number of tangents on a point in S. If there exists at least one secant through o, then the number of tangents through o is at most t.* □

Now we are ready to derive the bound on the size of non-affine caps.

7.1.3 Theorem. *Let S be a complete cap in $PG(r-1,q)$, where q is a prime power and $r \geq 2$. If S is not affine then*

$$|S| \leq \frac{|PG(r-1,q)|}{q+1}.$$

Proof. We will first show that the number of tangents through any point on S is the same. Let x be a point on S. Consider a hyperplane H not on x. Then every line through x intersects H. Any line through x is either a secant of S, or a tangent of S. There are $|S|-1$ secants, and so the number of tangents is $t = |H| - (|S| - 1)$.

Let o be a point not on S. By Lemma 7.1.2, it follows that the number of tangents through o, denote $t(o)$, is at most t. Let l be a tangent to S. Then counting the pairs $\{o,\ l\}$,

$$|S|tq = \sum_{o \notin S} t(o) \leq t(|PG(r-1,q)| - |S|).$$

(To obtain the left hand side, we consider that each point of S has t tangents on it, and each tangent contains q external points of S.) Thus we obtain the bound. □

Applying this bound to binary caps in $PG(r-1,2)$, we get that if a cap is not affine, then its size is at most $\frac{2^r-1}{3}$.

This bound implies that any cubelike graph on 2^n vertices with valency greater than $2^n/3$ is bipartite. This result agrees with the result of Brandt (see Section 5).

The bound of Theorem 7.1.3 is best possible in the case when r is four.

The results of Davydov and Tombak [6] on codes implies that all complete caps of size at least $2^{r-2}+2$ are skew to a subspace of codimension two, and thus are constructed by doubling. The size of complete large caps in $PG(r-1,2)$ are $2^{r-2}+2^{r-2-g}$, where $g = 0, 2, 3, \ldots, r-2$. Their proof is very complicated with a lot of lengthy calculations. In this chapter we will explain the ideas in a simpler way.

Bruen and Wehlau [5] strengthened the results of Davydov and Tombak by adding that all complete caps of size exactly $2^{r-2}+1$ are also skew to a subspace of codimension two.

Later, Bruen, Haddad, and Wehlau [4] published another paper describing a connection between linear binary codes and complete caps of size n in $PG(r-1,2)$, and gave a geometric proof that, if $n = 2^{r-2}+2^{r-3}$, then the geometric structure of the cap is unique.

In Section 7.2 we will describe the intersection properties of caps in $PG(r-1, q)$, then we will focus on binary caps. We will first characterize all complete large caps in $PG(4, 2)$, then we will prove that for any fixed k and sufficiently large r we can find a binary cap in $PG(r-1, 2)$ that is a k-block, after that we will sketch the proofs of Davydov and Tombak [6], and Bruen and Wehlau [5], showing that all large caps are skew to a subspace of codimension two. The proofs will be explained in a simpler way.

7.2 Caps in $PG(3, q)$

We will show that the complete cap in $PG(3, 2)$ of size five is unique. We will also describe the incidence structure of a cap of size $q^2 + 1$ and the hyperplanes in $PG(3, q)$.

7.2.1 Theorem. *Let S be a complete cap in $PG(3, 2)$ that is not affine. If $|S| = 5$ then S is unique.*

Proof. First of all, no hyperplane in $PG(3, 2)$ contains more than three points of S. To see this, let H be a hyperplane (the Fano plane, in this case) that contains four points of S. Then there is a line L in H that contains no points of S. Consider the two other hyperplanes of $PG(3, 2)$ on L. One of them must contain no point of S. Thus S is affine, a contradiction.

Since every hyperplane in $PG(3, 2)$ contains at most three points (and at least one point) of S, every subset of four points in S is linearly independent. Since $PGL(3, 2)$ acts transitively on sets of four linearly independent vectors, we can assume, without loss of generality, that S contains the coordinate vectors,

$$v_1 = 1000,\ v_2 = 0100,\ v_3 = 0010,\ v_4 = 0001.$$

Since no four points of S are coplanar, the last vector of S is 1111. Hence,

$$S = \{1000,\ 0100,\ 0010,\ 0001,\ 1111\}$$

is unique. □

In fact, this complete non-affine cap S is the set of points in an ovoid of $PG(3,2)$. Of the 15 planes in $PG(3,2)$, exactly 10 meet the ovoid in three points and 5 are tangent to it.

7.2.2 Theorem. *Let S be a cap in $PG(3,q)$ where q is a prime power. Suppose that $|S| = q^2+1$. Then every hyperplane meets S in either one point or $q+1$ points.*

Proof. Let a, b be two distinct points in S. There are $q+1$ hyperplanes on the line ab. (The number $q+1$ is obtained by considering the dual space.) These $q+1$ hyperplanes partition the set $S \setminus \{a,b\}$ into $q+1$ classes. On average, each class contains

$$\frac{q^2-1}{q+1} = q-1$$

points of $S \setminus \{a,b\}$.

On the other hand, let H be a hyperplane (plane, in this case) in $PG(3,q)$ on the line ab. Then $S \cap H$ is also a cap. If $S \cap H$ is complete, then it is the points of a smooth conic which contains $q+1$ points. This conic is not singular because S is a cap. So

$$|S \cap H| \leq q+1.$$

Therefore each hyperplane on ab contains exactly $q+1$ points.

The number of hyperplanes that intersect S in $q+1$ points is

$$\frac{(q+1)\binom{q^2+1}{2}}{\binom{q+1}{2}} = \frac{(q+1)(q^2+1)q^2}{(q+1)q} = q(q^2+1).$$

The number of tangent hyperplanes is (q^2+1).

Thus the number of hyperplanes that meet S in either one point or $q+1$ points is

$$q(q^2+1)+(q^2+1) = \frac{q^4-1}{q-1},$$

which is the total number of hyperplanes in $PG(3,q)$. □

For a complete characterization of conics, see Beutelspacher and Rosenbaum [1].

7.3 Complete Caps in $PG(4,2)$

Let S be a complete cap in $PG(4,2)$ of size at least 9. If S is affine then it is isomorphic to $AG(4,2)$. If it is not affine then either $|S| = 9$ or $|S| = 10$, by Theorem 7.1.3 (where the bound is computed with $r = 5$). We treat these two cases separately.

We first describe a construction of a complete cap in $PG(4,2)$ of size 9. Let H_2 be a subspace of codimension two, and let A, H, B be the three hyperplanes on H_2. Let a be a point in A, and let

$$S_A = \{a\}.$$

Let h be a point in $H \setminus H_2$ and define the set

$$S_H = H \setminus (H_2 \cup \{h\})$$

Then the point $b = a + h$ lies in $B \setminus H_2$. Let

$$S_B = \{b\}.$$

Define $S = S_A \cup S_H \cup S_B$.

Then S is a complete cap in $PG(4,2)$ of size 9. We will show that the structure described above is unique.

We will need the following lemma first (see Davydov and Tombak [6], Lemma 10).

7.3.1 Lemma. *Let S be a complete cap in $PG(r-1,2)$ of size exactly $2^{r-2}+1$, where $r \geq 5$. Let H be a hyperplane such that $|H \cap S|$ is maximal. Then $|S \setminus H| \leq 2^{r-3} - 1$.* □

7.3.2 Theorem. *Let S be a complete cap in $PG(4,2)$ that is not affine. If $|S| = 9$ then it is unique and is of the structure described above.*

Proof. Let H be a hyperplane in $PG(4,2)$ such that $|S \cap H|$ is maximal. Since $S \cap H$ is a cap in H, it follows that $|S \cap H| \leq 8$. By Lemma 7.3.1, it follows that $|S \setminus H| \leq 3$, and so $|S \cap H| \geq 6$. Put together, we have

$$6 \leq |S \cap H| \leq 8.$$

By Theorem 7.1.3, if a cap in $PG(3,2)$ is not affine, then its size is at most five. Thus, the small cap $S \cap H$ is affine, and so S is skew to a hyperplane of H, denote H_2. Clearly H_2 is a subspace of codimension two in $PG(4,2)$.

Let A, B be the two other hyperplanes on H_2. If $S \cap H$ is complete, then $|S \cap H| = 8$. Since $|S| = 9$, one of A, B contains no point of S, and so S is affine. Thus we can assume that $S \cap H$ is obtained from $H \setminus H_2$ by deleting one or two points. We will show that only one point is deleted.

Suppose, for contradiction, that $H \cap S$ is obtained from $H \setminus H_2$ by deleting two points x, y. Since S is complete, the point x lies on a secant of S, say $x = a + b$. But x cannot lie on any secant of $S \cap H$, since $x \notin H_2$. Thus, we can assume that $a \in A$ and $b \in B$. The set

$$(H \cap S) \cup \{a, b\}$$

contains 8 points. The point y also lies on some secant of S. Since $y \notin H_2$, this secant does not lie in $S \cap H$. Since S contains 9 points we can assume that y lies on the secant ba' where $a' \in A$. It follows that

$$S = (H \cap S) \cup \{a, b, a'\}.$$

However, the point $b' = a' + x = a + y$ does not lie on any secant of S. To see this, note that b' does not lie on any secant of $S \cap H$, since $b' \notin H_2$. It is also easy to check that b' does not lie on any secant of S with one end in $S \setminus H$. A contradiction.

Therefore, the set $S \cap H$ is obtained from $H \setminus H_2$ by deleting one point, and the hyperplanes A, B are tangent hyperplanes. The structure of S is unique. $\square$

Let M be the matrix of the complete non-affine cap in $PG(4,2)$ of size 9, then M is of the following form,

$$M = \left(\begin{array}{c|c|c} 0 \ldots 0 & 1 & 1 \\ \hline X \setminus \{x\} & 0 & x \end{array} \right)$$

where the matrix X is the check matrix of the extended Hamming code with length 8 and 4 check symbols, and x is a column of X. The check matrix of the extended Hamming code with length n and r check symbols, denote $X(n,r)$, can be constructed as follows. The first row is an all-ones row. The columns of the submatrix of $X(n,r)$ obtained by deleting the first row are the vectors in $\mathbb{Z}_2^{r-1}$.

By elementary row operations, we write the matrix M as follows,

$$\left(\begin{array}{cc} 00000 & 1111 \\ \hline 10001 & 0000 \\ 01001 & 1001 \\ 00101 & 0101 \\ 00011 & 0011 \end{array}\right)$$

(We write M this way just for convenience, since it will be used in the main proof later.)

Next we will consider complete caps in $PG(4,2)$ of size 10. We will show that if they are not affine then they are constructed by doubling.

We need the following lemma first.

7.3.3 Lemma. *Let S be a cap in $PG(r-1,2)$ that is not affine. If $r \geq 4$, then there exists a hyperplane that contains more than half of the points of S.*

Proof. Consider the incidence structure of hyperplanes and pairs in S. Suppose, for contradiction, that each hyperplane contains at most $|S|/2$ points of S. Then it contains at most

$$\binom{\frac{|S|}{2}}{2}$$

pairs of S. Since there are $2^r - 1$ hyperplanes, the total number of pairs of S that are contained in the hyperplanes is at most

$$(2^r - 1)\binom{\frac{|S|}{2}}{2}. \tag{7.1}$$

On the other hand, each pair of $|S|$ is contained in exactly $2^{r-2}-1$ hyperplanes. Hence the total number of pairs of S that are contained in the hyperplanes is exactly

$$(2^{r-2}-1)\binom{|S|}{2} \tag{7.2}$$

By Theorem 7.1.3, the size of S is at most $\frac{2^r-1}{3}$ for $r \geq 4$. It can be verified that the bound in (7.1) is strictly less than the bound in (7.2). A contradiction □

7.3.4 Theorem. *Let S be a complete cap in $PG(4,2)$ that is not affine. If $|S| = 10$ then it is constructed by doubling.*

Proof. Let H be a hyperplane in $PG(4,2)$ such that $|S \cap H|$ is maximal. By Lemma 7.3.3, it follows that $|S \cap H| \geq 6$. We know that if a cap in $PG(3,2)$ is not affine then its size is at most five, and so $S \cap H$ is affine in H. In other words, there is a subspace in $PG(4,2)$ of codimension two skew to S. By Lemma 6.4.6, the cap S is constructed by doubling. □

7.4 k-Blocks

Tutte [14] defined a *k-block* over $GF(q)$ to be a subset S such that,

(a) the dimension of any space that contains S is at least k,

(b) every subspace of dimension k contains at least one point of S.

We present a version of Brouwer, Bruen, and Wehlau's [3] proof that there exist caps that block all subspaces of fixed codimension.

7.4.1 Theorem. *For any $k \geq 0$ and sufficiently large r there exists a cap in $PG(r-1,2)$ that is a k-block.*

Proof. Let X be a graph with r vertices, and let A be the incidence matrix of X. It is easy to see that X is triangle-free if and only if no three columns of A are linearly dependent over $\mathbb{Z}_2$. If X is triangle-free, we can view A as a matrix whose columns are the coordinate vectors of a binary cap S in $PG(r-1,2)$. As we have showed before, if S is not a k-block, then X has a linear 2^k-colouring. It is well-known (due to Erdös) that there exists a triangle-free graph with arbitrarily large chromatic number (there is a proof in Tutte's book "Connectivity in Graphs"). Thus for some r (the number of vertices of X), if the chromatic number of X is larger than 2^k, then the incidence matrix A gives us a cap in $PG(r-1,2)$ that is a k-block. □

7.5 Large Caps

Recall that a cap in $PG(r-1,2)$ is large if its size is at least $2^{r-2}+1$. We will prove that if $r \geq 4$ then all large complete caps are either affine or skew to a subspace of codimension two. We will switch back and forth between coding theory and geometry.

The following lemma is proved by McWilliams and Sloane [10].

7.5.1 Lemma. *Suppose that the cap matrix M is represented in the following form*

$$M = \left(\begin{array}{c|c} 0\ldots0 & \overbrace{1\ldots1}^{w} \\ \hline A & B \end{array}\right)$$

where w is the smallest weight of a codeword in the code generated by M. Let w_A be the smallest weight of a codeword in the code generated by the matrix A. Then we have $2w_A \geq w$.

Proof. Let C be the code generated by the matrix M. Suppose that $[u|v] \in C$ where $wt(u) = w_A$. Since $[u|\bar{v}] \in C$, we have

$$w_A + wt(v) \geq w,$$
$$w_A + w - wt(v) \geq w,$$

and, by adding the two equations, we get $2w_A \geq w$. □

The following lemma is crucial in the proof of the main theorem that all large caps are skew to a subspace of codimension two. We will sketch a proof of this lemma by Davydov and Tombak. Some lengthy calculations will be omitted.

7.5.2 Lemma. *Let S be a complete cap in $PG(r-1,2)$ of size at least $2^{r-2}+2$, and let H be a hyperplane such that $|H \cap S|$ is maximal. Suppose that $S \cap H$ is contained in a complete cap C in H, and suppose that C is obtained by an $(r-5)$-fold doubling of the unique cap of size five in $PG(3,2)$ (the ovoid). Then S is skew to a subspace of codimension two in $PG(r-1,2)$.*

Proof. Let M be the matrix of the complete cap S in $PG(r-1,2)$ of size n, where $n \geq 2^{r-2}+2$. Suppose that

$$n = 2^{r-2} + \beta,$$

where $\beta \geq 2$. We can represent M in the following forms

$$M = \left(\begin{array}{c|c} \overbrace{0\ldots0}^{n_0} & \overbrace{1\ldots1}^{w} \\ \hline A & B \end{array}\right) = \left(\begin{array}{c} \overbrace{0\ldots01\ldots1}^{n} \\ \hline M_1 \\ \hline M_0 \end{array}\right) = \left(\begin{array}{c|c} 0\ldots0 & 1\ldots1 \\ \hline A_1 & B_1 \\ \hline A_0 & B_0 \end{array}\right)$$

where w is the minimum weight of a codeword in the row space of M. Suppose that the hyperplane H is the kernel of the vector $[10\ldots0]$. Let $|S \cap H| = n_0$. Then the matrix A is an $(r-1) \times n_0$ matrix, and the matrix B is an $(r-1) \times w$ matrix.

(a) We will show that the row space of M contains a pair of codewords in which zeros do not occur in identical positions. (This statement is equivalent to that there exists a subspace of codimension two skew to S.) Let M_0 be the submatrix of M formed by its bottom four rows. We will show that the pair of codewords satisfying the property is contained in the row space of M_0. The existence of such a pair depends on the type of the columns of M_0, but not on the number of columns of each type. Let A_0 be the submatrix of A formed by it bottom four rows, and let B_0 be the submatrix of B formed by its bottom four rows. Then $M_0 = [A_0|B_0]$. Since $S \cap H$ is contained in a complete cap in H that is obtained by doubling the ovoid in $PG(3,2)$, and since the points in the ovoid are

$$(1000)^T,\ (0100)^T,\ (0010)^T,\ (0001)T,\ (1111)^T,$$

it follows that the matrix A_0 contains only the columns of the above types (four vectors of weight one, and one vector of weight four). If B_0 contains only these columns, then there exists a pair of codewords satisfying the property. Now suppose that B_0 contains m_i varieties of columns of weight i, where $i = 0, 2, 3$. It can be verified that if $m_2 + m_3 \leq 2$ and $m_0 = 0$, there exists a pair of codewords in which no zeros occur in identical positions. For example, if $m_2 = 2$ and the columns of B_2 are of type $(1100)^T$ and $(0011)^T$, then there exists a pair of codewords in which no zeros occur in identical positions.

Thus, to prove the lemma, it suffices to show that

$$m_2 + m_3 \leq 2,\ m_0 = 0.$$

(b) The columns of the submatrix A are the coordinate vectors of the points in $S \cap H$, which is contained in a complete cap C in H. Let M_C be the matrix of C. Since we are given that C is obtained by successively doubling of the ovoid in $PG(3,2)$, and so the matrix M_C is of the following form,

$$M_C = \left(\begin{array}{c|c|c|c|c} E & E & E & E & E \\ \hline 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 1\ldots1 \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 \end{array}\right)$$

where the columns of E form the set of all vectors in $\mathbb{Z}_2^{r-5}$.

Since $H \cap S$ is contained in C, we can assume that the matrix A is of the following form,

$$A = \left(\begin{array}{c|c|c|c|c} W_1 & W_2 & W_3 & W_4 & W_5 \\ \hline 1\dots1 & 0\dots0 & 0\dots0 & 0\dots0 & 1\dots1 \\ 0\dots0 & 1\dots1 & 0\dots0 & 0\dots0 & 1\dots1 \\ 0\dots0 & 0\dots0 & 1\dots1 & 0\dots0 & 1\dots1 \\ 0\dots0 & 0\dots0 & 0\dots0 & 1\dots1 & 1\dots1 \end{array}\right)$$

where the columns of W_i form a set of $2^{r-5} - \Delta_i$ distinct vectors in $\mathbb{Z}_2^{r-5}$, for $1 \leq i \leq 5$.

Let $n_0 = 5 \cdot 2^{r-5} - \Delta$, and so

$$\sum_{1 \leq i \leq 5} \Delta_i = \Delta.$$

Recall that A_0 is the submatrix of A formed by its bottom four rows. Then A_0 contains a codeword of weight

$$2 \cdot 2^{r-5} - \max\{\Delta_i + \Delta_j\},$$

where the maximum is over pairs of indices. (This is true because the sum of any two rows of A_0 is in the row space of A_0.)

Let w_A be the minimum weight of a codeword in the row space of A. Then

$$w_A \leq 2 \cdot 2^{r-5} - \max\{\Delta_i + \Delta_j\} \leq 2^{r-4} - 2\Delta/5.$$

By Lemma 7.5.1, it follows that

$$n - (5 \cdot 2^{r-5} - \Delta) = w \leq 2w_A \leq 2^{r-3} - 4\Delta/5.$$

Substituting $n = 2^{r-2} + \beta$ we get

$$\Delta \leq \frac{5(2^{r-5} - \beta)}{9}. \tag{7.3}$$

Let Ψ be the set of points in $PG(r-1, 2) \setminus H$ but not in S. Since $|S \setminus H| = w$, it follows that

$$|\Psi| = 2^{r-1} - w.$$

Substituting $w = n - (5 \cdot 2^{r-5} - \Delta)$ and $n = 2^{r-2} + \beta$ we get

$$|\Psi| = 13 \cdot 2^{r-5} - \Delta - \beta. \tag{7.4}$$

We will show that if the property

$$m_2 + m_3 \leq 2, \;\; m_0 = 0$$

does not hold, then Equation (7.4) is violated.

(c) Since $d = 3 \cdot 2^{r-5} + \beta + \Delta \geq 3 \cdot 2^{r-5} + 2$, there exists at least i columns of B such that the top $k - 5$ entries are identical, where $i \geq 4$. By adding the top row of M we can assume that M contains the following submatrix

$$G = \left(\begin{array}{c|c} 00000 & \overbrace{1111}^{i\geq 4} \\ \hline 00000 & 0000 \\ \cdots & \cdots \\ 00000 & 0000 \\ \hline 10001 & \\ 01001 & K \\ 00101 & \\ 00011 & \end{array}\right)$$

Consider the submatrix of G formed by its top row and bottom four rows, denote G_0. Here G_0 is the check matrix of some $[n, n-5, 4]$-code C_0, where $n \geq 9$. This code C_0 cannot be the extended Hamming code, since the all-ones vector is not in the row space of G_0. By Theorem 7.1.3 (where the bound is computed with $r = 5$), it follows that $n = 9, 10$. Following the discussion in Section 7.3, the code C_0 is either the unique $[9, 9-5, 4]$-code of covering radius two, or the $[10, 10-5, 4]$-code of covering radius two, or obtained from the $[10, 10-5, 4]$-code by deleting one column from its check matrix. We have characterized the first two cases in Section 7.3. In the third case, we can show that all the codes obtained by deleting one column from the check matrix are equivalent up to row operations.

Thus, there are three choices for the submatrix K.

$$K_1 = \begin{pmatrix} 0000 \\ 1001 \\ 0101 \\ 0011 \end{pmatrix}, \ K_2 = \begin{pmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{pmatrix}, \ K_3 = \begin{pmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix}$$

(d) As a sketch of the proof, we will only discuss the first case. Similar idea can be applied to the other two cases.

In the first case, where $K = K_1$, the matrix M contains the following submatrix

$$N = \left(\begin{array}{c|c|c|c|c|c|c} 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1111 & \overbrace{1\ldots1}^{v} \\ \hline W_1 & W_2 & W_3 & W_4 & W_5 & 0000 & t_1\ldots t_v \\ \hline 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 0000 & \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1001 & f_1\ldots f_v \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 & 0101 & \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 & 0011 & \end{array} \right)$$

$$= \left(\begin{array}{c|c|c|c|c|c|c} & & & & & 1111 & 1\ldots1 \\ & & & & & 0000 & t_1\ldots t_v \\ A_1 & A_2 & A_3 & A_4 & A_5 & 0000 & \\ & & & & & 1001 & f_1\ldots f_v \\ & & & & & 0101 & \\ & & & & & 0011 & \end{array} \right)$$

Let Ψ_i denote the set of points in $PG(r-1,2) \setminus H$ but not in S, where the top coordinate of is one and the bottom four coordinates constitute the binary representation of the number i. Clearly,

$$|\Psi| = \sum_{i=0}^{15} |\Psi_i|.$$

Let A_i be the submatrix of M that corresponds to W_i. Define

$$A_i + x = \{a + x \ : \ a \in A_i\}.$$

Note that the bottom four coordinates of the vectors in $A_i + x$ are the same. If these four coordinates represent the number j, we obtain

$$A_i + x \subseteq \Psi_j,$$

and so

$$|A_i| \leq |\Psi_j|.$$

(e) Suppose, for a contradiction, that the condition

$$m_2 + m_3 \leq 2, \ m_0 = 0$$

is not satisfied. Here we will only consider one case (all the other cases are proved similarly). Suppose that $m_0 = 0$ is violated.

In the matrix N, we can assume that $v = 1$ and $f_1 = \mathbf{0}$. Consider the sets

$$A_i + x,$$

where

$$x \in \{0100^T, \ 0010^T, \ 0001^T, \ 0111^T, \ 0000^T\}.$$

The following table lists the numbers whose binary representations correspond to the bottom four coordinates of the vectors in $A_i + x$.

$A_1 + x$	$A_2 + x$	$A_3 + x$	$A_4 + x$	$A_5 + x$
$8, 9, 10, 12, 15$	$0, 3, 4, 5, 6$	$0, 2, 3, 5, 6$	$0, 1, 3, 5, 6$	$8, 11, 13, 14, 15$

If the number k appears in both column $A_i + x$ and column $A_j + x$ in the above table, then we can use either one of the following two inequalities

$$|A_i| \leq \Psi_k, \ |A_j| \leq \Psi_k.$$

Hence we have the following inequalities,

$$\begin{aligned}
|A_1| &\leq \Psi_i,\ i = 8, 9, 10, 12\\
|A_2| &\leq \Psi_i,\ i = 0, 4\\
|A_3| &\leq \Psi_i,\ i = 2, 3\\
|A_4| &\leq \Psi_i,\ i = 1, 5, 6\\
|A_5| &\leq \Psi_i,\ i = 11, 13, 14, 15\\
0 &\leq \Psi_7.
\end{aligned}$$

Therefore, it follows that

$$\begin{aligned}
|\Psi| &= \sum_{i=1}^{15} \Psi_i\\
&\geq 4|A_1| + 2|A_2| + 2|A_3| + 3|A_4| + 4|A_5|\\
&\geq 16 \cdot 2^{r-5} - (4\Delta_1 + 2\Delta_2 + 2\Delta_3 + 3\Delta_4 + 4\Delta_5) - 2^{r-5}\\
&\geq 15 \cdot 2^{r-5} - 4\Delta\\
&\geq 15 \cdot 2^{r-5} - \Delta - 3(5 \cdot 2^{r-5}/9)\\
&> 13 \cdot 2^{r-5} - \Delta - \beta.
\end{aligned}$$

This is a contradiction. It follows that

$$m_0 = 0.$$

Similarly, we can show that we cannot take

$$f_1 \in \{(0011)^T,\ (0101)^T,\ (0110)^T\}.$$

Now in the matrix N, if $f_1 = (1100)^T, f_2 = (1110)^T$, then $m_2 + m_3 = 3$. Reasoning as before, we have a contradiction. Therefore, the relation is verified in the first case.

For the other cases, we use similar methods, together with Inequality 7.3 and Equation 7.4 to get a contradiction.

Therefore, the matrix M contains a pair of codewords in which no zeros occur in identical positions, and so the cap S is skew to a subspace of codimension two. □

The main theorem of this section states that large caps are either affine, or there exists a subspace of codimension two skew to it. The original proof was due to Davydov and Tombak. We sketch the proof as follows.

7.5.3 Theorem. *Let S be a complete cap in $PG(r-1, 2)$ of size $n \geq 2^{r-2}+2$, where $r \geq 4$ If S is not affine, then there exists a subspace of codimension two skew to it.*

Proof. Let M be the cap matrix of S. Then M is an $r \times n$ matrix. We prove the result by induction on r, the number of rows of M. We have the following two cases.

(a) When $r = 4$, the only complete cap of size at least six is the affine space $AG(3, 2)$. So M is the check matrix of the extended Hamming code of length 8 and 4 check symbols.

(b) Suppose that S is not affine, and $r \geq 5$. We represent the matrix M as the following form,

$$M = \left(\begin{array}{c|c} \overbrace{0\ldots0}^{n_0} & \overbrace{1\ldots1}^{w} \\ \hline A & B \end{array}\right)$$

where the first row has the smallest weight w in the code generated by M.

Since S is not affine, we have $2^{r-2} + 2 \leq n < 2^{r-1}$. By Lemma 7.3.3, we have $n_0 > n/2 \geq 2^{r-3} + 1$.

Let $n_0 = 2^{r-3} + \alpha$ where $\alpha \geq 2$. then the matrix A is the matrix of a cap in $PG(r-2, 2)$, which is either complete or is contained in a complete cap D. Let $|D| = n_D$ and then

$$n_0 \leq n_D.$$

By induction hypothesis, the cap D is skew to a space of codimension two. By Lemma 6.4.6, the cap D is obtained by successive doubling. Then we can assume that

$$n_D = 2^{r-3} + 2^{r-3-g}$$

where $g = 0, 2, 3, \ldots, r-3$. Note that $g \neq 1$, since the smallest complete cap that is not affine is the ovoid in $PG(3,2)$ of size five.

- If $g = 0$ the cap D is affine, and we are done.
- if $g = 2$. Then the cap D is a $(r-5)$-fold doubling of the ovoid in $PG(3,2)$ of size 5, and so by Lemma 7.5.2, the cap S is skew to a subspace of codimension two.
- If $g \geq 3$. Then the cap D is a $(r-3-g)$-fold doubling of a cap in $PG(g+1,2)$ of size $2^g + 1$, denote this small cap E.

  Represent the matrix of E as the following form,

  $$M_E = \left(\begin{array}{c|c} 0\ldots0 & \overbrace{1\ldots1}^{w_E} \\ \hline A_E & B_E \end{array}\right)$$

  where w_E is the smallest weight of a codeword in the code generated by M_E. By Lemma 7.3.1, we have $w_E \leq 2^{g-1} - 1$. Thus

  $$w_D \leq 2^{r-3-g}(2^{g-1} - 1) = 2^{r-4} - 2^{r-3-g}.$$

  By Lemma 7.5.1, it follows that

  $$w \leq 2 \cdot w_D \leq 2^{r-3} - 2^{r-2-g}.$$

  Thus

  $$n_0 = n - w \geq 2^{r-3} + 2^{r-2-g} + 2 > n_D.$$

  A contradiction. Hence the case $g \geq 3$ is ruled out.

It follows that there exists a subspace of codimension two skew to S, and by Lemma 6.4.6, the cap S is constructed by doubling. □

7.5.4 Corollary. *Let S be a complete cap in $PG(r-1,2)$ that is not affine. If $|S| \geq 2^{r-2}+2$ then $|S| = 2^{r-2}+2^{r-2-g}$ where $2 \leq g \leq r-2$.*

Proof. This result follows from the fact that the smallest complete cap that is not affine is the unique cap in $PG(3,2)$ of size five. □

The following corollary is due to Bruen and Wehlau.

7.5.5 Theorem. *Let S be a complete cap in $PG(r-1,2)$ of size $2^{r-2}+1$. Then S is skew to a subspace of codimension two.*

Proof. Embed S in a hyperplane H in $PG(r,2)$. Let S' be a cap in $PG(r,2)$ obtained by doubling the cap S. Then $|S'| = 2^{r-1}+2$. By Theorem 7.5.3, there is a subspace of codimension two skew to S', denote this subspace H_2. Then the subspace $H_2 \cap H$ is either a hyperplane in H (when H_2 is a subspace of H), or is a subspace of codimension two in H (when H_2 is not a subspace of H). □

Bibliography

[1] Albrecht Beutelspacher and Ute Rosenbaum. *Projective Geometry: from Foundations to Applications.* Cambridge University Press, Cambridge, 1998.

[2] Stephan Brandt. A 4-colour Problem for Dense Triangle-Free Graphs. *Discrete Math.*, 251(1-3):33–46, 2002. Cycles and colourings (Stará Lesná, 1999).

[3] A. E. Brouwer, A. A. Bruen, and D. L. Wehlau. There Exist Caps Which Block All Spaces of Fixed Codimension in $\mathbf{PG}(n, 2)$. *J. Combin. Theory Ser. A*, 73(1):168–169, 1996.

[4] Aiden A. Bruen, Lucien Haddad, and David L. Wehlau. Binary Codes and Caps. *J. Combin. Des.*, 6(4):275–284, 1998.

[5] Aiden A. Bruen and David L. Wehlau. Long Binary Linear Codes and Large Caps in Projective Space. *Des. Codes Cryptogr.*, 17(1-3):37–60, 1999.

[6] A. A. Davydov and L. M. Tombak. Quasiperfect Linear Binary Codes with Distance 4 and Complete Caps in Projective Geometry. *Problemy Peredachi Informatsii*, 25(4):11–23, 1989.

[7] Chris Godsil and Gordon Royle. *Algebraic Graph Theory.* Springer-Verlag, New York, 2001.

[8] J. H. B. Kemperman. On Small Sumsets in an Abelian Group. *Acta Math.*, 103:63–88, 1960.

[9] L. Lovász. Spectra of Graphs with Transitive Groups. *Period. Math. Hungar.*, 6(2):191–195, 1975.

[10] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes. I.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[11] Reza Naserasr and Claude Tardif. Chromatic Number of Cayley Graphs on $\mathbb{Z}_2^n$. *Unpublished.*

[12] Charles Payan. On the Chromatic Number of Cube-like Graphs. *Discrete Math.*, 103(3):271–277, 1992.

[13] Beniamino Segre. Introduction to Galois Geometries. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8)*, 8:133–236, 1967.

[14] W. T. Tutte. On the Algebraic Theory of Graph Colorings. *J. Combinatorial Theory*, 1:15–50, 1966.