Phan Geometries and Error Correcting Codes

by

Betty Iboroma Fyn-Sydney

A thesis submitted to
The University of Birmingham
for the degree of
Doctor of Philosophy

School of Mathematics
The University of Birmingham
August, 2013

Abstract

In this thesis, we define codes based on the Phan geometry of type A_n. We show that the action of the group $\mathrm{SU}_{n+1}(q)$ is not irreducible on the code. In the rank two case, we prove that the code is spanned by those apartments which only consist of chambers belonging to the Phan geometry and obtain submodules for the code.

Dedicated to the memory of my dearly beloved mother, Mrs Warriboko Fyn-Sydney (1953-2010).

Acknowledgements

Firstly, I would like to thank my supervisor, Dr Corneliu Hoffman, for his invaluable help, support and patience throughout the entire course of this thesis. It has been a real privilege working with him. I would also like to thank Dr Kay Magaard for his advice and helpful comments in the last stages of this thesis. I also wish to express my sincere gratitude to Prof Sergey Shpectorov for his encouragements and helpful advice in matters that have affected me. I am most grateful to Mrs Janette Lowe for her continued support, love and kindness towards me. She has helped make my stay in Birmingham a most memorable one. My thanks also go to all the staff in the department and to all my course mates for making my stay in Birmingham an interesting one.

I would also like to thank all my friends and family for their unwavering support, love and encouragement. Finally, I would like to acknowledge the Birmingham International Scholarship I received from the School of Mathematics.

Contents

Introduction

We are concerned with defining *error-correcting codes* on group geometries and buildings. The theory of error-correcting codes is a branch of Engineering and Mathematics which deals with the transmission and storage of data in a reliable way. In practice, absolute reliability of information media is not certain and so when information is being transmitted over a medium, data may become distorted due to *noise* (any form of interference or disturbance) in the communication channel.

The aim of an error-correcting code is to *encode* the message to be communicated, by adding some form of *redundancy*, so that the received message may be *decoded* by the decoder into a message resembling, as close as possible, the original message if (not too many) errors have occurred, or at least the presence of errors can be detected. The degree of resemblance will depend on how good the code is in relation to the channel in question.

In recent years, finite geometries have played a significant role in the theory of error-correcting codes. More specifically, finite geometries acted upon by groups have been found to provide spaces on which codes can be defined, and these codes have generally been found to have high error-correcting capabilities. Two examples of such codes are the Hamming code and the Golay code. These are error-correcting codes which have desirable properties in the sense that they are relatively short and can correct errors quickly. This is partly due to the fact that they are highly symmetric, i.e., they admit large automorphism groups. One related observation is that the codewords in each code have some natural meaning in the defining geometry for the automorphism group of the code. For example, in the case of the Hamming code, its automorphism group is the group $L_3(2)$ whose natural geometry is the rank 2 Projective geometry over $\mathbb{F}_2 = \{0, 1\}$. We identify the codewords with the lines of this projective space. The points and lines of this projective geometry are an example of a classical building of rank two.

For the purpose of this introduction, we define a *building* to be a simplicial complex consisting of a family of subcomplexes called *apartments* which satisfy certain axioms that we shall describe later in Chapter 1. Jacques Tits introduced buildings in order to provide a systematic approach for the geometric interpretation of semisimple complex Lie groups and also semisimple algebraic groups over an arbitrary field. Buildings played a significant role in the classification of the finite simple groups because these geometries allow certain abstract groups to be identified as groups of Lie type.

We obtain codes from buildings by using elementary algebraic topology following S. D. Smith and S. Yoshiara [14]. Their method involves defining *homolgy groups* on buildings which may be viewed as (linear) codes; and so *codewords* are just cycles in the homology group. An advantage of this construction is that, we can use the geometric information of the building to determine those cycles which have the smallest possible *weight*. This weight is called the *minimal weight* of the code and determines its error correction capability. There are other geometric implications of such a construction. In the particular case of a building associated with a simple Chevalley group, minimal cycles are given by apartments. Furthermore, the (top dimensional) homology group provides a natural construction of the irreducible complex Steinberg module. So, just as in the case of the Hamming and the Golay codes, this code is also very symmetric. It is therefore reasonable to ask if such a construction exists for other group geometries.

A subclass of Tits buildings are the buildings coming from *Phan geometries*. These geometries are named after Kok-Wee Phan who proved several results in [10] and [11] which played significant roles in the classification of the finite simple groups. Our interest lies with the *Phan geometry of type* A_n. The *Phan geometry* $\Gamma = \Gamma(n, q)$ *of type* A_n is the simplicial complex whose vertex set consists of all the proper non-degenerate subspaces of the unitary space $V = V(n, q)$ for the unitary group $SU_{n+1}(q)$. This geometry was instrumental in the revision of Phan's first theorem which states that, for $q > 4$ and $n \geq 3$, the group $SU_{n+1}(q)$ is the universal completion of the amalgam of its fundamental subgroups having rank one and two.

It was M. Aschbacher [2] who first observed that, using standard geometric results, simple connectedness of this geometry would imply Phan's first theorem. He and K.M. Das [8] did some work towards a new proof of Phan's theorem and Das proved that Γ is simply connected for q odd, $q \neq 3$. Later, C. Bennett and S. Shpectorov [5] gave a complete proof of Phan's theorem, which partially generalizes to the cases $q = 2$ and $q = 3$. The significance of this geometry in the revision of Phan's theorem makes it an important geometry for the group $SU_{n+1}(q)$.

We define (linear) codes based on this geometry Γ and investigate some of its properties. The main motivation for our research was to obtain codes which would have properties analogous to those of the Hamming and Golay codes, and also possess some nice geometric properties. We employ the methods of Smith and Yoshiara [14] in defining linear codes based on the geometry Γ and refer to the code obtained in this way as the *Phan code*. Utilizing information about the code based on the projective geometry Δ for the unitary space V, and the action of the unitary group $G = SU_{n+1}(q)$ on the geometry Γ, we obtain the following result regarding the *length* and *minimal weight* of the Phan code.

Theorem 0.0.1. *The Phan code has length* $|G : G_C|$ *and minimal weight* $(n+1)!$*, where* G_C *denotes the stabilizer of a chamber* C *in* Γ*.*

In [9], Devillers *et al* proved that if $q > 2^{n-1}(\sqrt{q}+1)$ the Phan geometry Γ is *Cohen-Macaulay*, that is, reduced homology vanishes from top dimension. This enables us to determine the dimension of the Phan code.

Theorem 0.0.2. *Let* Γ_i *denote the set of* i*-dimensional simplices in* Γ *and suppose* $q > 2^{n-1}(\sqrt{q}+1)$*. Then the dimension of the Phan code is given by*

$$\chi(\Gamma) = \sum_{i=0}^{n+1} (-1)^i |\Gamma_{n-i}|.$$

We further obtain a recursive formula for the dimension of the Phan code, more on this can be found in Chapter 5.

We investigate the properties of the Phan code and prove that unlike the Hamming and Golay codes given above, the action of the group G on the Phan code is not irreducible.

Theorem 0.0.3. *The Phan code is not irreducible.*

In the rank two case, we obtain a basis for the Phan code and show that it is spanned by the set of codewords corresponding to apartments which consist only of chambers in Γ.

The structure of the thesis is as follows. In Chapter 1, we introduce Buildings and BN-pairs and collect some relevant results. We also give a description of the building of type A_n. Homology and Simplicial complexes are covered in Chapter 2. In Chapter 3, we describe linear codes and how they can be obtained from homology. We also define codes on buildings using the method of Smith and Yoshiara. Chapter 4 is dedicated to the unitary space and the unitary group. The main results of this thesis can be found in Chapter 5. In addition, we investigate the properties of the code in the rank two case in more detail.

Chapter 1

Buildings

In this chapter, we collect some results on Chamber systems, Coxeter groups, groups with BN-pairs and Buildings which we will use in later parts of this thesis.

1.1 Chamber systems

In this section, we explore the concept of a chamber system. A more detailed description can be found in [1], [12] and [17].

Definition 1.1.1. *A* chamber system *over a set I is a nonempty set $\mathcal{C}$ together with a family of equivalence relations $(\sim_i)_{i\in I}$ on $\mathcal{C}$ indexed by I. The elements of $\mathcal{C}$ are called* chambers *and the equivalence classes with respect to $\sim_i$ are called i-*panels*, a* panel *being an i-panel for some $i \in I$. Two chambers C and D are i-*adjacent*, written $C \sim_i D$, if they lie in the same i-panel, and we say they are adjacent if they are i-adjacent for some $i \in I$. We require further that each panel contains at least two chambers.*

A chamber system is said to be *thin* if every panel contains exactly two chambers and *thick* if every panel contains at least three chambers. For any set I, let M_I denote the *free monoid* on I, that is, the set of all words in the alphabet I including the empty word, with multiplication given by concatenation.

Definition 1.1.2. *Let $\mathcal{C}$ be a chamber system and let $C, D \in \mathcal{C}$. A* gallery *of length k connecting C and D is a sequence $\gamma = (C_0, \ldots, C_k)$ such that $C_0 = C$, $C_k = D$ and $C_{j-1} \sim_{i_j} C_j$ for some $i_j \in I$. The* type *of the the gallery γ is the word $i_1 \cdots i_k \in M_I$.*

A chamber system $\mathcal{C}$ is said to be *connected* if any two chambers $C, D \in \mathcal{C}$ can be connected by a gallery. The *distance* $d(C, D)$ from C to D is defined to be the length of a shortest gallery from C to D if such a gallery exists, and ∞ otherwise. A gallery from C to D is said to be *minimal* if it has length $d(C, D)$. The *diameter* of $\mathcal{C}$ denoted $\mathrm{diam}(\mathcal{C})$ is the supremum of the set $\{d(A, B) \mid A, B \in \Delta\}$. We say that two chambers C and D are *opposite* if $d(C, D) = \mathrm{diam}(\Delta) < \infty$.

1.2 Coxeter groups

In this section, we shall be concerned with finite groups W having a generating set S of involutions (elements of order 2) subject to certain relations. We make reference to [1], [6] and [7].

Definition 1.2.1. *Let S be a set. A* Coxeter matrix *of type S is a square symmetric array $M = (m(s, s'))_{s,s' \in S}$ such that $m(s, s')$ are positive integers or $+\infty$ satisfying the following relations:*

- *$m(s, s) = 1$ for all $s \in S$*

- $m(s, s') \geq 2$ *for all* $s \neq s' \in S$.

A Coxeter group W *is a group having a presentation*

$$\langle s \in S \mid (ss')^{m(s,s')} = 1 \text{ for all } s, s' \in S \rangle.$$

The set S *is called the* generating set *for* W *and we call the pair* (W, S) *a* Coxeter system.

Observe that the condition that $m(s, s) = 1$ for all $s \in S$ implies that the elements of S are involutions. Furthermore, if $m(s, s') = 2$, then $ss' = s's$, that is, s and s' commute. If W is a finite Coxeter group, then $m(s, s') < \infty$ for all $s, s' \in S$.

Definition 1.2.2. *We define the* Coxeter diagram *of a Coxeter matrix* $M = (m(s, s'))_{s,s' \in S}$ *to be the graph with vertex set* S *and edge set consisting of all unordered pairs* $\{s, s'\}$*, such that* $m(s, s') \geq 3$ *together with the labeling which assigns the label* $m(s, s')$ *to each edge* $\{s, s'\}$*. The* rank *of a Coxeter diagram is the cardinality of its vertex set* S*.*

Let (W, S) be a Coxeter system and let Π be the corresponding Coxeter diagram. Then we say (W, S) is a *Coxeter system of type* Π. We remark that two vertices s and s' are adjacent in Π if and only if they do not commute. A Coxeter system is said to be *irreducible* if the underlying graph of its corresponding Coxeter diagram is connected. From now on we consider only finite Coxeter systems.

Definition 1.2.3. *Let* (W, S) *be a finite Coxeter system. For* $w \in W$*, we define the* length $l(w)$ *of* w *(with respect to* S*) to be the least integer* k *such* *that w is a product of k elements of S. A* word *in the generating set S (called an S-word) is a finite sequence $\mathbf{s} = (s_1, s_2, \ldots, s_k)$ of elements of S. It is said to be* reduced *if the corresponding element $w = s_1 s_2 \cdots s_k$ has length $l(w) = k$, and we say that* $\mathbf{s}$ *is a* reduced decomposition *of w.*

By convention the empty word is reduced and the corresponding product is $1 \in W$. The elements of the generating set S are the only elements having length 1. We collect some results on the length function l of the Coxeter group W.

Proposition 1.2.4. *Let (W, S) be a finite Coxeter system and $w, w' \in W$. We have the following:*

(i) $l(ww') \leq l(w) + l(w')$,

(ii) $l(w^{-1}) = l(w)$,

(iii) $|l(w) - l(w')| \leq l(ww'^{-1})$.

Proof. This is Proposition 1 in Chapter IV of [6]. □

We have an important assertion about Coxeter systems known as the *exchange condition*.

(E) **(The Exchange Condition)**

Let (W, S) be a finite Coxeter system and let $w \in W$ and $s \in S$ such that $l(ws) \leq l(w)$. If $(s_1, \ldots, s_q)$ is any reduced decomposition of w, then there is an integer j such that $1 \leq j \leq q$ and

$$s_{j+1} \ldots s_q s = s_j s_{j+1} \ldots s_q.$$

Similarly, we also have

$$ss_1 \cdots s_{j-1} = s_1 \cdots s_{j-1} s_j,$$

if $l(sw) \leq l(w)$.

Proposition 1.2.5. *Let (W, S) be a finite Coxeter system. Let $s \in S$, $w \in W$ and $\mathbf{s} = (s_1, \ldots, s_q)$ be a reduced decomposition of w. Then one of the following holds.*

(a) $l(sw) = l(w) + 1$ and $(s, s_1, \ldots, s_q)$ is a reduced decomposition of sw.

(b) $l(sw) = l(w) - 1$ and there is some integer j, $1 \leq j \leq q$ such that $(s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_q)$ is a reduced decomposition of sw and

$$(s, s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_q)$$

is a reduced decomposition of w.

Proof. Let $w' = sw$. Then by Proposition 1.2.4 (iii),

$$\begin{aligned} |l(w) - l(w')| &\leq l(ww'^{-1}) \\ &= l(s) = 1. \end{aligned}$$

If $l(w') > l(w)$, then $|l(w) - l(w')| = 1$ which implies $l(w') = l(w) + 1 = q + 1$ and $(s, s_1, \ldots, s_q)$ is a reduced decomposition of w'.
If $l(w') \leq l(w) = q$, then by the exchange condition, there exists $j \in \{1, \ldots, q\}$ such that

$$w = ss_1 \cdots s_{j-1} s_{j+1} \cdots s_q,$$

and so $w' = sw = s_1 \cdots s_{j-1}s_{j+1} \cdots s_q$. Thus $q-1 \leq l(w') \leq q$ and since $l(w')$ is an integer, we must have that $l(w') = q - 1$. So $(s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_q)$ is a reduced decomposition of w'. $\square$

Let V be a finite dimensional real vector space endowed with a symmetric positive definite bilinear form $(\ ,\ )$ taking values in $\mathbb{R}$. Let $O(V)$ denote the set T of linear transformations from V to itself such that $(T(u), T(v)) = (u, v)$ for all $u, v \in V$. A *reflection* is an element $s \in O(V)$ such that $s \neq 1$ and s fixes every vector in some hyperplane in V.

Definition 1.2.6. *A subgroup of $O(V)$ generated by reflections is referred to as a* group generated by reflections.

Our main aim is to describe finite Coxeter groups as groups generated by reflections.

Definition 1.2.7. *A* root system Δ *in V is a finite set of vectors having the following properties.*

1. *$0 \notin \Delta$ and Δ spans V.*

2. *If $\alpha \in \Delta$, then $-\alpha \in \Delta$; moreover if $c\alpha \in \Delta$ for some $c \in \mathbb{R}$, then $c = \pm 1$.*

3. *For each $\alpha \in \Delta$, we have $s_\alpha \Delta = \Delta$, where s_α is the reflection fixing the hyperplane $\langle \alpha \rangle^\perp$.*

The group $W = W(\Delta)$ generated by the reflections $\{s_\alpha \mid \alpha \in \Delta\}$ is the subgroup of $O(V)$ associated with the root system Δ. The next result shows that Coxeter groups can be identified with finite groups generated by reflections.

Theorem 1.2.8. *Let (W, S) be a finite Coxeter system with generating set $S = \{s_1, \dots, s_n\}$. Let V be a vector space of dimension n over $\mathbb{R}$ with basis $\{e_1, \dots, e_n\}$. Define the bilinear form $B : V \times V \to \mathbb{R}$ by*

$$B(e_i, e_j) = -\cos \pi / m_{ij}$$

$1 \leq i, j \leq n$, where m_{ij} is the order of $s_i s_j$ in W. For each $s_i \in S$ define a linear transformation $T(s_i)$ on V by

$$T(s_i)e_j = e_j - 2B(e_i, e_j)e_j, \ 1 \leq j \leq n.$$

Then the following hold.

(i) The map $T : S \to \operatorname{End} V$ extends to a faithful representation $T : W \to GL(V)$, where $\operatorname{End} V$ denotes the set of endomorphisms of V.

(ii) The bilinear form B is symmetric, positive definite and $T(w)$-invariant for all $w \in W$.

(iii) The group $T(W)$ is a finite group generated by reflections, and the set $\{T(s_1), \dots, T(s_n)\}$ can be identified with a set of fundamental reflections in $T(W)$.

(iv) If the Coxeter system (W, S) is irreducible, then the representation T is absolutely irreducible.

Proof. See Theorem 64.28 in [7]. □

We shall now consider a certain important family of subgroups of a Coxeter group.

Definition 1.2.9. *Let (W, S) be a finite Coxeter system, let $J \subseteq S$ and denote by W_J the subgroup of W spanned by J. The subgroups $\{W_J\}_{J \subseteq S}$ are called* standard parabolic subgroups *of W. Their conjugates are called* parabolic subgroups *of W.*

We collect some results on parabolic subgroups of a Coxeter group.

Proposition 1.2.10. *Let (W, S) be a finite Coxeter system with length function l. Then the following statements hold.*

(i) For each $w \in W_J$, all reduced expressions for w have all their factors in J.

(ii) For each $J \subseteq S$, the pair (W_J, J) is a Coxeter system.

(iii) The map $J \to W_J$, $J \subseteq S$, is a bijection from the family of all subsets of S to a family of subgroups of W.

(iv) For all $J, K \subseteq S$, $W_J \cap W_K = W_{J \cap K}$.

(v) The set S is a minimal set of generators for W.

Proof. (i) is Lemma 64.33 in [7], (ii) follows from Proposition 64.36 in [7], (iii) follows from (i) and the definition of parabolic subgroups, (iv) also follows from (i), and (v) follows from Proposition 1.2.8 (i) and (iii). □

We now wish to collect some results on double cosets of the Coxeter group W. First we require the following definition.

Definition 1.2.11. *Let W be a group and U a subgroup of W. Then the group $U \times U$ acts on W by $(u, u').w = uwu'^{-1}$ for $u, u' \in U$ and $w \in W$.*

The orbits of $U \times U$ on W are the sets UwU for $w \in W$, and are called the double cosets *of W with respect to U. They form a partition of W and the corresponding quotient is denoted by $U \setminus W/U$.*

Note that if C, C' are two double cosets, then their product CC' is a union of double cosets.

Proposition 1.2.12. *Let (W, S) be a Coxeter system and $J, K \subseteq S$. There is a unique element x of minimal length in every double coset $W_J w W_K \in W_J \setminus W/W_K$. Furthermore, each element in $W_J x W_K$ has an expression uxv, with $u \in W_J$, $v \in W_K$ and*

$$l(uxv) = l(u) + l(x) + l(v).$$

Proof. See [7], Proposition 64.38. □

Observe that if $J = \emptyset$, then $W_J w W_K = wW_K$. Thus, by Proposition 1.2.12, every left coset wW_K has a unique element of minimal length. Similar remarks hold if $K = \emptyset$.

Definition 1.2.13. *An element x of minimal length in a double coset $W_J \setminus W/W_K$ (as in Proposition 1.2.12) will be called a* distinguished double coset representative*. We denote by D_{JK} the set of all distinguished double coset representatives for all the double cosets in $W_J \setminus W/W_K$.*

1.3 BN-pairs

In this section, we collect some results on groups with BN-pairs. Most of our results are taken from [7] and we also refer to [4] and [6].

We recall the definition of double cosets of a group as given in Definition 1.2.11.

Definition 1.3.1. *A* BN-pair *(or* Tits system*) in a group G is a pair of subgroups (B, N) of G, satisfying the following axioms.*

(B1) $G = \langle B, N \rangle$.

(B2) $H = B \cap N$ *is normal in* N.

(B3) $W = N/H$ *is a Coxeter group with generating set* $S = \{s_i \mid i \in I\}$.

(B4) For any $w \in W$ and $s \in S$ we have $BsBwB \subseteq BwB \cup BswB$, and $sBs \neq B$.

The group W is called the *Weyl group* of the BN-pair and the cardinality $|I|$ of I is the rank of the BN-pair. Any subgroup of G which is conjugate to B is called a *Borel subgroup*.

Remark 1.3.2. *Every element of W is a coset modulo $H = B \cap N$ and is therefore a subset of G. Thus, products of the form BwB make sense. In particular, if π denotes the natural homomorphism from N to $W = N/H$ given by $\pi(n) = nH$, then the product BwB may be taken to represent each BnB such that $\pi(n) = w$. For instance, $(B4)$ may be rewritten as $Bn_iBnB \subseteq BnB \cup Bn_inB$ and $n_iBn_i \neq B$ for all $n_i, n \in N$ such that $\pi(n_i) = s_i \in S$ and $\pi(n) = w \in W$. Additionally, for any subset $A \subset W$, we let BAB denote the subset $\bigcup_{w \in A} BwB$.*

Example 1.3.3. *For* $G \leq GL_n(q)$*, take*

$$\begin{aligned} B &:= G \cap \text{ upper triangular matrices} \\ N &:= G \cap \text{ monomial matrices} \\ H &:= G \cap \text{ diagonal matrices.} \end{aligned}$$

Then B *and* N *form a* BN*-pair for* G*. For instance, take* $G = SL_3(2)$*. Then* B *consists of matrices of the form*

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

The subgroup N *in this case is just the set of permutation matrices (since the only nonzero element in* $\mathbb{F}_2$ *is* 1*). So* $T = B \cap N = \{1\}$ *and the Weyl group* $W = N/T \cong S_3$*.*

For the remaining part of this section let G, B, N, W and S be as in Definition 1.3.1. We collect some results on BN-pairs, proofs can be found in [7].

Proposition 1.3.4. *Let* $w, w' \in W$*, then* $BwB = Bw'B$ *if and only if* $w = w'$*. Hence, there is a bijection* $w \mapsto BwB$ *from* W *to* $B \backslash G/B$*. Furthermore, for any* $s \in S$*, if* $l(sw) = l(w) + 1$*, then* $BsBwB = BswB$*.*

Proof. See Theorem 65.4 and Proposition 65.5 in [7]. □

As a consequence of Proposition 1.3.4, we have that $G = \dot{\bigcup}_{w \in W} BwB = BWB$. This is called the *Bruhat decomposition* for the group G.

For any subset $J \subseteq S$, recall from the previous section that W_J is the subgroup of W generated by J. Let P_J denote the union BW_JB of double cosets BwB, $w \in W_J$. Then $P_\emptyset = B$ and $P_S = G$.

Theorem 1.3.5. *Let $J \subseteq S$. Then P_J is a subgroup of G containing B. If $P \leq G$ contains B, then $P = P_J$ for some $J \subseteq S$.*

Proof. See Theorem 65.13 in [7]. □

Definition 1.3.6. *The subgroups $\{P_J\}_{J \subseteq S}$ of G which contain the (standard) Borel subgroup B of G are called* standard parabolic subgroups *of G. A* parabolic subgroup *of G is a conjugate of a standard parabolic subgroup.*

Each P_J contains a BN-pair with Borel subgroup B and Weyl group W_J. We collect some properties of parabolic subgroups.

Proposition 1.3.7. *Let $I, J \subseteq S$. The following hold.*

(i) $I \subseteq J$ if and only if $P_I \subseteq P_J$.

(ii) $P_I \cap P_J = P_{I \cap J}$.

(iii) The map $I \to P_I$ gives a bijection from the set of subsets of S to the set of standard parabolic subgroups of G.

Proof. See Proposition 65.17 in [7]. □

Corollary 1.3.8. *The set S is a minimal generating set of generators of W.*

Theorem 1.3.9. *We have the following.*

(i) For each parabolic subgroup P of G, we have $N_G(P) = P$.

(ii) If P_1 and P_2 are two parabolic subgroups of G such that $P_1 \cap P_2$ is parabolic, then $gP_1g^{-1} \leq P_2$ if and only if $P_1 \leq P_2$ and $g \in P_2$.

Proof. See Theorem 65.19 in [7]. $\square$

Corollary 1.3.10. *Every parabolic subgroup of G is conjugate to a unique standard parabolic subgroup of G.*

The next result shows a connection between parabolic subgroups of G and parabolic subgroups of W.

Theorem 1.3.11. *Let $J, K \subseteq S$. There exists a bijection of double cosets*

$$W_J \setminus W/W_K \leftrightarrow P_J \setminus G/P_K$$

given by $W_K w W_K \leftrightarrow BW_J w W_K B = P_J w P_K$.

Proof. This is Theorem 65.21 in [7]. $\square$

1.4 Buildings

Throughout this section let I be a set and M be a Coxeter matrix over I, let (W, S) be a Coxeter system of type M, where $S = \{s_i \mid i \in I\}$ and let l denote the length function of the Coxeter group W. Most of our work in this section is taken from [1], and we also make reference to [12] and [17].

Definition 1.4.1. *A* building *of type (W, S) (or M) is a pair $(\mathcal{C}, \delta)$, where $\mathcal{C}$ is a chamber system over S and δ is a function from $\mathcal{C} \times \mathcal{C}$ to W such that for any pair of chambers $C, D \in \mathcal{C}$ and any reduced S-word $\mathbf{s} = (s_1, s_2, \ldots, s_k)$, $\delta(C, D) = s_1 s_2 \cdots s_k$ if and only if there exists a gallery of type $\mathbf{s}$ connecting*

C and D. The group W is called the Weyl group *and the map δ is called the* Weyl distance function *of $\mathcal{C}$.*

Observe that the definition implies that any two chambers can be joined by a reduced gallery in a building. For the ease of notation we shall denote a building $(\mathcal{C}, \delta)$ simply by $\mathcal{C}$.

Example 1.4.2. *Let (W, S) be a Coxeter system and let $\Sigma = \Sigma_W$ be the chamber system whose chambers are the elements of W. Two chambers $x, y \in \Sigma$ are adjacent if and only if $y = xs$ for some $s \in S$. Then Σ_W together with the map $\delta = \delta_W$ defined by*

$$\delta(x, y) = x^{-1}y$$

for all $x, y \in W$ is a building of type M.

The following result provides an alternative definition for buildings.

Lemma 1.4.3. *Let Δ be a chamber system over S and let δ be a map from $\Delta \times \Delta$ to W. Then (Δ, δ) is a building if and only if δ satisfies the following conditions.*

(i) *$\delta(C, D) = 1$ if and only if $C = D$.*

(ii) *If $\delta(C, D) = w$ and $C' \in \Delta$ is such that $\delta(C', C) = s \in S$, then $\delta(C', D) \in \{sw, w\}$. Furthermore, if $l(sw) = l(w) + 1$, then $\delta(C', D) = sw$.*

(iii) *If $\delta(C, D) = w$, then for any $s \in S$, there exists $C' \in \Delta$ such that $\delta(C', C) = s$ and $\delta(C', D) = sw$.*

Proof. See [1], Proposition 5.23. □

Proposition 1.4.4. *Let Δ be a building. Then Δ is connected.*

Proof. This follows from the definition since any two chambers can be joined by a gallery of reduced type. □

Proposition 1.4.5. *A gallery is minimal if and only if its type $\boldsymbol{s}$ is reduced. Furthermore, if $\boldsymbol{s}$ is reduced, then a gallery of type $\boldsymbol{s}$ is unique.*

Proof. See [12], (3.1). □

Recall the definition of the distance $d(C, D)$ between two chambers C and D in a chamber system, defined in section 1.1.

Corollary 1.4.6. *For any two chambers C, D in a building Δ, the following hold:*

1. $\delta(C, D) = \delta(D, C)^{-1}$.
2. $d(C, D) = l(\delta(C, D))$.

Recall that if $J \subseteq S$ the group $W_J = \langle J \rangle \leq W$ is a Coxeter group of type J, thus (W_J, J) is a Coxeter subsystem of (W, S).

Definition 1.4.7. *Let $J \subseteq S$. We say that the chambers $C, D \in \Delta$ are* J-equivalent *denoted $C \sim_J D$ provided $\delta(C, D) \in W_J$. Observe that Lemma 1.4.5 implies that $C \sim_J D$ if and only if there is a gallery connecting C and D of type $(s_1, s_2, \ldots, s_k)$ with $s_i \in J$ for all $i \in [1, k]$. It follows that*

J-equivalence is an equivalence relation. We call the equivalence classes J-residues*. Thus, for each chamber $C \in \Delta$ there is a unique J-residue containing C. We denote this residue by $R_J(C)$. Hence*

$$R_J(C) = \{D \in \Delta \mid \delta(C, D) \in W_J\}.$$

A residue *is a subset $\mathcal{S}$ of Δ which is a J-residue for some $J \subseteq S$. The set J is referred to as the* type *of the residue $\mathcal{S}$, and the cardinality $|J|$ is referred to as its* rank*. We also refer to the set $S \setminus J$ as the* cotype *of $\mathcal{S}$.*

Observe that panels are residues of rank 1 (and type s for some $s \in S$), a single chamber is a residue of rank 0 (and type $\emptyset$), and the building Δ is the unique residue of type S.

We now collect some results pertaining to residues. First, we fix some notation.

Definition 1.4.8. *Let $\mathcal{S}, \mathcal{T} \subseteq \Delta$. We define the* Weyl function *$\delta(\mathcal{S}, \mathcal{T})$ by $\delta(\mathcal{S}, \mathcal{T}) = \{\delta(X, Y) \mid X \in \mathcal{S}, Y \in \mathcal{T}\}$.*

Lemma 1.4.9. *Given a J-residue $\mathcal{R}$ and a K-residue $\mathcal{S}$ of a building Δ, $J, K \subseteq S$, the Weyl function $\delta(\mathcal{R}, \mathcal{S})$ is a double coset of the form $W_J w W_K$. In particular, $\delta(\mathcal{R}, \mathcal{R}) = W_J$.*

Proof. See [1], Theorem 5.29. □

Corollary 1.4.10. *Suppose $\mathcal{R}$ is a J-residue for some $J \subseteq S$. Then $(\mathcal{R}, \delta|_{\mathcal{R}\times\mathcal{R}})$ is a building of type (W_J, J).*

Note that if $J = \emptyset$, then the J-residue $\mathcal{R}$ consists of a single chamber C and

$\delta(C, \mathcal{S}) = \delta(\{C\}, \mathcal{S})$ is a left coset wW_K. We obtain a similar result if K is empty.

Let $J, K \subseteq S$ and $w \in W$. Recall that a double coset $W_J w W_K$ has a unique element of minimal length. We denote this element by $\min(W_J w W_K)$, so $w_1 = \min(W_J w W_K)$ if and only if w_1 has minimal length in $W_J w W_K$. Thus, if $\mathcal{R}, \mathcal{S}$ are any two residues, then we have a well-defined minimal element $w_1 = \min(\delta(\mathcal{R}, \mathcal{S})) \in W$. Set

$$d(\mathcal{R}, \mathcal{S}) = min\{d(C, D) \mid C \in \mathcal{R}, D \in \mathcal{S}\}.$$

Notice that for any $C \in \mathcal{R}$ and $D \in \mathcal{S}$ satisfying $d(C, D) = d(\mathcal{R}, \mathcal{S})$, Corollary 1.4.6 implies that $l(\delta(C, D)) = d(\mathcal{R}, \mathcal{S})$. In particular, $\delta(C, D)$ is minimal in $\delta(\mathcal{R}, \mathcal{S})$ and so by uniqueness, we have that

$$\delta(C, D) = \min(\delta(\mathcal{R}, \mathcal{S})) = w_1.$$

This gives us a characterization for the unique minimal element $w_1 \in \delta(\mathcal{R}, \mathcal{S})$. We wish to study projection of chambers onto residues. In order to do this, we require a technical result known as the *gate property.*

Lemma 1.4.11. *Suppose Δ is a building and let $\mathcal{R}$ be a residue and $D \in \Delta$. Then there exists a unique chamber $C_1 \in \mathcal{R}$ such that $d(C_1, D) = d(\mathcal{R}, D)$. Furthermore, C_1 has the following properties:*

1. *$\delta(C_1, D) = \min(\delta(\mathcal{R}, D))$.*

2. *$\delta(C, D) = \delta(C, C_1)\delta(C_1, D)$ for all $C \in \mathcal{R}$.*

3. $d(C, D) = d(C, C_1) + d(C_1, D)$ *for all* $C \in \mathcal{R}$*.*

Proof. A proof can be found in [1], Proposition 5.34. $\square$

Definition 1.4.12. *Let $\mathcal{R}$ be a residue in a building Δ and let $D \in \Delta$. We call the unique chamber $C_1 \in \mathcal{R}$ at minimal distance from D the* projection of D onto $\mathcal{R}$ *and denote it by* $\mathrm{proj}_{\mathcal{R}}(D)$*. By Lemma 1.4.11(1), it is the unique element in $\mathcal{R}$ satisfying*

$$\delta(C_1, D) = \min(\delta(\mathcal{R}, D)).$$

Definition 1.4.13. *Let Δ be a building. A nonempty subset $\mathcal{C}$ of Δ is said to be* convex *if for any two chambers $C, D \in \mathcal{C}$, every minimal gallery connecting C and D in Δ is contained in $\mathcal{C}$.*

Note that a convex subset $\mathcal{C}$ of a building Δ is necessarily connected.

Proposition 1.4.14. *Let Δ be a building. Then all residues of Δ are convex.*

Proof. Let $\mathcal{R}$ be a residue of Δ of type $J \subseteq S$ and let A, B be chambers in $\mathcal{R}$. Let γ be a minimal gallery connecting A and B. Suppose there exists $C \in \gamma$ such that $C \notin \mathcal{R}$ and let $D = \mathrm{proj}_{\mathcal{R}} C$. Then Lemma 1.4.11(3) implies $d(A, C) > d(A, D)$ and $d(B, C) > d(B, D)$. Thus any gallery connecting A and B passing through C is longer than any gallery connecting A and B passing through D. This contradicts the minimality of γ and so γ must be contained in $\mathcal{R}$. $\square$

Definition 1.4.15. *Suppose (Δ, δ) is a building of type (W, S). Let $\mathcal{C}$ be a subset of Δ and $\delta_{\mathcal{C}} = \delta|_{\mathcal{C} \times \mathcal{C}}$. If $(\mathcal{C}, \delta_{\mathcal{C}})$ is a building of type (W, S), then $(\mathcal{C}, \delta_{\mathcal{C}})$ is called a* subbuilding *of (Δ, δ).*

A building (Δ, δ) is said to be *thin (respectively, thick)* if Δ is a thin (respectively, thick) chamber system.

Lemma 1.4.16. *Suppose $\mathcal{A}$ is a thin building. Then for all $C, D, E \in \mathcal{A}$, we have $\delta(C, E) = \delta(C, D)\delta(D, E)$.*

Proof. See [1], Lemma 5.55. □

Definition 1.4.17. *Let Δ be a building. An* apartment *$\mathcal{A}$ of Δ is a thin subbuilding of Δ.*

We now collect some properties of apartments.

Proposition 1.4.18. *Let $\mathcal{A}$ be a subset of a building Δ of type (W, S). The following are equivalent.*

(i) $\mathcal{A}$ is an apartment.

(ii) $\mathcal{A}$ is thin and convex.

(iii) $\mathcal{A}$ is isomorphic to Σ_W, where Σ_W denotes the Coxeter chamber system of W.

Proof. A proof can be found in [17]. □

Definition 1.4.19. *For any subset X of W, define a map $\alpha : X \to \Delta$ to be an* isometry *if it preserves the W-distance δ. Thus,*

$$\delta_\Delta(\alpha(x), \alpha(y)) = \delta_W(x, y) = x^{-1}y$$

for all $x, y \in X$, where δ_Δ and δ_W denote the Weyl distance functions in Δ and W respectively.

Theorem 1.4.20. *Any isometry of a subset X of W into Δ extends to an isometry of W into Δ.*

Proof. This is Theorem 3.6 in [12]. □

Corollary 1.4.21. *Any two chambers lie in a common apartment.*

Observe that an isometry $\alpha : W \to \Delta$ is uniquely determined by its image $\mathcal{A} = \alpha(W)$ and the chamber $C = \alpha(1)$.

Definition 1.4.22. *Let Δ be a building, fix an apartment $\mathcal{A} \in \Delta$ and a chamber $C \in \mathcal{A}$ and let α be an isometry such that $\mathcal{A} = \alpha(W)$ and $C = \alpha(1)$. Let $\rho_{C,\mathcal{A}} : \Delta \to \mathcal{A}$ be a map defined by*

$$\rho_{C,\mathcal{A}}(D) = \alpha(\delta(C, D)) \text{ for all } D \in \Delta.$$

Then $\rho_{C,\mathcal{A}}$ is called the retraction of Δ onto $\mathcal{A}$ with centre C*.*

Recall that for a fixed chamber C in an apartment $\mathcal{A}$ and every $w \in W$, there is a unique chamber $D \in \mathcal{A}$ such that $\delta(C, D) = w$. Thus the retraction map $\rho_{C,\mathcal{A}}$ maps every chamber D in the building, at distance $w \in W$, to the unique chamber $D' \in \mathcal{A}$ at distance w from C. In particular, $\rho_{C,\mathcal{A}}(D) = D$ for all $D \in \mathcal{A}$.

Lemma 1.4.23. *Let Δ be a building. Any two apartments $\mathcal{A}_1$ and $\mathcal{A}_2$ are isomorphic. Moreover there is an isomorphism $\pi : \mathcal{A}_1 \to \mathcal{A}_2$ such that $\pi(C) = C$ for all $C \in \mathcal{A}_1 \cap \mathcal{A}_2$.*

Proof. See Corollary 5.68 in [1]. □

Recall that residues are buildings, so we can talk about apartments of residues.

Proposition 1.4.24. *Let Δ be a building and $\mathcal{R}$ a residue of Δ. The following hold.*

(i) If $\mathcal{A}_0$ is an apartment of R, then $\mathcal{A}_0 = \mathcal{A} \cap \mathcal{R}$ for some apartment $\mathcal{A}$ of Δ.

(ii) Let C be a chamber of Δ and let $\mathrm{proj}_{\mathcal{R}} C = D$. Then D is contained in every apartment of Δ containing C and some chamber of $\mathcal{R}$.

Proof. See Proposition 8.14 and Theorem 8.21 in [17]. □

We shall be mainly concerned with *spherical buildings* (that is, buildings having finite Weyl groups). The next result shows that every apartment in a spherical building of rank n is a triangulation of an $(n-1)$-sphere.

Theorem 1.4.25. *A spherical building Δ of rank n is homotopic to a bouquet of $(n-1)$-spheres, where there is one sphere for each apartment containing a fixed chamber C.*

Proof. See Appendix 4 in [12]. □

We now show the connection between buildings and groups with BN-pairs.

Throughout the remaining part of this section let G be a group with a BN-pair and let W be the corresponding Weyl group with generating set S.

Definition 1.4.26. *Let Δ be a building and let $G \leq \mathrm{Aut}(\Delta)$. We say G is* strongly transitive *if it satisfies the following conditions.*

(i) For each $w \in W$, G acts transitively on the set of ordered pairs of chambers (C, D) such that $\delta(C, D) = w$.

(ii) There is an apartment $\mathcal{A}$ whose stabilizer in G is transitive on the set of chambers of $\mathcal{A}$ (thus inducing the Coxeter group W on $\mathcal{A}$).

The aim here is to show that a building Δ admitting a strongly transitive group G determines a Tits system. Fix a chamber $C \in \Delta$, the chambers in Δ correspond to the left cosets gB where $B = Stab_G(C)$. Thus, a double coset BwB consists of those chambers which lie in the same orbit as wB under the action of B.

Theorem 1.4.27. *Let Δ be a thick building admitting a strongly transitive group G of automorphisms, let $\mathcal{A}$ be as in 1.4.26(ii) and let W be the corresponding Coxeter group. Fix $C \in \mathcal{A}$ and let $B = Stab_G(C)$, $N = Stab_G(\mathcal{A})$. Then (B, N) is a Tits system, and*

$$\delta(C, D) = w \text{ if and only if } D \subseteq BwB$$

where D is taken to be a left coset of B.

Proof. See Theorem 5.2 in [12]. □

The next result also shows that a Tits system in a group G also defines a building.

Theorem 1.4.28. *Every Tits system (B, N) in a group G defines a building (Δ, δ), the chambers being the left cosets of B, with s-adjacency given by*

$$gB \sim_s hB \text{ if and only if } g^{-1}h \in B\langle s \rangle B.$$

Furthermore $\delta(B, gB) = w$ if and only if $gB \subseteq BwB$, N stabilizes an apartment and the action of G is strongly transitive.

Proof. This is Theorem 5.3 in [12]. □

Proposition 1.4.29. *Let Δ, C, $\mathcal{A}$ and B be as in Theorem 1.4.27 and let A be a face of C of cotype J for some $J \subseteq S$. The* stabilizer *of A in G is the parabolic subgroup*

$$P_J = \bigcup_{w \in W_J} BwB = BW_JB.$$

Proof. This is Proposition 6.27 in [1]. □

1.5 The Building of type A_n

Let V be an $(n+1)$-dimensional vector space over a field K. Let Γ be the set consisting of all the proper nontrivial subspaces of V. We call Γ the projective geometry of V of dimension n. A sequence $\{Y_1, \ldots, Y_k\}$ of subspaces in Γ is said to be *nested* if $Y_i \subset Y_{i+1}$ for $1 \leq i \leq k-1$. We also call such a nested sequence a *flag*. We define a chamber system $\mathcal{C} = \mathcal{C}(\Gamma)$ by taking as chambers the maximal flags $\{Y_1, \ldots, Y_n\}$ of Γ with $\dim_K Y_i = i$. Its index set I is the set $\{1, \ldots, n\}$ and we say two chambers $\{Y_1, \ldots, Y_n\}$ and $\{Y_1', \ldots, Y_n'\}$ are i-adjacent if $Y_j = Y_j'$ for all $j \neq i$ and $Y_i \neq Y_i'$. A set $\mathcal{F} = \{L_1, L_2, \ldots, L_{n+1}\}$ consisting of 1-dimensional subspaces of V such that $V = L_1 \oplus \cdots \oplus L_{n+1}$ is called a *frame* in V. An apartment in $\mathcal{C}$ is given by a frame in V. Let $\mathcal{A} = \mathcal{A}(\mathcal{F})$ be an apartment given by the frame $\mathcal{F} = \{L_1, \ldots, L_{n+1}\}$. Then $\mathcal{A}$ consists of all the subspaces of V spanned by a proper subset of $\mathcal{F}$, and all flags of such subspaces. The chambers of this apartment are all the maximal flags consisting of subspaces of V spanned by proper nonempty subsets of $\mathcal{F}$. The associated Coxeter group is the symmetric group S_{n+1} on the set $\{1, 2, \ldots, n+1\}$.

Let $C = \{Y_1, \ldots, Y_n\}$ and $C' = \{Y'_1, \ldots, Y'_n\}$ be two chambers of $\mathcal{C}$ and let $Y_0 = Y'_0 = \{0\}$ and $Y_{n+1} = Y'_{n+1} = V$. Set $\delta(C, C') = \sigma$ where $\sigma = \sigma(C, C')$ is obtained as follows.

$$\sigma(i) = \min\{j \in \{1, \ldots, n+1\} \mid Y'_i \subseteq Y'_{i-1} + Y_j\}.$$

for all $i \in [1, n+1]$. Thus,

(i) $Y'_i \nsubseteq Y'_{i-1} + Y_{j-1}$

(ii) $Y'_i \cap Y_j = (Y'_i \setminus Y'_{i-1}) \cap (Y_j \setminus Y_{j-1})$ is 1-dimensional.

Observe that if $\sigma(i) = \sigma(k) = j$, then $Y_i = Y_{i-1} + \langle v \rangle$ and $Y_k = Y_{k-1} + \langle w \rangle$ where $v, w \in Y'_j \setminus Y'_{j-1}$. Thus v can be written as $v = \lambda w + u$ for some $u \in Y'_{j-1}$. So $i \leq k$ for otherwise, we have that $Y_k \subseteq Y_{i-1}$ and so

$$Y_i = Y_{i-1} + \langle v \rangle = Y_{i-1} + \langle u \rangle \subseteq Y_{i-1} + Y'_{j-1},$$

a contradiction to the minimality of j. By a similar argument, we also get $k \leq i$ and so σ is injective and hence a bijection. Hence σ is a permutation of the set $\{1, 2, \ldots, n+1\}$. Its inverse is the map $\sigma' = \sigma(C', C)$.

Now $\delta(C, C') = \sigma$ if and only if for all $1 \leq i \leq n+1$ there exists $e_i \in Y_i \setminus Y_{i-1}$

such that $e_i \in Y'_j \setminus Y'_{j-1}$ where $\sigma(j) = i$. That is,

$$e_i = e_{\sigma(j)} \in Y'_j \setminus Y'_{j-1}.$$

Evaluating at each $i, j \in \{1, 2, \ldots, n+1\}$, we get a frame

$$\mathcal{F} = \{\langle e_1 \rangle, \langle e_2 \rangle, \ldots, \langle e_{n+1} \rangle\}$$

such that

$$Y_i = \langle e_1 \rangle + \langle e_2 \rangle + \cdots + \langle e_i \rangle$$

and

$$Y'_i = \langle e_{\sigma(1)} \rangle + \langle e_{\sigma(2)} \rangle + \cdots + \langle e_{\sigma(i)} \rangle.$$

In particular, the chambers C and C' are contained in the apartment $\mathcal{A}(\mathcal{F})$ given by this frame. Thus, we have shown that any two chambers lie in a common apartment. This gives rise to an isomorphism $\phi_{C,\mathcal{F}} : S_{n+1} \to \mathcal{A}(\mathcal{F})$ defined by

$$\sigma \mapsto C_\sigma$$

where $C_\sigma := \{L_{\sigma(1)}, L_{\sigma(1)} + L_{\sigma(2)}, \ldots, L_{\sigma(1)} + L_{\sigma(2)} + \cdots + L_{\sigma(n)}\}$. Its inverse is the map $\psi_{C,\mathcal{F}} : \mathcal{A}(\mathcal{F}) \to S_{n+1}$ defined by

$$D \mapsto \delta(C, D).$$

Observe that $\psi_{C,\mathcal{F}}$ does not make any reference to $\mathcal{F}$, only to C. It turns out that if $\mathcal{F}'$ is another frame whose apartment $\mathcal{A}(\mathcal{F})$ contains C, then $\psi_{C,\mathcal{F}}$

and $\psi_{C,\mathcal{F}'}$ agree on $\mathcal{A}(\mathcal{F}) \cap \mathcal{A}(\mathcal{F}')$. It therefore follows that the map

$$\phi_{C,\mathcal{F}'} \circ \psi_{C,\mathcal{F}} : \mathcal{A}(\mathcal{F}) \to \mathcal{A}(\mathcal{F}')$$

is an isomorphism fixing the intersection $\mathcal{A}(\mathcal{F}) \cap \mathcal{A}(\mathcal{F}')$ pointwise. Hence, (C, δ) is indeed a building.

An i-panel (or residue of type i) in this building corresponds to the set of 1-spaces in a 2-space V_{i+1}/V_{i-1}. More generally, if $J = \{j_1, \ldots, j_k\} \subset I$, a residue of cotype J (or of type $I \setminus J$) in this building corresponds to a flag

$$\mathcal{F} = \{Y_{i_1}, Y_{i_2}, \ldots, Y_{i_k}\}.$$

Denote this residue by $\mathrm{Res}(\mathcal{F})$. Its chambers are the maximal flags $C = \{Y_1', \ldots, Y_n'\}$, such that $Y_j' = Y_j$ for all $j \in J$.

Let $C_1 = \{Y_1', \ldots, Y_{j_1-1}'\}$, then C_1 is a chamber in the projective geometry for the space Y_{j_1}. Similarly, the flag

$$C_2 := Y_{j_1+1}'/Y_{j_1} \subset Y_{j_1+2}'/Y_{j_1}' \subset \cdots \subset Y_{j_2-1}'/Y_{j_1}'$$

is a chamber in the geometry for the space Y_{j_2}/Y_{j_1}. In general, the flag

$$C_{m+1} := Y_{j_m+1}'/Y_{j_m} \subset Y_{j_m+2}'/Y_{j_m}' \subset \cdots \subset Y_{j_{m+1}-1}/Y_{j_m}$$

is a chamber in the geometry for the space $Y_{j_{m+1}}'/Y_{j_m}'$, $1 \leq m \leq k$. Thus, each chamber C in $\mathrm{Res}(\mathcal{F})$ corresponds to a k-tuple $(C_1, C_2, \ldots, C_k)$. Moreover, $\mathrm{Res}(\mathcal{F})$ corresponds to the direct product $\Delta_1 \times \Delta_2 \times \cdots \times \Delta_k$ where Δ_i is the projective building on the space $Y_{j_i}/Y_{j,i-1}$, $1 \leq i \leq k$. The stabilizer of the flag $\mathcal{F}$ is the subgroup of the general linear group $\mathrm{GL}_n(K)$ of dimension n over K, consisting of the matrices of the form

$$\left(\begin{array}{c|c|c|c} A_1 & * & * & * \\ \hline 0 & A_2 & * & * \\ \hline 0 & 0 & \ddots & * \\ \hline 0 & 0 & 0 & A_k \end{array}\right),$$

where A_i is an invertible matrix of dimension dim $Y_{j_i}/Y_{j,i-1}$, for $1 \leq i \leq k$.

Chapter 2

Homology and the Steinberg Module

2.1 Simplicial complexes

Definition 2.1.1. *Let X be a set and Δ a collection of (finite) subsets of X, with the property that if $B \in \Delta$ and $A \subseteq B$, then $A \in \Delta$. Furthermore, every singleton subset $\{x\}$ of X lies in Δ. Then we say that Δ is an (abstract)* simplicial complex *with* vertex set X. *The elements of Δ are called* simplices.

A simplex $B = \{x_0, x_1, \ldots, x_q\}$ consisting of $q+1$ vertices is said to be q-*dimensional* and we refer to B as a q*-simplex*. If $A \subseteq B \in \Delta$, then we say A is a *face* of B. The *codimension* of A in B is given as $|B - A|$. If A has codimension 1 in B, then we say A is a *facet* of B. The *dimension* of a simplicial complex Δ is the largest dimension of its simplices. That is,

$$\dim \Delta = max\{\dim A \mid A \in \Delta\}.$$

The relations $A \subseteq B$ holding in a simplicial complex Δ are called the *face relations* of Δ.

Two simplices A and B in Δ are said to be *adjacent* if they have a common facet. A simplex $A \in \Delta$ is said to *maximal* if A is not a proper face of any other simplex in Δ. A simplicial complex Δ is said to be *pure* if it is finite dimensional and every maximal simplex has the same dimension. A *subcomplex* of a simplicial complex Δ is a subset Y of Δ which is a simplicial complex with the face relations from Δ.

Example 2.1.2. *Let Δ be a simplicial complex. For any simplex $B \in \Delta$, the set* $\mathrm{lk}\ B = \{A \in \Delta \mid A \cup B \in \Delta,\ A \cap B = \emptyset\}$ *called the* link *of B is a subcomplex of Δ.*

Throughout the remaining part of this section let Δ be a simplicial complex with vertex set X.

Definition 2.1.3. *Let S be a finite subset of $\mathbb{R}^n$. An* affine combination *of the points $p_i \in S$ is a point $x = \sum \lambda_i p_i$, such that $\lambda_i \in \mathbb{R}$ and $\sum \lambda_i = 1$. The set S is said to be* affinely independent *if no point in S is an affine combination of the other points. A* convex combination *is an affine combination with non-negative coefficients λ_i. The* convex hull $\mathrm{conv}(S)$ *of S is the set of all convex combinations of points in S.*

Definition 2.1.4. *Suppose $X = \{x_1, \ldots, x_n\}$. Let e_i be the i-th unit coordinate vector in $\mathbb{R}^n$. For any subset $A \subseteq X$, define*

$$|A| = \mathrm{conv}\{e_i \mid x_i \in A\}.$$

So if A is a q-simplex in Δ, then $|A|$ is called a geometric *q-simplex in $\mathbb{R}^n$. We define the* geometric realization *$|\Delta|$ of the simplicial complex Δ to be*

$$|\Delta| = \bigcup_{A \in \Delta} |A|.$$

Thus $|\Delta|$ inherits from the topology on $\mathbb{R}^n$ the structure of a topological space. If Y is any topological space homeomorphic to $|\Delta|$, then we call Δ a *triangulation* of Y.

Definition 2.1.5. *Let Δ be a simplicial complex. Then Δ is a* chamber complex *if it satisfies the following conditions.*

(i) Every simplex is contained in a maximal simplex.

(ii) For any two maximal simplices $A, B \in \Delta$, there is a gallery connecting A to B.

The maximal simplices in Δ are called chambers *of Δ.*

Observe that the maximal simplices in a chamber complex Δ all have the same dimension. This follows from condition (ii) above. Thus, if Δ is finite dimensional then Δ is pure.

Definition 2.1.6. *Let $\mathcal{S} = (X, \Delta)$ and $\mathcal{S}' = (X', \Delta')$ be two simplicial complexes. A* morphism *from $\mathcal{S}$ to $\mathcal{S}'$ is a map from X to X' which takes simplices to simplices.*

Definition 2.1.7. *Let G be a finite group. We say that G* acts *on Δ if G acts on the vertices of Δ and if the action of G takes simplices to simplices. We call Δ a G-*complex *in this case.*

2.2 Homology

Definition 2.2.1. *A* differential group *is a pair* (C, ∂) *consisting of an abelian group* C *and an endomorphism* $\partial : C \to C$ *satisfying* $\partial\partial = 0$. *The endomorphism* ∂ *is called the* differential *or* boundary operator *of the differential group.*

The elements of $\text{Ker}\partial$ are called *cycles* and those of $\text{Im}\partial$ are called *boundaries*, and the requirement that $\partial\partial = 0$ implies $\text{Im}\partial \subseteq \text{Ker}\partial$. The quotient group $H(C)$ defined by

$$H(C) = Ker\partial/\text{Im}\partial$$

is called the *Homology group* of C. The elements of $H(C)$ are called *homology classes*, two cycles being *homologous* if they lie in the same homology class.

Definition 2.2.2. (Chain Complex) *A* chain complex C *over a ring* K *is a family* $\{C_q, \partial_q\}$, $q \in \mathbb{Z}$, *of abelian groups* C_q *and homomorphisms* $\partial_q : C_q \to C_{q-1}$ *such that* $\partial_q\partial_{q+1} = 0$.

The elements of C_q are the *q-chains* of the complex. If $C_q = 0$ for $q < 0$, we say the complex is *nonnegative*. A *free chain complex* is a chain complex in which C_q is free abelian for all q. Again the condition that $\partial_q\partial_{q+1} = 0$ implies $\text{Im}\partial_{q+1} \subseteq \text{Ker}\partial_q$. The homology group $H(C)$ consists of the family $\{H_q(C) = \text{Ker}\partial_q/\text{Im}\partial_{q+1}\}$ of quotient groups.

We now turn attention to chain complexes defined over a simplicial complex.

Throughout the remaining part of this section, let Δ be a simplicial complex. An *ordered q-simplex* of Δ is a sequence $(v_0, v_1, \ldots, v_q)$ of $q + 1$ vertices belonging to some q-simplex of Δ. If $q < 0$ then no ordered q-simplex exists.

Definition 2.2.3. *An* ordered chain complex $C(\Delta)$ *of* Δ *is a family* $\{C_q(\Delta), \partial_q\}$, *where* $C_q(\Delta)$ *is the free abelian group generated by the ordered q-simplexes of* Δ *and* ∂_q *is given by the equation*

$$\partial_q(v_0, v_1, \dots, v_q) = \sum_{0 \le i \le q} (-1)^i (v_0, \dots, \hat{v}_i, \dots, v_q),$$

where $(v_0, \dots, \hat{v}_i, \dots, v_q)$ *denotes the ordered* $(q-1)$*-simplex obtained by deleting the* i^{th} *vertex* v_i.

If $q < 0$ then $C_q(\Delta) = 0$ and so the ordered chain complex is also a free nonnegative chain complex. A chain complex $C = \{C_q, \partial_q\}$ is said to be *finitely generated* if C_q is finitely generated for all q and $C_q = 0$ for all but finitely many integers q. If C is finitely generated then $H(C)$ is also finitely generated.

Definition 2.2.4. (Reduced Homology) *We define the* augmented chain complex $\tilde{C}(\Delta)$ *of* Δ *by setting* $\tilde{C}_q(\Delta) = C_q(\Delta)$ *for* $q \ge 0$ *and* $\tilde{C}_q(\Delta) = \mathbb{Z}$ *for* $q = -1$. *Define* $\partial_0(v) = 1$ *for each vertex* v. *The reduced homology* $\tilde{H}_q(\Delta)$ *is the homology of* $\tilde{C}_q(\Delta)$.

We shall be interested in complexes which satisfy the well-known Cohen-Macaulay property. Recall that the link lk F of a simplex F in Δ is the subcomplex lk $F = \{E \in \Delta \mid E \cup F \in \Delta, \text{ and } E \cap F = \emptyset\}$. Let K denote the ring of integers $\mathbb{Z}$ or a field $\mathbb{F}$.

Definition 2.2.5. (Cohen- Macaulay) *A simplicial complex* Δ *is said to be* Cohen-Macaulay *over* K *if* $\tilde{H}_i(\text{lk } F, K) = 0$ *for all* $F \in \Delta$ *and* $i < \dim(\text{lk } F)$.

Definition 2.2.6. *Let G be a finite group. We say that G acts on a chain complex $C = \{C_q, \partial_q\}$ over K if each C_q is a finite dimensional KG-module and if ∂_q commutes with the action of G. If G acts on C then the homology spaces $\{H_q(C)\}$ are also KG-modules affording what we refer to as the* homology representations *of G.*

2.3 The Solomon-Tits Theorem

In this section, we collect some results on homology representation of groups and the Steinberg module. We also state the well-known Solomon-Tits theorem as given in [7].

Definition 2.3.1. *Let (W, S) be a finite Coxeter system with $|S| \geq 2$. Let Γ be the partially ordered set (poset), referred to as the W-poset, consisting of all the left cosets*

$$\{wW_J \mid w \in W \text{ and } J \subset S\},$$

ordered by inclusion. We call Γ the Coxeter poset*, and the action of W on Γ is given by left translation. That is, for $x \in W$,*

$$wW_J \mapsto xwW_J,$$

for all $w \in W$ and $J \subset S$.

Definition 2.3.2. *Let (W, S) be a finite Coxeter system. The* sign representation *ε of W is the representation $\varepsilon : W \to \mathbb{Q}$ of degree 1, given uniquely by*

$$\varepsilon(s) = -1 \text{ for all } s \in S.$$

We have the following results.

Theorem 2.3.3. *Let V be a finite dimensional vector space over the real field $\mathbb{R}$, let Φ be a root system in V and let (W, S) be the Coxeter system associated with Φ. Thus $W = W(\Phi)$ (see Theorem 1.2.8) and S is the set of reflections associated with a fundamental system $\Pi \subseteq \Phi$. Let $n = |S| = \dim V$ and suppose $n \geq 2$. Then the following statements hold:*

(i) The group W acts on the unit sphere $S^{n-1} = \{v \in V \mid \| v \| = 1\}$ in V and there is a W-equivariant homeomorphism

$$|\Gamma| \simeq S^{n-1}$$

where $|\Gamma|$ denotes the underlying topological space of the Coxeter poset Γ associated with the Coxeter system (W, S).

(ii) The homology representation of W on $H(\Gamma)$ over $\mathbb{Q}$ is the following: $H_i(\Gamma) = 0$ except in dimension 0 and $n-1$. Furthermore, $H_0(\Gamma)$ affords the trivial representation 1_W, while $H_{n-1}(\Gamma)$ affords the sign representation ε.

Proof. See Theorem 66.28 in [7]. □

Theorem 2.3.3 shows that S^{n-1} is the geometric realization $|\Gamma|$ of the W-poset Γ and thus determines the homology representation of W on Γ.

Corollary 2.3.4. *Let ε be the sign character of a finite Coxeter group W. Then*

$$\varepsilon = \sum_{J \subseteq S} (-1)^{|J|} (1_{W_J})^W.$$

Proof. See Corollary 66.29 in [7]. □

Proposition 2.3.5. *The correspondence*

$$\xi = \sum_{J \subseteq S} n_J (1_{W_J})^W \to \hat{\xi} = \sum_{J \subseteq S} n_J (1_{P_J})^G, \ n_J \in \mathbb{Z},$$

defines a mapping of virtual characters of W to virtual characters of G that preserves scalar product. Furthermore,

$$\xi \in IrrW \Rightarrow \pm\hat{\xi} \in IrrG.$$

Proof. This is Proposition 67.9 in [7]. □

We shall now introduce the concept of a combinatorial building. Recall the definition of parabolic subgroups as given in Definition 1.3.6.

Definition 2.3.6. *The* combinatorial building Δ *of a group G with a BN-pair of rank $n > 1$ is the poset of all proper parabolic subgroups P of G, called G-poset, ordered by inclusion, with the G-action given by conjugation:*

$$P \to gPg^{-1}, \ \textit{for } g \in G, P \in \Delta.$$

The statement of the well-known Solomon-Tits theorem which was first proved by L. Solomon in [15] is as follows.

Theorem 2.3.7. *(Solomon-Tits) Let Δ be the combinatorial building of a finite group with a BN-pair of rank $n \geq 2$, and let $H(\Delta) = \{H_q(\Delta) \mid q \geq 0\}$ denote the homology of Δ with coefficients in $\mathbb{Q}$. Then $H_q(\Delta) = 0$ except* *in dimensions $q = 0$ and $q = n - 1$. In these dimensions, $H_0(\Delta)$ affords the trivial representation, while $H_{n-1}(\Delta)$ affords an absolutely irreducible nontrivial representation.*

Definition 2.3.8. *Let G be a group with a BN-pair of rank n and let Δ be the combinatorial building of G. The* Steinberg representation St_G *is the nontrivial absolutely irreducible $\mathbb{Q}$-representation of G afforded by the rational homology group $H_{n-1}(\Delta)$, if $n > 1$. If $n = 1$, it is the unique nontrivial irreducible component of the permutation representation of G afforded by the left cosets G/B.*

We also denote by St_G the character of G afforded by the Steinberg representation.

Theorem 2.3.9. *The character St_G of the Steinberg representation of a finite group G with a BN-pair is given by*

$$\mathrm{St}_G = \sum_{J \subseteq S} (-1)^{|J|} (1_{P_J})^G.$$

Furthermore, $\mathrm{St}_G \in \mathrm{Irr}G$, and deg $St_G = |B : B \cap {}^{w_0}B|$, where w_0 is the unique element of maximal length in W.

Proof. By Corollary 2.3.4, the sign character of W is given by

$$\varepsilon = \sum_{J \subset S} (-1)^{|J|} (1_{W_J})^W.$$

By Proposition 2.3.5, we have that the character St_G is a virtual character such that $\pm\mathrm{St}_G \in \mathrm{Irr}G$. We now wish to calculate $\mathrm{St}_G(1)$ and we use the formula

$$\mathrm{St}_G(1) = \sum_{J \subseteq S} (-1)^{|J|} |G : P_J|.$$

Let $D_{\emptyset J}$ denote the set of distinguished double coset representatives in $B \setminus G/P_J$ (see 1.2.12). By Theorem 1.3.11,

$$G = \dot{\bigcup}_{x \in D_{\emptyset J}} BxP_J.$$

Furthermore, $|BxP_J/P_J| = |B : B \cap {}^xP_J|$, $x \in D_{\emptyset J}$. So we have that

$$|G : P_J| = \sum_{x \in D_{\emptyset J}} |BxP_J/P_J| = \sum_{x \in D_{\emptyset J}} |B : B \cap {}^xP_J|.$$

Recall that $P_J = \bigcup_{w \in W_J} BwB$. We want to show that $B \cap {}^xP_J = B \cap {}^xB$. It suffices to show that

$$xBwBx^{-1} \cap B = \emptyset, \text{ for } 1 \neq w \in W_J, x \in D_{\emptyset J}.$$

This is equivalent to showing that

$$xBwB \cap BxB = \emptyset, \text{ for } x \in D_{\emptyset J},\ w \in W_J,\ w \neq 1.$$

By Proposition 1.2.12, $l(xw) = l(x) + l(w)$ for all $w \in W_J$ and $x \in D_{\emptyset J}$, thus $xBw \subset BxwB$. This implies that $xBwB \cap BxB = \emptyset$ for all $1 \neq w \in W_J$ and $x \in D_{\emptyset J}$ by the uniqueness part of the Bruhat decomposition. So $|G : P_J| = \sum_{x \in D_{\emptyset J}} |B : B \cap B^x|$.

Substituting for $|G : P_J|$ in the formula for $\mathrm{St}_G(1)$ we have

$$\mathrm{St}_G(1) = \sum_{J \subseteq S} (-1)^{|J|} \sum_{x \in D_{\emptyset J}} |B : B \cap {}^x B|.$$

By Proposition 1.2.12 we have that $x \in W$ belongs to $D_{\emptyset J}$ if and only if $l(xs) > l(x)$ for all $s \in J$. But this happens if and only if $J \subseteq R(x)$ where $R(x) = \{s \in S \mid l(xs) \geq l(x)\}$. Also, if $J = \emptyset$, then $D_{\emptyset\emptyset} = W$. So

$$\begin{aligned} \mathrm{St}_G(1) &= \sum_{J \subseteq S} (-1)^{|J|} \sum_{D_{\emptyset J}} |B : B \cap {}^x B| \\ &= \sum_{x \in W} (\sum_{J \subseteq R(x)} (-1)^{|J|}) |B : B \cap {}^x B|. \end{aligned}$$

Hence for each $x \in W$, we have that $|B : B \cap {}^x B|$ appears in the formula for $\mathrm{St}_G(1)$ precisely $\sum_{J \subseteq R(x)} (-1)^{|J|}$ times. Now if $R(x) \geq 1$, then the alternating sum $\sum_{J \subseteq R(x)} (-1)^{|J|}$ has $2^{|R(x)|}$ terms half of which are positive and the other half negative. It therefore follows that $\sum_{J \subseteq R(x)} (-1)^{|J|} = 0$ in this case. Thus we are left with the case $R(x) = \emptyset$. This happens if and only if $x = w_0$ where w_0 is the unique element of maximal length in W. The contribution of this element to $\mathrm{St}_G(1)$ is $|B : B \cap {}^{w_0} B|$, so $St_G(1) = |B : B \cap {}^{w_0} B|$ completing the proof. $\square$

Chapter 3

Codes

3.1 Linear codes

Throughout this section, let $\mathbb{F}_q$ denote the Galois field with q elements, where q is a prime power, and we write $V(n, q)$ for the n-dimensional vector space over $\mathbb{F}_q$, where n is a positive integer. We shall write $x_1x_2 \cdots x_n$ for the vector $(x_1, x_2, \ldots, x_n)$ and consider linear codes defined over finite fields.

Definition 3.1.1. *(Linear Codes) A* linear code *C over $\mathbb{F}_q$ is a subspace of $V(n, q)$. Thus C is nonempty and satisfies the following properties:*

(i) for all $x, y \in C$, $x + y \in C$; and

(ii) for all $x \in C$ and $\lambda \in \mathbb{F}_q$, $\lambda x \in C$.

The elements of C are called codewords. *The* dimension *of the linear code is defined to be the vector space dimension of C and the* length *of the linear code is given as the dimension of $V(n, q)$. If C is k-dimensional, then C is said to be a* linear (n, k)-code.

Example 3.1.2. *Set $V = V(3,2)$, then V consists of the eight vectors*

$$000, 100, 010, 001, 110, 101, 011, 111.$$

Take C to be the subspace of V given by the basis $\{110, 011\}$. Then C is a linear $(3,2)$-code and consists of the four codewords

$$000, 011, 110, 101.$$

Definition 3.1.3. *The* rate *of a linear (n,k)-code is given as $R = k/n$ and the* redundancy *of the code is $n - k$.*

The rate of the code measures the fraction of the information which is non-redundant.

An important feature of a linear code C is the minimum distance of the code, which is an indicator of the error correcting capability of the code.

Definition 3.1.4. (*Hamming distance*) *The* (Hamming) distance *between two vectors $x, y, \in V(n,q)$ denoted $d(x,y)$, is the number of places at which x and y differ. Thus,*

$$d(x,y) = |\{i \mid x_i \neq y_i\}|.$$

The minimum distance $d(C)$ of a linear code C is given as

$$\min\{d(x,y) \mid x, y \in C\}.$$

Example 3.1.5. *Let $V(3,2)$ and C be as in Example 3.1.2, then $d(101, 111) = 1$ and $d(C) = 2$.*

Proposition 3.1.6. *The Hamming distance is a metric on $V(n,q)$. That is, for all x, y and w in $V(n,q)$, the following hold.*

(i) $d(x,y) \geq 0$ *and* $d(x,y) = 0$ *if and only if* $x = y$.

(ii) $d(x,y) = d(y,x)$.

(iii) $d(x,y) \leq d(x,w) + d(w,y)$.

Proof. The first two conditions follow immediately from the definition. To verify the third property, observe that $d(x,y)$ is the minimum number of changes required to change x to y. However, we may decide to change x to y by first changing x to w (making $d(x,w)$ changes) and then w to y (making $d(w,y)$ changes). It therefore follows that $d(x,y) \leq d(x,w) + d(w,y)$. □

Definition 3.1.7. *Let $v = (v_1, v_2, \ldots, v_n)$ be a vector in $V(n,q)$. The* support *of v denoted* Supp(v) *is the set $\{i \mid v_i \neq 0\}$, and we define the (Hamming)* weight $w(v)$ *of v to be* $|\mathrm{Supp}(v)|$. *The* minimum weight $w(C)$ *of a linear code C is the minimum of the weights of the non-zero codewords in C.*

It is obvious from the definition that $w(v) = d(0,v)$ for all $v \in V$ and $w(v) = 0$ if and only if $v = 0$. In fact, $d(u,v) = w(u-v) = w(v-u)$ for all $u, v \in V$. This motivates the next result.

Lemma 3.1.8. *Let C be a linear code, then $d(C) = w(C)$.*

Proof. Let $x, y \in C$ such that $d(C) = d(x,y)$. Since $x - y \in C$, we have

$$d(C) = d(x,y) = w(x-y) \geq w(C).$$

Let x be a nonzero codeword in C with $w(x) = w(C)$. Then the vector 0 is a codeword and so

$$w(C) = w(x) = d(x, 0) \geq d(C).$$

The two inequalities yield the desired result. □

Lemma 3.1.9. *Let C be a linear code and let $d = d(C)$. Then C can correct up to $\lfloor (d-1)/2 \rfloor$ errors and detect up to $d-1$ errors.*

Proof. A proof can be found in [3]. □

3.2 Codes from Homology

Let Δ be a (pure) finite simplicial complex of dimension n. We consider the reduced complex over Δ. Let Δ_k denote the set of k-dimensional simplices in Δ, $-1 \leq k \leq n$, where Δ_{-1} consists of the single empty simplex. The kth chain group $C_k = C_k(\Delta)$ is the free $\mathbb{Z}$-module generated by the k-dimensional simplices Δ_k of Δ. We restrict attention to the top dimension n of the complex. Thus, $C_n(\Delta) = \mathbb{Z}(\Delta_n)$ and the associated boundary map ∂_n maps $C_n(\Delta)$ into $C_{n-1}(\Delta)$. The cycle subgroup $Z_n(\Delta)$ is the kernel of ∂_n. As we are in the top dimension, $\partial_{n+1} = 0$, so the homology group $H_n(\Delta) = Z_n(\Delta)$.

For linear codes, we wish to go from $\mathbb{Z}$-modules to modules over some finite field K. The modules defined in this way are in fact vector spaces over the field K. We restrict attention to the case $K = \mathbb{F}_2$, the field with 2 elements, and define the groups $C_n(\Delta, \mathbb{F}_2)$ and $Z_n(\Delta, \mathbb{F}_2)$ over $\mathbb{F}_2$ analogously. By the universal coefficient theorem, we have that the groups over $\mathbb{F}_2$ can be obtained from the groups over $\mathbb{Z}$ by tensoring with $\mathbb{F}_2$. Let $\overline{C_n}$ and $\overline{Z_n}$ denote the spaces over $\mathbb{F}_2$ obtained under this map. So, for instance, if $x \in C_n$, then $x = \sum_{c\in\Delta_n} f_c(x) \cdot c$ with coeficients $f_c(x) \in \mathbb{Z}$, and its image $\overline{x}$ in $\overline{C_n}$ is $\sum_{c\in\Delta_n} \overline{f_c(x)} \cdot c$, with coefficients $\overline{f_c(x)} \in \mathbb{F}_2$.

Again, the n-dimensional simplices Δ_n are the standard basis of the $\mathbb{F}_2$-space $\overline{C_n}$. Since Δ is finite, Δ_n is also finite and so C_n is finite dimensional. So, in the language of coding theory, we may identify each element $\overline{x} \in \overline{C_n}$ with the vector of coefficients $\overline{f_c(x)}$, a word in the alphabet $\mathbb{F}_2 = \{0, 1\}$. As $\overline{Z_n}$ is a subspace of $\overline{C_n}$, it follows that $\overline{Z_n}$ is a linear code. We call it the *cycle code* of Δ. The following result is immediate from the definition of linear codes.

Lemma 3.2.1. *The cycle space* $\overline{Z_n}$ *is a linear code in* $\overline{C_n}$ *with length* $\dim \overline{C_n} = |\Delta_n|$ *and dimension* $\dim \overline{Z_n}$.

In general, the dimension of the cycle code can be obtained by linear-algebraic calculations involving the boundary map ∂. However, if Δ is Cohen-Macaulay, then the cycle code is given by the reduced Euler characteristic. Hence we have the following result.

Lemma 3.2.2. *Suppose* Δ *is Cohen-Macaulay. Then the dimension of the cycle code is given by the reduced Euler characteristic*

$$\tilde{\chi}(\Delta) = \sum_{i=0}^{n+1} (-1)^i |\Delta_{n-i}|,$$

where $|\Delta_{-1}| = 1$ *by convention.*

Proof. Since Δ is Cohen-Macaulay, reduced homology vanishes away from top dimension and this happens in the link of every simplex in Δ. Now

$\emptyset \in \Delta$ and $\mathrm{lk}(\emptyset) = \Delta$, so we have $\dim \tilde{H}_i(\Delta) = 0$ for all $i < n$. In particular, $\mathrm{Ker}\partial_i = \mathrm{Im}\partial_{i+1}$ for $0 \leq i < n$. Thus,

$$\begin{aligned}
\dim Z_n &= \dim C_n - \dim \mathrm{Im}\partial_n \\
&= \dim C_n - \dim C_{n-1} + \dim \mathrm{Im}\partial_{n-1} \\
&= \dim C_n - \dim C_{n-1} + \cdots - \dim C_1 + \dim C_0 - \dim \mathrm{Im}\partial_0 \\
&= \dim C_n - \dim C_{n-1} + \cdots - \dim C_1 + \dim C_0 - 1 \\
&= |\Delta_n| - |\Delta_{n-1}| + \cdots - |\Delta_1| + |\Delta_0| - |\Delta_{-1}| \\
&= \sum_{i=0}^{n+1} (-1)^i |\Delta_{n-i}| \\
&= \tilde{\chi}(\Delta).
\end{aligned}$$

□

As with any code, an important feature of the cycle code is the minimal weight. We may identify a chain vector $\bar{x} \in \overline{C}$ with the set of those chambers $c \in \Delta_n$ such that the coefficient $f_c(\overline{x})$ is non-zero. Then the Hamming weight of $\overline{x}$ coincides with the size $|\overline{x}|$ regarded as a set. Thus, we have the following result.

Lemma 3.2.3. *The minimal weight of the cycle code $\overline{Z_n}$ is given by*

$$\min_{0 \neq \overline{z} \in \overline{Z_n}} |\overline{z}|.$$

3.3 Smith-Yoshiara

In [14], Smith and Yoshiara explore a byproduct of the action of groups on geometries, namely the definition of the associated linear codes using elementary topology. In this section, we take a close look at their method on defining codes based on buildings and collect some results.

Let $G = G(q)$ be an (untwisted) Chevalley group of rank $n+1$ over the finite field $\mathbb{F}_q$ with q elements. It is a well known fact that G has a Tits' system (details can be found in [4]). Let B denote the Borel subgroup of G, and let W be the associated Weyl group with generating set S and l its length function. By Theorem 1.4.28, this Tits' system defines a building (Δ, δ) with chambers gB, $g \in G$. Furthermore, the Bruhat decomposition partitions these cosets into double cosets: $gB \subseteq BwB$ if and only if $\delta(B, gB) = w$. We have the following results.

Proposition 3.3.1. *For each $w \in W$ the number of cosets in BwB is $q^{l(w)}$.*

Proof. Let C be the chamber stabilized by the Borel subgroup B. Consider the set

$$\mathcal{A}_w^C = \{D \in \Delta \mid \delta(C, D) = w\}.$$

By Theorem 1.4.28, $\delta(C, D) = w$ if and only if $D \subseteq BwB$. Thus the number of cosets in BwB is $|\mathcal{A}_w^C|$. Let $w = s_1 \cdots s_n$ be a reduced decomposition of w (so $l(w) = n$). Then, for each $D \in \mathcal{A}_w^C$, there is a unique minimal gallery of type $\mathbf{s} = (s_1, \ldots, s_n)$ connecting C and D by Definition 1.4.1 and Lemma 1.4.5(ii). Thus, $|\mathcal{A}_w^C|$ is equal to the number of such minimal galleries.

Let $\Gamma = (C_0, \ldots, C_n)$ be a minimal gallery of type $\mathbf{s}$ connecting C and D.

Then $C = C_0$, $C_n = D$ and $\delta(C_{i-1}, C_i) = s_i$. Furthermore, $l(s_1 \cdots s_i) > l(s_1 \cdots s_{i-1})$ and so $\delta(C_0, C_i) = s_1 \cdots s_i$ for all $1 \leq i \leq n$ (by 1.4.3). Now each panel contains $q+1$ chambers, it therefore follows that there are exactly q choices for each C_i, $1 \leq i \leq n$ and so $|\mathcal{A}_w^C| = q^n = q^{l(w)}$. □

This gives us a formula for the length of the cycle code in terms of q and W. That is,

$$|\Delta_n| = \sum_{w \in W} q^{l(w)}.$$

In [15], Solomon describes the cycle space Z_n in the so called Solomon-Tits theorem. In particular, the proof of that theorem shows that Δ is Cohen-Macaulay. Thus the dimension of the code is given by the reduced Euler characteristic.

Lemma 3.3.2. *The dimension of the cycle code $\overline{Z_n}$ is q^m, where $m = l(w_0)$ and w_0 is the unique element of maximal length in W .*

Proof. Since Δ is Cohen-Macaulay, the cycle code is given by the reduced Euler characteristic by Lemma 3.2.2. Observe that if $J \subseteq S$, then

$$|\Delta_k| = \sum_{|J|=|S|-(k+1)} |G : P_J|,$$

by the Orbit-Stabilizer theorem, since the action of G on Δ is transitive. Thus we may rewrite Lemma 3.2.2 as $\sum_{J \subseteq S} (-1)^{|J|} |G : P_J|$. By Proposition 2.3.9,

$$\sum_{J \subseteq S} (-1)^{|J|} |G : P_J| = |B : B \cap {}^{w_0}B|.$$

Observe that $|B : B \cap {}^{w_0}B|$ is precisely the number of left cosets gB in the double coset Bw_0B. Hence

$$\dim \overline{Z_n} = |B : B \cap {}^{w_0}B| = q^m.$$

□

Let us identify the group B with the actual chamber in Δ_n it stabilizes. Then an apartment is given by the set of Weyl group translates $\{wB \mid w \in W\}$. Denote this apartment by A. Then the apartment A is a subcomplex of Δ. We shall show that the minimal weight of the code is given by apartments.

Proposition 3.3.3. *Let A be as above and let $z_A = \sum_{w\in W}(-1)^{l(w)}wB \in C_n(A)$. Then $z_A \in Z_n(A)$.*

Proof. Since the apartment A is isomorphic to the Weyl group W it is enough to prove the result for $z_W = \sum_{w\in W}(-1)^{l(w)}w$. We want $\partial(z_W) = \sum_{w\in W}(-1)^{l(w)}\partial(w) = 0$. Recall that panels in W are of the form $\{w, ws\}$ for $w \in W$ and $s \in S$. Let $S = \{s_1, \ldots, s_k\}$, then

$$\partial(w) = \sum_{i=1}^{k}(-1)^i\{w, ws_i\}.$$

Now consider $\partial(ws_i) = \sum_{j=1}^{k}(-1)^j\{ws_i, ws_is_j\}$. At the point $j = i$, $\partial(w)$ and $\partial(ws_i)$ coincide, and since W is a thin building, each panel $\{w, ws_i\}$ appears exactly twice in $\partial(z_W)$, once in $\partial(w)$ and once in $\partial(ws_i)$. Furthermore, their coefficients in $\partial(z_W)$ have different signs and so the panel $\{w, ws_i\}$ in $\partial(w)$ and $\partial(ws_i)$ cancel out, yielding the desired result. □

Notice that $|z_A| = |W|$ implies that the minimal weight of our cycle code is at most $|W|$.

Lemma 3.3.4. *The cycle code $\overline{Z_n}$ of the building Δ has minimal weight $|W|$.*

Proof. We already know that the minimal weight of the cycle code is at most $|W|$, it only remains to show that it is at least $|W|$. Pick $\overline{z} \in \overline{Z_n}$ such that $\overline{z} \neq 0$. By the universal coefficient theorem, $\overline{z}$ is the image of $z \in Z_n$. Since $\overline{z_n} \neq 0$, there is some chamber C in $\overline{z}$ viewed as a set. By chamber transitivity and on conjugating appropriately if necessary, we may assume $C = B$. Thus, $f_B(z) \notin 2\mathbb{Z}$.

Let $\alpha : W \to \Delta$ be an isometry given by $w \mapsto wB$, so in particular, $\alpha(1) = B$ and $\alpha(W) = A$. (Recall that $\delta(B, gB) = w$ if and only if $gB \subset BwB$.) The retraction map $\rho = \rho_{B,A} : \Delta \to A$ defined by $\rho(gB) = \alpha(\delta(B, gB))$ maps all the left cosets in BwB to the coset wB, and so maps $C_n(\Delta)$ into $C_n(A)$. Furthermore, ρ is a morphism of the complexes Δ and A and so commutes with the corresponding boundary maps ∂ of Δ and A. In particular, ρ maps $Z_n(\Delta)$ into $Z_n(A)$. Now A is a triangulation of an n-sphere and so $Z_n(A)$ is one dimensional. By Proposition 3.3.3, $z_A \in Z_n(A)$ and so must span this space. We get similar results over $\mathbb{F}_2$ using the Universal Coefficient theorem, in particular, $\overline{Z_n(A)}$ is one dimensional. Since ρ is linear on the chain spaces, the coefficient of $\rho(B)$ in the image $\rho(z)$ is just $f_B(z) \notin 2\mathbb{Z}$, so $\overline{\rho(z)}$ is a non-zero cycle in $\overline{Z_n(A)}$. Now $\overline{z_A}$ is also in $\overline{Z_n(A)}$ and $\overline{Z_n(A)}$ is a one dimensional $\mathbb{F}_2$-space and so contains a unique nonzero element. Thus, we must have that $\rho(z) = \overline{z_A}$. Since $\overline{z_A}$ is simply the sum of the chambers wB of A, we must have that the original preimage $\overline{z}$ before retraction must have at least one chamber in each double coset BwB, and hence $|\overline{z}| \geq |W|$.

completing the proof. $\square$

Chapter 4

Unitary spaces and the Unitary group

Throughout this chapter let $\mathbb{F}_{q^2}$ denote the finite field $\mathrm{GF}(q^2)$ with q^2 elements, where q is a power of a prime. The field $\mathbb{F}_{q^2}$ may be viewed as the splitting field of the polynomial $x^{q^2} - x$. It is well known that the multiplicative group $\mathbb{F}_{q^2}^* = \mathbb{F}_{q^2} \setminus \{0\}$ is cyclic.

Let V be an n-dimensional vector space over the finite field $\mathbb{F}$ and let $\sigma \in \mathrm{Aut}(\mathbb{F})$ be an involution such that $\sigma(a) = \overline{a} = a^q$ for all $a \in \mathbb{F}$. We say that V is equipped with a *hermitian form* $(\ ,\ ) : V \times V \to \mathbb{F}$ if for all $u, v, w \in V$ and $\alpha \in \mathbb{F}$, w e have the following:

(i) $(u + v, w) = (u, w) + (v, w)$,

(ii) $(\alpha u, v) = \alpha(u, v)$,

(iii) $(u, v) = \overline{(v, u)}$.

We shall refer to (v, v) as the norm of v. A non-zero vector $v \in V$ is said to be *isotropic* if $(v, v) = 0$. For any subspace W of V, we define

$W^{\perp} = \{v \in V \mid (v,u) = 0 \text{ for all } u \in W\}$. The hermitian form $(\ ,\ )$ is said to be *non-degenerate* if $\mathrm{Rad}(V) = \{v \in V \mid (v,u) = 0 \text{ for all } u \in V\} = \{0\}$. It is said to be *degenerate* otherwise. A non-degenerate hermitian form is a *unitary form.* A vector space endowed with a unitary form is called a *unitary space.*

From now on, let V be a finite dimensional unitary space over $\mathbb{F}$ and $(\ ,\ )$ be the unitary form on V.

Proposition 4.0.5. *There are non-isotropic vectors $v \in V$.*

Proof. Suppose not, then for all $v \in V$, $(v,v) = 0$. Thus,

$$\begin{aligned} 0 &= (u+v, u+v) \\ &= (u,u) + (u,v) + (v,u) + (v,v) \\ &= (u,v) + (v,u). \end{aligned}$$

This implies

$$(u,v) = -(v,u) = -\overline{(u,v)} \tag{4.1}$$

for all $u, v \in V$. Let $\alpha \in A = \{\gamma \in \mathbb{F} \mid \overline{\gamma} = -\gamma\}$. Then for any $a \in \mathbb{F}$, $\overline{a\alpha} = \bar{a}\bar{\alpha} = -\bar{a}\alpha = -a\alpha$ if and only if $a \in \mathbb{F}^{\sigma}$. Let $a \in \mathbb{F} \setminus \mathbb{F}^{\sigma}$. Using (4.1) we have,

$$\begin{aligned} a(u,v) = (au, v) &= -\overline{(au,v)} \\ &= -\overline{a}\overline{(u,v)} \\ &= \overline{a}(u,v). \end{aligned}$$

Since $a \notin \mathbb{F}^\sigma$, we must have that $(u,v) = 0$ for all $u, v \in V$, a contradiction to the fact that V is non-degenerate. Thus, there exists $v \in V$ such that $(v,v) = a \neq 0$. Furthermore, $a \in \mathbb{F}^\sigma$ since for all $v \in V$, $(v,v) = \overline{(v,v)}$ implies $(v,v) \in \mathbb{F}^\sigma$. $\square$

Definition 4.0.6. *The subset* $\mathbb{F}^\sigma = \mathrm{Fix}(\sigma) = \{\alpha \in \mathbb{F} \mid \overline{\alpha} = \alpha\}$ *of* $\mathbb{F}$ *is called the* fixed subfield *of the automorphism* σ*.*

It can be easily shown that the field $\mathrm{GF}(q)$ is the fixed subfield of $\mathbb{F}$ under the action of σ. Thus, we shall simply refer to the field $\mathrm{GF}(q)$ instead of $\mathbb{F}^\sigma$.

Definition 4.0.7. *The* norm $N : \mathbb{F} \to \mathrm{GF}(q)$ *is defined by* $N(\alpha) = \alpha\overline{\alpha}$ *for all* $\alpha \in \mathbb{F}$*.*

Proposition 4.0.8. *The norm function* N *satisfies the following properties:*

(i) $N(\alpha\beta) = N(\alpha)N(\beta)$ *for all* $\alpha, \beta \in \mathbb{F}$*;*

(ii) N *is surjective.*

Proof. It is clear from the definition of the norm that (i) holds. Observe that $N(\alpha) = 0$ if and only if $\alpha = 0$, so we may consider the map $N : \mathbb{F}^* \to \mathrm{GF}(q)^*$. Property (i) implies that N is a group homomorphism. The kernel

$$\mathrm{Ker}(N) = \{\alpha \in \mathbb{F} \mid \alpha\overline{\alpha} = \alpha^{q+1} = 1\}.$$

If $\alpha \in \mathrm{Ker}(N)$, then α is a root of the polynomial $x^{q+1} - 1 = 0$. Since this polynomial has at most $q+1$ solutions, we have that $|\mathrm{Ker}(N)| \leq q+1$. Using the first isomorphism theorem, we have $|\mathrm{Im}(N)| = |\mathbb{F}^*|/|\mathrm{Ker}(N)| \geq \frac{q^2-1}{q+1} = q-1$. Since $\mathrm{Im}(N) \leq \mathrm{GF}(q)^*$ which has $q-1$ elements, it follows that $|\mathrm{Im}(N)| = q-1$ and $|KerN| = q+1$. Thus, $\mathrm{Im}(N) = \mathrm{GF}(q)^\star$ and N is surjective. $\square$

Corollary 4.0.9. *The field* $\mathrm{GF}(q) = \{\alpha\overline{\alpha} \mid \alpha \in \mathbb{F}\}$.

Proof. The result follows from Proposition 4.0.8 since

$$\mathrm{GF}(q)^* = \mathrm{Im}(N) = \{\alpha\overline{\alpha} \mid \alpha \in \mathbb{F}^*\}.$$

$\square$

Corollary 4.0.10. *For every* $\alpha \in \mathbb{F}^*$*, there are precisely* $q+1$ *elements* $\beta \in \mathbb{F}^*$ *such that* $\beta\overline{\beta} = \alpha\overline{\alpha}$*. In particular, for every* $\lambda \in \mathrm{GF}(q)^*$*, there are precisely* $q+1$ *elements* $\beta \in \mathbb{F}^*$ *such that* $N(\beta) = \lambda$*.*

Proof. Consider the homomorphism $N : \mathbb{F}^* \to \mathrm{GF}(q)^*$. Let the isomorphism $\phi : \mathbb{F}^*/\mathrm{Ker}(N) \to \mathrm{GF}(q)^*$ be defined by $\beta\mathrm{Ker}(N) \mapsto \beta\overline{\beta}$ for all $\beta \in \mathbb{F}^*$. Since ϕ is an isomorphism, it follows that $\alpha\overline{\alpha} = \beta\overline{\beta}$ for all α in the coset $\beta\mathrm{Ker}(N)$. Thus, the elements of the coset $\beta\mathrm{Ker}(N)$ are precisely the $q+1$ elements in $\mathbb{F}^*$ which have the same norm as β. In particular, if $\beta\overline{\beta} = \lambda$ then $\alpha\overline{\alpha} = \lambda$ for all $\alpha \in \beta\mathrm{Ker}(N)$. $\square$

Definition 4.0.11. *Consider* $\mathbb{F}$ *as a vector space over* $\mathrm{GF}(q)$*. The map* $\mathrm{Tr} : \mathbb{F} \to \mathrm{GF}(q)$ *defined by* $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$ *is called the* trace *map.*

Proposition 4.0.12. *For every element* $\lambda \in \mathrm{GF}(q)$*, there are precisely* q *elements* $\alpha \in \mathbb{F}$ *such that* $\mathrm{Tr}(\alpha) = \lambda$*.*

Proof. Observe that Tr is $\mathrm{GF}(q)$-linear. Consider the Kernel of the map Tr. If $|\mathrm{KerTr}| = q$, then we are done. Now, since $\mathrm{ImTr} \leq \mathrm{GF}(q)$, We have that either $\mathrm{Tr} \equiv 0$ or Tr is surjective. If $\mathrm{Tr} \equiv 0$ then $\overline{\alpha} = -\alpha$ for all $\alpha \in \mathbb{F}$. By the proof of Proposition 4.0.5, considering $\mathbb{F}$ as a vector space over itself, we have that this possibility $\overline{\alpha} = -\alpha$ for all $\alpha \in \mathbb{F}$ does not exist. Thus, Tr is surjective. It follows that $|\mathbb{F}/\mathrm{KerTr}| = q$ which implies that $|\mathrm{KerTr}| = q$. Hence, the q elements of a coset of KerTr all map onto the same unique element in $\mathrm{GF}(q)$. $\square$

Lemma 4.0.13. *The unitary space V over $\mathbb{F}$ admits an orthonormal basis.*

Proof. We first show that V contains elements having norm 1. Let $v \in V$ be such that $v \neq 0$ and $(v, v) = a \neq 0$. Then $a \in \mathrm{GF}(q)$ and for any $\alpha \in \mathbb{F}$, we have $(\alpha v, \alpha v) = \alpha\overline{\alpha}(v, v) = N(\alpha)a$. Since N is surjective, there exists $\alpha \in \mathbb{F}$ such that $N(\alpha) = \frac{1}{a}$. Fix such an α and take $u = \alpha v$, then $(u, u) = 1$.

We proceed by induction on the dimension of V. Again, choose a non-zero vector $v \in V$ having non-zero norm. Without loss of generality, $(v, v) = 1$. Since v is non-degenerate, $\langle v \rangle^{\perp}$ is also non-degenerate. By induction, we have that $\langle v \rangle^{\perp}$ has an orthonormal basis. Thus, this basis together with v yields an orthonormal basis for V. $\square$

Lemma 4.0.14. *Suppose* $\dim V \geq 2$. *Then V contains isotropic vectors.*

Proof. By Lemma 4.0.13, there are non-zero vectors $v_1, v_2 \in V$ such that $(v_i, v_j) = \delta_{ij}$, $i, j \in \{1, 2\}$. Then

$$(\alpha v_1 + \beta v_2, \alpha v_1 + \beta v_2) = \alpha\overline{\alpha} + \beta\overline{\beta} = 0$$

if and only if $\frac{\alpha\overline{\alpha}}{\beta\overline{\beta}} = -1$ if and only if $N(\frac{\alpha}{\beta}) = -1$. Choose $\beta = 1$ and α such that $N(\alpha) = -1$. Set $e = \alpha v_1 + v_2$, then $(e, e) = 0$. $\square$

Definition 4.0.15. *Let the unitary space V be n-dimensional over $\mathbb{F}$. If $n = 2m$ for some m, then a* hyperbolic basis *for V is a basis $\{e_i, f_i\}$, $1 \le i \le m$ such that $(e_i, f_j) = \delta_{ij}$, and $(e_i, e_j) = 0 = (f_i, f_j)$ for all i, j.*
If $n = 2m + 1$, then the basis is required to contain an additional element, g, such that $(g, e_i) = (g, f_i) = 0$ for all i, and $(g, g) = 1$.

Proposition 4.0.16. *The unitary space V over $\mathbb{F}$ admits a hyperbolic basis.*

Proof. Let $n = \dim V$. If n=1, there is nothing to prove. Suppose $n = 2$ and let $e \in V$ such that $e \neq 0$ and $(e, e) = 0$. By Lemma 4.0.14, such an element exists. Observe that $\langle e \rangle^{\perp} \neq V$ since V is non-degenerate. Hence, there is some non-zero vector $v \in V$ such that $(e, v) \neq 0$. Without loss of generality, $(e, v) = 1$. (Indeed, if $(e, v) = a \neq 0$, then $(e, \frac{1}{a}v) = 1$.) Let $u = \alpha e + \beta v$ be a non-zero vector. Then

$$\begin{aligned} (u, u) &= (\alpha e + \beta v, \alpha e + \beta v) \\ &= \alpha\overline{\beta} + \beta\overline{\alpha} + \beta\overline{\beta}(v, v) \\ &= \beta\overline{\beta}(\frac{\alpha}{\beta} + \frac{\overline{\alpha}}{\overline{\beta}} + (v, v)) \\ &= \beta\overline{\beta}(\mathrm{Tr}(\frac{\alpha}{\beta}) + (v, v)). \end{aligned}$$

Since Tr is surjective, there exists $\frac{\alpha}{\beta} \in \mathbb{F}$ such that $\mathrm{Tr}(\frac{\alpha}{\beta}) = -(v, v)$. Set $u = \alpha e + v$ where $\beta = 1$ and α is such that $\mathrm{Tr}(\alpha) = -(v, v)$. Then $(u, u) = 0$. Let $(e, u) = t$ and set $f = \frac{1}{t}u$, then $(e, f) = 1$ and $(f, f) = 0$. Thus, $\{e, f\}$ is a hyperbolic basis for V.

Now suppose $n > 2$, and let $v_1, v_2, \ldots, v_n$ be an orthonormal basis for V. Pair off the basis vectors so that if n is odd, one is left over. Each two dimensional subspace thus formed is a unitary space and hence admits a hyperbolic basis (by the above argument). This yields the desired result. $\square$

4.1 Unitary Groups

Let V be an n-dimensional unitary space over the finite field $\mathbb{F}$ and let f denote the unitary form on V. The *general unitary group* denoted $\mathrm{GU}_n(q)$ is the group of all non-singular linear transformations of V which preserve the unitary form. That is,

$$\mathrm{GU}_n(q) = \{g \in \mathrm{GL}_n(q^2) \mid f(u^g, v^g) = f(u, v) \text{ for all } u, v \in V\}.$$

Remark 4.1.1. *Note that the underlying field of* $\mathrm{GU}_n(q)$ *has* q^2 *elements and not* q *elements.*

Let $\{x_1, x_2, \ldots, x_n\}$ be a basis of V. The matrix $A = (a_{ij})$ of f with respect to this basis is given by $a_{ij} = f(x_i, x_j)$. So $g \in \mathrm{GU}(n, q)$ if and only if $g^t A\overline{g} = A$. Taking determinants, we have that $\det(g) det(\overline{g}) = 1$. It follows that the map

$$\det : \mathrm{GU}_n(q) \to \mathrm{Ker}(N)$$

is onto, where $\mathrm{Ker}(N) = \{\alpha \in \mathbb{F} \mid \alpha\overline{\alpha} = \alpha^{q+1} = 1\}$, as described in the previous section. The *special unitary group* $\mathrm{SU}_n(q)$ is defined to be the Kernel of this map and has index $q + 1$ in $\mathrm{GU}_n(q)$. That is,

$$\mathrm{SU}_n(q) = \{g \in \mathrm{GU}_n(q) \mid \det(g) = 1\}.$$

We wish to determine the order of the groups $GU_n(q)$ and $SU_n(q)$. First, we need the following result.

Lemma 4.1.2. *The unitary space V contains $(q^{n-1} - (-1)^{n-1})(q^n - (-1)^n)$ isotropic vectors and $q^{n-1}(q^n - (-1)^n)$ vectors having norm 1.*

Proof. Let x_n denote the number of isotropic vectors and y_n the number of vectors of norm 1 in V, where $n = \dim(V)$. If $v \in V$ with $f(v, v) = 1$, then $f(\alpha v, \alpha v) = \alpha\overline{\alpha} = N(\alpha)$. It follows that every non-zero norm vector is a multiple of a vector of norm 1. Hence, if $\beta \in \mathrm{GF}(q)^*$, then the number of vectors in V of norm β is y_n. Since there are $q-1$ possible values β can take, we have that

$$|V| = q^{2n} = 1 + x_n + (q-1)y_n. \tag{4.2}$$

Let $v \in V$ be a norm 1 vector and let $u \in v^{\perp}$ and consider the subspace U generated by $\{u, v\}$. The gram matrix of U is given by

$$\begin{pmatrix} 1 & 0 \\ 0 & f(u,u) \end{pmatrix}.$$

If $f(u, u) = 0$, then $f|_U$ is degenerate. It follows that there are as many degenerate 2-spaces containing v as isotropic 1-spaces in $v^{\perp}$. Hence number of degenerate 2-spaces containing v is $\frac{x_{n-1}}{q^2-1}$. Furthermore, for $a, b \in \mathbb{F}$, $f(av + bu, av + bu) = a\overline{a} = 0$ if and only if $a = 0$. So the isotropic vectors in U are the scalar multiples of u. Thus each degenerate 2-space has $q^2 - 1$ isotropic vectors.

If $f(u, u) \neq 0$, then U is non-degenerate. So there are as many non-degenerate 2-spaces containing v as non-isotropic 1-spaces in $u^{\perp}$. If $f(u, u) = 1$, then

$f(\alpha u, \alpha u) = \alpha\overline{\alpha}$. If $\alpha\overline{\alpha} = 1$ then there are $q+1$ choices for α (by Lemma 4.0.8). Thus number of non-degenerate 2-spaces containing v is $\frac{y_{n-1}}{q+1}$. Furthermore, for $a, b \in \mathbb{F}$, we have $f(av+bu, av+bu) = a\overline{a} + b\overline{b} = 0$ if and only if $\frac{a}{b}\frac{\overline{a}}{\overline{b}} = -1$. If $x = \frac{a}{b}$, then $x\overline{x} = -1$, so there are $q+1$ choices for x and for each choice of x and each choice of b we get $a = bx$. So there are $(q^2-1)(q+1)$ choices for the pair (a, b). That is, there are $(q^2-1)(q+1)$ isotropic vectors in a non-degenerate 2-space containing v. Thus,

$$\begin{aligned} x_n &= \frac{x_{n-1}}{q^2-1}(q^2-1) + \frac{y_{n-1}}{q+1}(q^2-1)(q+1) \\ &= x_{n-1} + (q^2-1)y_{n-1}. \end{aligned}$$

So $x_{n+1} = x_n + (q^2-1)y_n$. Substituting for y_n from (4.2) we solve the resulting recurrence relation as follows:

$$\begin{aligned} x_{n+1} &= (q^{2n}-1)(q+1) - qx_n \\ &= (q+1)(q^{2n}-1)(q+1) - q(q+1)(q^{2(n-1)}-1) + q^2x_{n-1} \\ &= (q^2-1)(q^{2n-1}+1) + q^2x_{n-1} \\ &= (q^2-1)(q^{2n-1}+1) + q^2((q+1)(q^{2(n-2)}-1) - qx_{n-2}) \\ &= (q^3+1)(q^{2n-2}-1) - q^3x_{n-2}. \end{aligned}$$

Thus, $x_{n+1} = (q^k - (-1)^k)(q^{2n-(k-1)} - (-1)^{k-1}) + q^kx_{n-(k-1)}$ for all $k < n$. Observe that $x_0 = x_1 = 0$, so when $k = n$, we have

$$x_{n+1} = (q^n - (-1)^n)(q^{n+1)} - (-1)^{n-1}).$$

Thus $x_n = (q^{n-1} - (-1)^{n-1})(q^n - (-1)^n)$. So substituting for x_n in (4.2) we get $y_n = q^{n-1}(q^n - (-1)^n)$. $\square$

The group $\mathrm{GU}_n(q)$ acts regularly on the set of ordered orthonormal bases of V. Hence, the order of $\mathrm{GU}_n(q)$ is equal to the number of ordered orthonormal bases of V, which is the product $y_n y_{n-1} \cdots y_1$. So

$$|\mathrm{GU}_n(q)| = q^{\frac{1}{2}n(n-1)} \Pi_{i=1}^{n} (q^i - (-1)^i).$$

Since the index of the group $\mathrm{SU}_n(q)$ in $\mathrm{GU}_n(q)$ is $q+1$, we also have that

$$|\mathrm{SU}_n(q)| = q^{\frac{1}{2}n(n-1)} \Pi_{i=2}^{n} (q^i - (-1)^i).$$

Chapter 5

Type A_n Phan Codes

Throughout this chapter, let V be an $(n+1)$-dimensional vector space over the finite field $\mathbb{F}_{q^2} = \mathrm{GF}(q^2)$, endowed with a non-degenerate Hermitian form $(\ ,\ )$. Let Δ be the A_n building on V (that is, the projective building on V) viewed as a simplicial complex. Thus, the vertex set of Δ consists of all the proper nontrivial subspaces of V, with incidence given by inclusion. Define a map $\tau : \Delta \to \Delta$ by

$$U^\tau = U^\perp = \{v \in V \mid (u, v) = 0 \text{ for all } u \in U\}.$$

Note that since V is non-degenerate, for every non-degenerate subspace U of V, we have $V = U \oplus U^\tau$. We recall that chambers are maximal simplices in Δ. Let $C = Y_1 \subset \cdots \subset Y_n$ be a chamber in Δ. Then $C^\tau = Y_n^\tau \subset \cdots \subset Y_1^\tau$.

5.1 The Phan geometry of type A_n

In this section, we describe and gather some results about the Phan geometry of type A_n.

Definition 5.1.1. *Let $C = Y_1 \subset \cdots \subset Y_n$ and $C' = Y_1' \subset \cdots \subset Y_n'$ be two chambers in Δ. We say that C and C' are* opposite *if and only if*

$$Y_i \oplus Y'_{n+1-i} = V.$$

Let Γ be the subcomplex of Δ whose vertex set consists of all the subspaces U of V satisfying $U \oplus U^\tau = V$. (This is equivalent to U and U^τ being non-degenerate with respect to the form $(\ , \ )$.) Thus, the vertex set of Γ consists of all the non-degenerate proper subspaces of V. We also require that $\{0\} \in \Gamma$. Furthermore, we say a chamber $C \in \Delta$ belongs to Γ if and only if C and C^τ are opposite. (Note that the possibility C and C^τ are not opposite does arise, for instance, when C consists of degenerate subspaces of V.)

Definition 5.1.2. *The subcomplex Γ described above is called the* Phan geometry of type A_n.

Note that $G = \mathrm{GU}_{n+1}(q)$ acts transitively on the set of k-dimensional non-degenerate subspaces of V by Witt's Lemma. Let U be a non-degenerate subspace of V of dimension k. As $V = U \oplus U^\perp$, the stabilizer G_U of U will also stabilize $U^\perp$. If $\{e_1, e_2, \ldots, e_k\}$ is a basis for U, we can extend it to a basis $\{e_1, e_2, \ldots, e_{n+1}\}$ for V by choosing $\{e_{k+1}, \ldots, e_{n+1}\}$ to be a basis for $U^\perp$. Then, G_U consists of matrices having the shape

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

where A_1 and A_2 are non-singular $k \times k$ and $(n-k+1) \times (n-k+1)$ unitary matrices, respectively. Thus, $G_U \cong \mathrm{GU}_k(q) \times \mathrm{GU}_{n-k+1}(q)$.

If $C = Y_{k_1} \subset Y_{k_2} \subset \cdots \subset Y_{k_l}$ is a simplex of Γ with $\dim Y_{k_i} = k_i$, then the stabilizer G_C of C consists of matrices having the shape

$$\begin{pmatrix} A_{k_1} & & & 0 \\ & A_{k_2} & & \\ & & \ddots & \\ 0 & & & A_{k_{l+1}} \end{pmatrix},$$

such that A_{k_1}, A_{k_i}, for $2 \leq i \leq l$, and $A_{k_{l+1}}$ are non-singular $k_1 \times k_1$, $(k_i - k_{i-1}) \times (k_i - k_{i-1})$ and $(n-k_l+1) \times (n-k_l+1)$ unitary matrices, respectively. So $G_C \cong \mathrm{GU}_{k_1}(q) \times \mathrm{GU}_{k_2-k_1}(q) \times \cdots \times \mathrm{GU}_{n-k_l+1}(q)$.
We summarize the above remarks about the stabilizers of a vertex and simplex of Γ in the following proposition.

Proposition 5.1.3. *Let U be a vertex of Γ with $\dim U = k$. Then its stabilizer $G_U \cong \mathrm{GU}_k(q) \times \mathrm{GU}_{n-k+1}(q)$. Suppose $C = Y_{k_1} \subset Y_{k_2} \subset \cdots \subset Y_{k_l}$ is a simplex of Γ, with $\dim Y_{k_i} = k_i$. Then its stabilizer*

$$G_C \cong \mathrm{GU}_{k_1}(q) \times \mathrm{GU}_{k_2-k_1}(q) \times \cdots \times \mathrm{GU}_{k_l-k_{l-1}}(q) \times \mathrm{GU}_{n-k_l+1}(q).$$

Bennett and Shpectorov showed in [5] that the unitary group $SU_{n+1}(q)$ acts transitively on the set of chambers in Γ. Thus, by the Orbit-Stabilizer theorem, the following lemma is immediate.

Lemma 5.1.4. *Let C be a chamber in Γ. Then the number of chambers in*

Γ *is* $|G : G_C|$, *where* $G = \mathrm{SU}_{n+1}(q)$ *and* G_C *denotes the stabilizer in* G *of* C.

5.2 The Phan Code

As in the building case, we adopt the methods of Smith and Yoshiara in defining linear codes based on Γ. We restrict attention to the top dimension $n-1$ of Γ. Let Γ_i denote the set of i-dimensional simplices in Γ. The top dimensional chain space $C_{n-1}(\Gamma)$ is the module $\mathbb{Z}[\Gamma_{n-1}]$ on the basis given by the chambers Γ_{n-1} of Γ, the cycle space $Z_{n-1}(\Gamma)$ is just the kernel of the boundary map $\partial = \partial_{n-1}$ and the homology group $H_{n-1}(\Gamma) = Z_{n-1}(\Gamma)$. We also denote by $\overline{Z_{n-1}(\Gamma)}$ and $\overline{C_{n-1}(\Gamma)}$ the spaces in $\mathbb{F}_2$ obtained from those over $\mathbb{Z}$ by tensoring with $\mathbb{F}_2$.

Since the group $SU_{n+1}(q)$ acts chamber transitively on Γ, it also acts on the cycle space $Z_{n-1}(\Gamma)$. In fact, $Z_{n-1}(\Gamma)$ provides a representation for the group $SU_{n+1}(q)$ with respect to Γ. We therefore refer to it as the *Phan module.* In similar vein, we refer to the corresponding cycle code $\overline{Z_{n-1}(\Gamma)}$ as the *Phan code.* This makes the cycle space $Z_{n-1}(\Gamma)$ an interesting module for the group $SU_{n+1}(q)$. Our aim is to study the components of the Phan module and hence the Phan code. First, we fix some terminology.

Terminology 5.2.1. *We call a vertex* $x \in \Delta$ bad *(for the geometry* Γ*) if* $x \notin \Gamma$*; we say* x *is* good *otherwise. Similarly, we call a chamber* $D \in \Delta$ bad *if at least one of its vertices is bad, and we say* D *is* good *otherwise. Finally, an apartment* $\mathcal{A} \in \Delta$ *will be called* bad *if* $\mathcal{A}$ *contains a bad chamber; we say* $\mathcal{A}$ *is* good *otherwise.*

With this terminology, we can say an apartment $\mathcal{A}$ belongs to Γ if $\mathcal{A}$ is good.

(Strictly speaking, Γ does not contain any apartment as it is not a building.)

Lemma 5.2.2. *Fix a chamber $C \in \Gamma$ and a (good) apartment $\mathcal{A}$ containing C. Let $\phi = \phi_C : \mathcal{A} \to S_{n+1}$ be the isomorphism given by*

$$D \mapsto \delta(C, D) \quad \textit{for all } D \in \mathcal{A}.$$

The element $a_C = \sum_{C' \in \mathcal{A}} sgn(C')C' \in Z_n(\Gamma)$, where

$$sgn(C') = sgn(\phi(C')) = \begin{cases} +1, & \textit{if } \phi(C') \textit{ is even} \\ -1, & \textit{if } \phi(C') \textit{ is odd} \end{cases}$$

Moreover, if $C' \in \mathcal{A}$ then $a_{C'} = \pm a_C$.

Proof. We first show that $a_{C'} = \pm a_C$ for all $C' \in \mathcal{A}$. Let C' be an arbitrary chamber in $\mathcal{A}$. Then by Lemma 1.4.16,

$$\delta(C', C'') = \delta(C', C)\delta(C, C'') \text{ for all } C'' \in \mathcal{A}.$$

Recall that $\delta(C, C') = \delta(C', C)^{-1}$, so $\delta(C, C')$ and $\delta(C', C)$ have the same parity (that is, they're either both even or both odd). Thus, if $\delta(C, C')$ is even, then $\delta(C'C'')$ will be even provided $\delta(C, C'')$ is even, and $\delta(C', C'')$ will be odd if $\delta(C, C'')$ is odd. So $a_{C'} = a_C$ in this case.

Similarly, if $\delta(C, C')$ is odd, then $\delta(C', C'')$ will be odd provided $\delta(C, C'')$ is even, and it will be odd if $\delta(C, C'')$ is even. Thus, $a_{C'} = -a_C$ in this case.

Now $\partial(a_C) = \sum_{C' \in \mathcal{A}} sgn(C')\partial(C')$, and for each $C' \in \mathcal{A}$,

$$\partial(C') = \sum_{\beta < C'} [C' : \beta]\beta$$

where $\beta < C'$ means β is a facet of C' and $[C' : \beta] = (-1)^i$ where β is obtained from C' by deleting its ith vertex. Observe that two chambers are i-adjacent if and only if they have a facet of cotype i in common. Since $\mathcal{A}$ is thin, for each $\beta < C'$, there exists a unique chamber $D \in \mathcal{A}$ having the common facet β with C'. Thus, $\partial(C')$ and $\partial(D)$ agree at β and this β term appears exactly twice in $\partial(a_C)$, once in $\partial(C')$ and the other in $\partial(D)$, but with different signs since $sgn(C') \neq sgn(D)$. To see this, observe that

$$s_i = \delta(C', D) = \delta(C', C)\delta(C, D)$$

by Lemma 1.4.16. The map $sgn : S_{n+1} \to \{\pm 1\}$ defined by

$$sgn(\sigma) = \begin{cases} +1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd} \end{cases}$$

is a surjective group homomorphism and so $sgn(\delta(C', C))sgn(\delta(C, D)) = sgn(s_i) = -1$, that is, $sgn(C')sgn(D) = -1$ which implies $sgn(C') \neq sgn(D)$. Thus, the β term in $\partial(C')$ and $\partial(D)$ cancel out. So $\partial(a_C) = 0$ and hence $a_C \in Z_n(\Gamma)$. $\square$

In [9], Devillers, Gramlich and Mühlherr proved a result on the sphericity of the geometry Γ, analogous to the Solomon-Tits theorem. A statement of the theorem is given below.

Theorem 5.2.3. (Devillers, Gramlich, Muhlherr) *Let $\mathbb{F}$ be an arbitrary field and let σ be an automorphism of $\mathbb{F}$ of order two. Let V be an $(n+1)$-dimensional vector space over $\mathbb{F}$ endowed with a non-degenerate hermitian form f. Furthermore, let Γ be the simplicial complex whose vertices are the non-trivial subspaces of V which are non-degenerate with respect to f, with incidence given by inclusion. If $\mathbb{F}$ is finite of order q, assume $q > 2^{n-1}(\sqrt{q}+1)$. Then Γ is Cohen-Macaulay. In particular, $|\Gamma|$ is homotopy equivalent to a wedge of $(n-1)$-spheres.*

It is reasonable to give an example of n and q for which q satisfies the condition given in Theorem 5.2.3. Take $n = 3$ and $q \geq 25$, then q satisfies this condition.
Let us identify Γ with the rank n of its maximal simplices (or chambers). If q satisfies the property given in Theorem 5.2.3, then the Cohen-Macaulay property of Γ implies the next result.

Theorem 5.2.4. *Suppose Γ is Cohen-Macaulay. Then the dimension of the Phan code is given by the reduced Euler characteristic*

$$\chi(\Gamma) = \chi(n) = \sum_{i=0}^{n}(-1)^i|\Gamma_{n-1-i}|.$$

By convention, $|\Gamma_{-1}| = 1$.

Proof. Since Γ is Cohen-Macaulay, the result follows from Lemma 3.2.2. □

Notation: Let a_k^{n+1} denote the number of k-dimensional non-degenerate subspaces in an $(n+1)$-dimensional unitary space, let $\mathcal{F}_k^{n+1}$ be the set of all simplices in Γ whose smallest object has type k, and let $\Gamma_i^{n+1} = \Gamma_i$ be the set of all i-dimensional simplices in Γ.

Theorem 5.2.5. *Suppose q satisfies the condition in Theorem 5.2.3. Then the following results hold.*

(i) $|\Gamma_i^{n+1}| = \sum_{k=1}^{n} |\Gamma_i^{n+1} \cap \mathcal{F}_k^{n+1}| = \sum_{k=1}^{n} a_k^{n+1} |\Gamma_{i-1}^{n+1-k}|$, *for* $1 \leq i \leq n-1$.

(ii) The dimension of the Phan code is given by

$$\chi(n) = -1 - \sum_{k=1}^{n} a_k^{n+1} \chi(n-k).$$

Proof. (i) It is clear that $|\Gamma_i^{n+1}| = \sum_{k=1}^{n} |\Gamma_i^{n+1} \cap \mathcal{F}_k^{n+1}|$. It remains to show that $|\Gamma_i^{n+1} \cap \mathcal{F}_k^{n+1}| = a_k^{n+1} |\Gamma_{i-1}^{n+1-k}|$.
Let $\mathcal{F} \in \Gamma_i^{n+1} \cap \mathcal{F}_k^{n+1}$. Then $\mathcal{F}$ is an i-dimensional simplex and its smallest object V_k has dimension k. Since $V = V_k \oplus V_k^{\perp}$, every non-degenerate subspace U of V properly containing V_k corresponds to a non-degenerate subspace $U \cap V_k^{\perp}$ of $V_k^{\perp}$, which has dimension dim U − dim V_k. Thus $\mathcal{F}$ corresponds to an $(i-1)$-dimensional simplex in the Phan geometry Γ' defined on $V_k^{\perp}$. Thus, for each k-dimensional subspace V_k of V in Γ, there are precisely $|\Gamma_{i-1}^{n+1-k}|$ simplices of dimension i each of which have V_k as its smallest object, and since there are a_k^{n+1} subspaces of dimension k in Γ, it follows that

$$|\Gamma_i^{n+1} \cap \mathcal{F}_k^{n+1}| = a_k^{n+1} |\Gamma_{i-1}^{n+1-k}|.$$

Thus,

$$\begin{aligned}
|\Gamma_i^{n+1}| &= \sum_{k=1}^{n} |\Gamma_i^{n+1} \cap \mathcal{F}_k^{n+1}| \\
&= \sum_{k=1}^{n} a_k^{n+1} |\Gamma_{i-1}^{n+1-k}|,
\end{aligned}$$

for $1 \leq i \leq n-1$.

Now,

$$\begin{aligned}
\chi(n) &= \sum_{i=-1}^{n-1} (-1)^i |\Gamma_i^{n+1}| \\
&= -1 + \sum_{i=0}^{n-1} (-1)^i |\Gamma_i^{n+1}| \\
&= -1 + \sum_{i=0}^{n-1} (-1)^i \sum_{k=1}^{n} a_k^{n+1} |\Gamma_{i-1}^{n+1-k}| \\
&= -1 + \sum_{k=1}^{n} a_k^{n+1} \sum_{i=0}^{n-1} (-1)^i |\Gamma_{i-1}^{n+1-k}| \\
&= -1 + \sum_{k=1}^{n} a_k^{n+1} \left(\sum_{i=0}^{n-k} (-1)^i |\Gamma_{i-1}^{n+1-k}| + \underbrace{\sum_{i=n-k+1}^{n-1} (-1)^i |\Gamma_{i-1}^{n+1-k}|}_{=0} \right) \\
&= -1 + \sum_{k=1}^{n} a_k^{n+1} \sum_{i=0}^{n-k} (-1)^i |\Gamma_{i-1}^{n+1-k}| \\
&= -1 + \sum_{k=1}^{n} a_k^{n+1} (-\chi(n-k)).
\end{aligned}$$

This holds since

$$\begin{aligned}\chi(n-k) &= \sum_{i=-1}^{n-k-1} (-1)^i |\Gamma_i^{n+1-k}| \\ &= -\sum_{i=0}^{n-k} (-1)^i |\Gamma_{i-1}^{n+1-k}|.\end{aligned}$$

Thus, $\chi(n) = -1 - \sum_{k=1}^{n} a_k^{n+1} \chi(n-k)$. $\square$

Remark 5.2.6. *In [5], Bennett and Shpectorov showed that the Phan geometry Γ is connected if $(n,q) \neq (2,2)$. Suppose $n = 2$ and $q \geq 3$. Then the (augmented) chain complex*

$$C_1(\Gamma) \longrightarrow C_0(\Gamma) \longrightarrow C_{-1}(\Gamma) \longrightarrow 0$$

is exact, where $C_{-1}(\Gamma) = \mathbb{Z}$. This implies that $\operatorname{Ker} \partial_i = \operatorname{Im} \partial_{i+1}$ *for $i = -1, 0$. Hence, we deduce that the dimension of the Phan code $\overline{Z_1(\Gamma)}$ is again given by the reduced Euler characteristic $\chi(\Gamma) = \chi(1)$, and Γ need not satisfy the Cohen-Macaulay property in this case. Again, in [5], Bennett and Shpectorov showed that if $(n,q) \neq (3,2)$ or $(3,3)$, then Γ is simply connected. This implies that the fundamental group $\pi_1 = 0$. That is, the homology group $H_1(\Gamma) = 0$. So when $n = 3$ and $q \geq 4$, the dimension of the Phan code $\overline{Z_2(\Gamma)}$ is also given by the reduced Euler characteristic $\chi(\Gamma) = \chi(2)$.*

From now on, we work only in $\mathbb{F}_2$. For the ease of notation, we let $Z_{n-1}(\Gamma)$ denote the homology group with coefficients in $\mathbb{F}_2$.

Theorem 5.2.7. *Let w_m denote the minimal weight of the cycle code $Z_{n-1}(\Gamma)$. Then $w_m = (n+1)!$.*

Proof. Since $\Gamma \subset \Delta$, we may view $Z_{n-1}(\Gamma) \subset Z_{n-1}(\Delta)$. By Lemma 3.3.4, $Z_{n-1}(\Delta)$ has minimal weight $(n+1)!$. Thus, it suffices to show that a vector $z \in Z_{n-1}(\Delta)$ of minimal weight belongs to $Z_{n-1}(\Gamma)$. Indeed, if $\mathcal{A} \in \Delta$ is a good apartment, then the vector $a_{\mathcal{A}} = \sum_{C' \in \mathcal{A}} C' \in Z_{n-1}(\Gamma)$ by Lemma 5.2.2 and has weight $(n+1)!$. $\square$

5.3 Submodules

In this section, we take a close look at the composition of the Phan code $Z_{n-1}(\Gamma)$.

Definition 5.3.1. *We say a good apartment $\mathcal{A}$ is* special *if $\mathcal{A}^\tau = \mathcal{A}$.*

The following result gives a description of special apartments.

Lemma 5.3.2. *Let C be a chamber in Γ and suppose $\mathcal{A}$ is an apartment containing C and C^τ. Then $\mathcal{A}^\tau = \{D^\tau \mid D \in \mathcal{A}\} = \mathcal{A}$.*

Proof. Now C and C^τ are opposite, so the apartment $\mathcal{A}$ containing them is unique. As $C, C^\tau \in \mathcal{A}$ we have $C^\tau, C^{\tau\tau} = C \in \mathcal{A}^\tau$. Hence by the uniqueness of $\mathcal{A}$, we have $\mathcal{A}^\tau = \mathcal{A}$. $\square$

Proposition 5.3.3. *A good apartment $\mathcal{A}$ is special if and only if $\mathcal{A}$ is given by an orthonormal basis.*

Proof. Suppose $\mathcal{A}$ is a special apartment and let C be a chamber in $\mathcal{A}$. Then $C^\tau \in \mathcal{A}$. Now, if $C = V_1 \subset V_2 \subset \cdots \subset V_n$, then

$$\begin{aligned} C^\tau &= V_n^\tau \subset V_{n-1}^\tau \subset \cdots \subset V_1^\tau \\ &= V_n^\perp \subset V_{n-1}^\perp \subset \cdots \subset V_1^\perp. \end{aligned}$$

The apartment $\mathcal{A}$ is given by the basis $\{e_1, e_2, \ldots, e_{n+1}\}$ where $\langle e_1 \rangle = V_1$, $\langle e_2 \rangle = V_2 \cap V_1^\perp$, $\langle e_3 \rangle = V_3 \cap V_2^\perp$, $\ldots$, $\langle e_n \rangle = V_n \cap V_{n-1}^\perp$, $\langle e_{n+1} \rangle = V_{n+1} \cap V_n^\perp = V_n^\perp$, where $V_{n+1} = V$. Indeed, as V_1 is non-degenerate e_1 is non-isotropic. Furthermore, e_2 is non-isotropic since $e_1 \perp e_2$ and $\langle e_1, e_2 \rangle = V_2$ is non-degenerate. By similar argument, we also get that $e_3, e_4, \ldots, e_n, e_{n+1}$ are all non-isotropic. Without loss of generality, $(e_i, e_i) = 1$ for all $1 \leq i \leq n+1$. Then $\{e_1, e_2, \ldots, e_{n+1}\}$ is an orthonormal basis of V giving the apartment $\mathcal{A}$.

Now suppose $\mathcal{A}$ is given by an orthonormal basis $\{e_1, e_2, \ldots, e_{n+1}\}$. We want to show that for all $C \in \mathcal{A}$, $C^\tau \in \mathcal{A}$.
Let $C = \langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \cdots \subset \langle e_1, e_2, \ldots, e_n \rangle$. Then

$$\begin{aligned} C^\tau &= \langle e_1, e_2, \ldots, e_n \rangle^\tau \subset \langle e_1, e_2, \ldots, e_{n-1} \rangle^\tau \subset \cdots \subset \langle e_1 \rangle^\tau \\ &= \langle e_1, e_2, \ldots, e_n \rangle^\perp \subset \langle e_1, e_2, \ldots, e_{n-1} \rangle^\perp \subset \cdots \subset \langle e_1 \rangle^\perp. \end{aligned}$$

Since the basis $\{e_1, e_2, \ldots, e_{n+1}\}$ is orthonormal, we have

$$\begin{aligned}
\langle e_1\rangle^\perp &= \langle e_2, e_3, \ldots, e_{n+1}\rangle \\
\langle e_1, e_2\rangle^\perp &= \langle e_3, e_4, \ldots, e_{n+1}\rangle \\
\langle e_1, e_2, \ldots, e_k\rangle^\perp &= \bigcap_{i=1}^{k}\langle e_i\rangle^\perp \\
&= \langle e_{k+1}, \ldots, e_{n+1}\rangle.
\end{aligned}$$

Hence $C^\tau = \langle e_{n+1}\rangle \subset \langle e_n, e_{n+1}\rangle \subset \cdots \subset \langle e_2, e_3, \ldots, e_{n+1}\rangle$, which implies that $C^\tau \in \mathcal{A}$. Thus $\mathcal{A}$ is special.

$\square$

We remark that there are other good apartments $\mathcal{A}$ such that $\mathcal{A}^\tau \neq \mathcal{A}$. We illustrate this by means of an example in the rank two case.

Example 5.3.4. *Let V be a three dimensional unitary space over the field $\mathbb{F}_9 = \mathbb{F}_3(i)$ and suppose $\{e_1, e_2, e_3\}$ is an orthonormal basis of V. Let $\mathcal{A}$ be the apartment given by the basis $\{v_1, v_2, v_3\}$ such that $v_1 = e_1$, $v_2 = e_2$ and $v_3 = (1+i)(e_2 + e_3)$. Its Gram matrix is given below.*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1+i \\ 0 & 1-i & 1 \end{pmatrix}.$$

From the Gram matrix of $\mathcal{A}$, we see that all the vertices $\langle v_1\rangle$, $\langle v_2\rangle$, $\langle v_3\rangle$, $\langle v_1, v_2\rangle$, $\langle v_1, v_3\rangle$, and $\langle v_2, v_3\rangle$ of $\mathcal{A}$ are good but its basis $\{v_1, v_2, v_3\}$ is not orthonormal. Thus, $\mathcal{A}$ is a good apartment which is not special.

Lemma 5.3.5. *Let $\mathcal{A}$ be a good apartment. Then for all $g \in G$, $\mathcal{A}^g$ is special if and only if $\mathcal{A}$ is special.*

Proof. By Lemma 5.3.3, this is equivalent to proving that $\mathcal{A}^g$ is given by an orthonormal basis if and only if $\mathcal{A}$ is given by an orthonormal basis. The result then follows from the fact that G acts transitively on the set of bases of V and also preserves the form $(\quad,\quad)$. That is, if $\{v_1, v_2, \ldots, v_{n+1}\}$ is a basis giving $\mathcal{A}^g$, then $v_i = u_i^g$ where $\{u_1, u_2, \ldots, u_{n+1}\}$ is a basis giving $\mathcal{A}$. Thus $(v_i, v_j) = \delta_{ij}$ if and only if $(u_i, u_j) = \delta_{ij}$. $\square$

Recall that if $\mathcal{A}$ is an apartment, then the vector $a_{\mathcal{A}} = \sum_{C' \in \mathcal{A}} C'$.

Theorem 5.3.6. *Let $\mathcal{S} = \{a_{\mathcal{A}} \mid \mathcal{A}$ is a special apartment$\}$. Then $\mathcal{S}$ is a linearly independent set and the weight of every element of $\langle \mathcal{S} \rangle$ is a multiple of $(n+1)!$. Furthermore, $\langle \mathcal{S} \rangle$ is a proper submodule of $Z_{n-1}(\Gamma)$ of dimension $|G : H|/(n+1)!$, where H denotes the stabilizer of a chamber in Γ.*

Proof. Let $\mathcal{A}$ be a special apartment and suppose $D \in \mathcal{A}$. Since D and D^τ are opposite, the apartment $\mathcal{A}$ containing them is uniquely determined. It therefore follows that for any two special apartments $\mathcal{A}_1$ and $\mathcal{A}_2$, their intersection

$$\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset.$$

In particular, $\sum_{\substack{\mathcal{A} \in \Gamma \\ \mathcal{A} = \mathcal{A}^\tau}} \lambda_{\mathcal{A}} a_{\mathcal{A}} = 0$ if and only if $\lambda_{\mathcal{A}} = 0$ for all special apartments $\mathcal{A}$. Thus, the set $\mathcal{S}$ is linearly independent.

Note that since the special apartments are pairwise disjoint and each codeword generating $\mathcal{S}$ has weight $(n+1)!$, any linear combination of codewords in $\mathcal{S}$ would have as weight an integral multiple of $(n+1)!$. Let D

be a good chamber and suppose $\mathcal{A}_1$ and $\mathcal{A}_2$ are two distinct good apartments containing D. Suppose the codeword $a_{\mathcal{A}_1} + a_{\mathcal{A}_2}$ has weight w, then $(n+1)! < w \leq 2(n+1)! - 2 = 2((n+1)! - 1)$ which implies that w is not an integral multiple of $(n+1)!$. It therefore follows that $\langle \mathcal{S} \rangle$ is a proper subspace of $Z_{n-1}(\Gamma)$. By Lemma 5.3.5, $\mathcal{S}$ is a G-set and so $\langle \mathcal{S} \rangle$ is a proper submodule of $Z_{n-1}(\Gamma)$. Since special apartments are pairwise disjoint and each chamber in Γ lies in a unique special apartment, it follows that the dimension of $\langle \mathcal{S} \rangle$ is $|G : H|/(n+1)!$, where H denotes the stabilizer of a chamber in Γ.

$\square$

Remark 5.3.7. *Indeed, if C_1 and C_2 are two good chambers which are not opposite, then C_1 and C_2 lie in many good apartments. In particular, any linear combination of the codewords $\{a_{\mathcal{A}} \mid \mathcal{A}$ is good and $\mathcal{A} \ni C_1, C_2\}$ would not have weight which is a multiple of* $(n+1)!$ *(since every chamber that lies on a minimal gallery from C_1 to C_2 would appear in each of these apartments).*

Corollary 5.3.8. *The Phan module $Z_{n-1}(\Gamma)$ is not irreducible.*

5.4 The Rank two case

Throughout this section V is a 3-dimensional unitary space, so Δ is the projective building of rank two. Chambers are point-line flags, that is, if D is a chamber then $D = Y_1 \subset Y_2$, where Y_1 is a point and Y_2 is a line in Δ.

The objective of this section is to find a suitable basis for the Phan code in the rank 2 case, and to establish that it is spanned by codewords corresponding to good apartments.

Recall that by the axioms of a projective geometry, every point in Δ has $q^2 + 1$ lines passing through it and every line in Δ contains $q^2 + 1$ points.

Proposition 5.4.1. *Let l be a non-degenerate line and p a non-degenerate point in Δ. Then the following hold.*

(i) There are $q^2 - q$ non-degenerate points and $q + 1$ degenerate points in l.

(ii) There are $q + 1$ degenerate lines passing through the point p.

(iii) If p is a point not on l, then there are at least $q^2 - 2q - 1$ non-degenerate points on l which form a degenerate line with p.

Proof. Since l is a non-degenerate line, it may be viewed as a 2-dimensional unitary space on which the group $G = \mathrm{GU}_2(q)$ acts. Now G acts transitively on the set of non-degenerate points in l (by Witt's Lemma), so the number of non-degenerate points in l is given by $|G : G_p|$. By Proposition 5.1.3, $G_p = \mathrm{GU}_1(q) \times \mathrm{GU}_1(q)$. So

$$|G : G_p| = q(q + 1)(q^2 - 1)/(q + 1)^2 = q^2 - q.$$

Since l contains q^2+1 points and q^2-q of them are non-degenerate, there are $q^2+1-(q^2-q)=q+1$ degenerate points in l.

Now every degenerate point in $p^\perp$ forms a degenerate line with p, and so (ii) follows from the proof of Lemma 4.1.2. Since l has q^2-q non-degenerate points and p has $q+1$ degenerate lines passing through it, if p is not in l, then there are at least $q^2-q-(q+1)=q^2-2q-1$ non-degenerate points on l which form a degenerate line with p. $\square$

Fix a chamber $C \in \Gamma$; call it the *fundamental chamber*. Recall that Solomon-Tits theorem tells us that the set $\mathcal{D} = \{a_\mathcal{A} \mid \mathcal{A} \ni C\}$ forms a basis for the module $Z_1(\Delta)$. Thus for each $z \in Z_1(\Delta)$,

$$z = \sum_{\substack{\mathcal{A}\in\Delta \\ \mathcal{A}\ni C}} f_\mathcal{A}(z) a_\mathcal{A} \quad \text{with } f_\mathcal{A}(z) \in \mathbb{F}_2.$$

We say an apartment $\mathcal{A}$ is *represented* in $z \in Z_1(\Delta)$ if $f_\mathcal{A}(z) \neq 0 \in \mathbb{F}_2$, we also say $\mathcal{A}$ is *represented* in $Z_1(\Delta)$ if it is represented in some element $z \in Z_1(\Delta)$. Indeed as $Z_1(\Gamma)$ is contained in $Z_1(\Delta)$, each element $x \in Z_1(\Gamma)$ can be written as a sum of elements in $\mathcal{D}$. Thus x can be written as a sum of good and bad apartments in Δ. Furthermore, apartments containing bad opposite chambers to the fundamental chamber C cannot be represented. We remark that a bad apartment $\mathcal{A}$ containing C can only be represented in $Z_1(\Gamma)$ if and only if the opposite chamber C^{opp} to C in $\mathcal{A}$ is good. Hence, we only need to consider those apartments $\mathcal{A}$ containing C such that C^{opp} in $\mathcal{A}$ is good. The objective is to identify those apartments which are actually represented and how they would appear. We need the following definition.

Definition 5.4.2. *Let $C' = p' \subset l'$ be a chamber such that $d(C, C') = 2$. We say C' is of* type 1 *if the minimal gallery γ from C to C' has type $(1, 2)$ and the point p' is bad but the line l' is good. Similarly, we say C' is of* type 2 *if the minimal gallery γ from C to C' has type $(2, 1)$ and the point p' is good but the line l' is bad.*

Remark 5.4.3. *Note that if $C' = p' \subset l'$ is of type 1 and the fundamental chamber $C = p \subset l$, then $p' \subset l$. Similarly, if C' is of type 2, then $p \subset l'$.*

Let $\mathcal{A}_C$ denote an apartment containing the chamber C and suppose C^{opp} in $\mathcal{A}_C$ is good. There are four types to consider:

(Type 1) The apartment $\mathcal{A}_C$ is bad; $\mathcal{A}_C$ contains a bad chamber C' of type 1 such that every bad chamber in $\mathcal{A}_C$ lies on the minimal gallery γ from C to C'. (See Figure 5.1 (a).)

(Type 2) The apartment $\mathcal{A}_C$ is bad; $\mathcal{A}_C$ contains a bad chamber C' of type 2 such that every bad chamber in $\mathcal{A}_C$ lies on the minimal gallery γ from C to C'. (See Figure 5.1 (b).)

(Type 3) The apartment $\mathcal{A}_C$ is bad; $\mathcal{A}_C$ contains a bad chamber C' of type 1 and a bad chamber C'' of type 2, such that if γ is the minimal gallery from C to C' and β is the minimal gallery from C to C'', then every bad chamber in $\mathcal{A}_C$ lies in $\gamma \cup \beta$. In particular, the only good chambers in $\mathcal{A}_C$ are C and C^{opp}. (See Figure 5.1 (c).)

(Type 4) The apartment $\mathcal{A}_C$ is good, that is, all the chambers in $\mathcal{A}_C$ belongs to Γ. Then $\mathcal{A}_C$ is definitely represented in $Z_1(\Gamma)$.

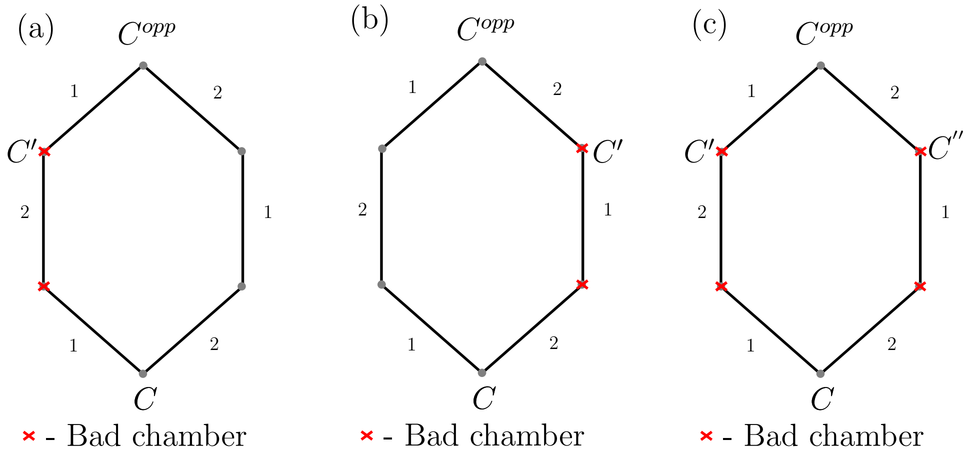

Figure 5.1: (a) Example of a Type 1 apartment, (b) Example of a Type 2 apartment, and (c) Example of a Type 3 apartment.

Definition 5.4.4. *Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be two apartments of type* 1 *(respectively, type* 2*) above. We say $\mathcal{A}_1$ and $\mathcal{A}_2$ are C'*-related *if they contain the same C' of type* 1 *(respectively, type* 2*), and we write $\mathcal{A}_1 \approx_{C'} \mathcal{A}_2$ or simply $\mathcal{A}_1 \approx \mathcal{A}_2$.*

The relation $\approx$ is an equivalence relation and partitions the apartments of type k, $k = 1, 2$, into corresponding equivalence classes.

Notation: We write $\mathcal{A}_{D,D'}$ for an apartment containing the chambers D and D', such that D and D' are opposite.

Proposition 5.4.5. *Let C' denote a chamber of type k, $k = 1, 2$. Suppose $\mathcal{A}_1 = \mathcal{A}_{C,C_1} = \mathcal{A}_{C',C_1'}$ and $\mathcal{A}_2 = \mathcal{A}_{C,C_2} = \mathcal{A}_{C',C_2'}$ are two apartments of type k, such that $\mathcal{A}_1 \approx_{C'} \mathcal{A}_2$. Then their symmetric difference*

$$\mathcal{A}_1 \triangle \mathcal{A}_2 = \mathcal{A}_{C_1,C_2'} = \mathcal{A}_{C_2,C_1'} = \mathcal{A}$$

is a good apartment. In particular, $a_{\mathcal{A}_1} + a_{\mathcal{A}_2} = a_{\mathcal{A}}$.

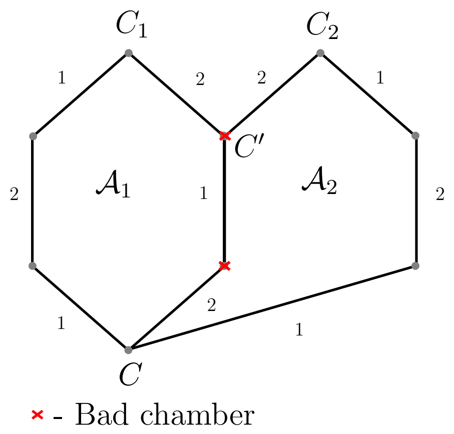

Figure 5.2: Example of type 2 apartments $\mathcal{A}_1$ and $\mathcal{A}_2$, such that $\mathcal{A}_1 \approx_{C'} \mathcal{A}_2$.

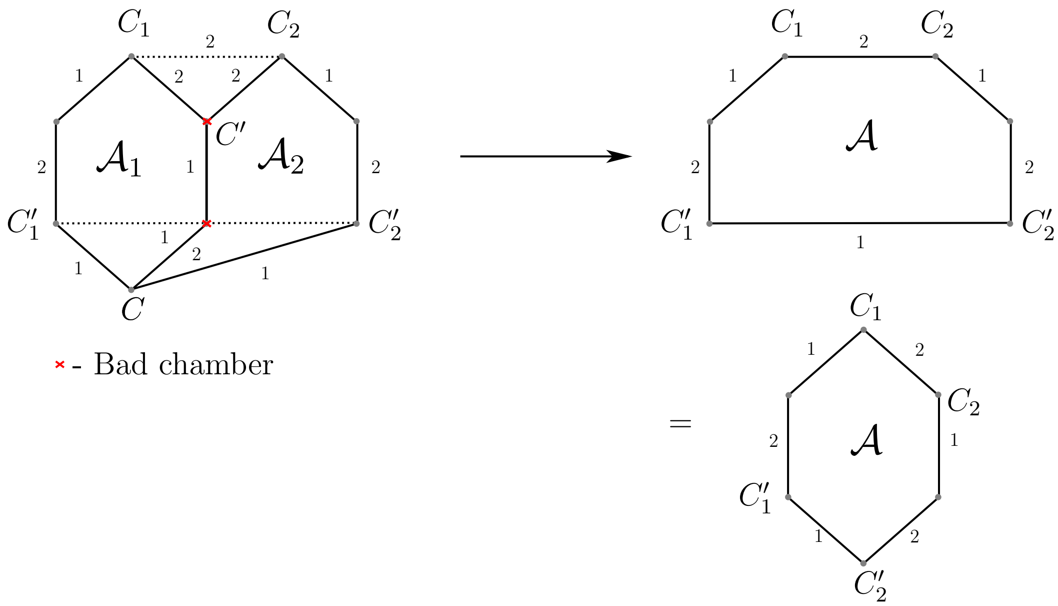

Figure 5.3: Description of how the good apartment $\mathcal{A}$ is obtained from the apartments $\mathcal{A}_1$ and $\mathcal{A}_2$.

Proof. Let $\gamma = (C, C_0, C')$ be the minimal gallery from C to C'. Then γ

lies in $\mathcal{A}_1$ and $\mathcal{A}_2$ (see Figure 5.2). If $k = 1$, then γ has type $(1, 2)$ and $C_1 \sim_1 C' \sim_1 C_2$ which implies $C_1 \sim_1 C_2$. Let C_1' and C_2' be the other neighbours of C in $\mathcal{A}_1$ and $\mathcal{A}_2$ respectively. (That is, $C_1' \neq C_0 \neq C_2'$.) Then as $C \sim_1 C_0$, we have $C_1' \sim_2 C \sim_2 C_2'$, which implies $C_1' \sim_2 C_2'$. Since $\mathcal{A}_1 \cap \mathcal{A}_2 = \{C, C_0, C'\}$, we have that $\mathcal{A}_1 \triangle \mathcal{A}_2$ contains every chamber in $\mathcal{A}_1 \cup \mathcal{A}_2$ except the chambers C, C_0 and C'. Note that C_1 and C_2' are opposite (similarly, C_2 and C_1') and hence every chamber in $\mathcal{A}_1 \triangle \mathcal{A}_2$ lies on some minimal gallery from C_1 to C_2' (similarly, from C_2 to C_1'). Note that all the chambers in $\mathcal{A}_1 \triangle \mathcal{A}_2$ are good (see Figure 5.3). It therefore follows that

$$\mathcal{A}_1 \triangle \mathcal{A}_2 = \mathcal{A}_{C_1, C_2'} = \mathcal{A}_{C_2, C_1'} = \mathcal{A}.$$

We get similar results in the case $k = 2$.

Now the sum $a_{\mathcal{A}_1} + a_{\mathcal{A}_2}$ is in $Z_1(\Gamma)$ (with coefficients in $\mathbb{F}_2$) and hence chambers which appear an even number of times are eliminated. Thus, $a_{\mathcal{A}_1} + a_{\mathcal{A}_2} = a_{\mathcal{A}}$. □

For each chamber C' of type k, $k \in \{1, 2\}$, denote by $X_{C'}$ the C'-equivalence class of type k apartments. Fix an apartment $\mathcal{A}_{C'} \in X_{C'}$. For any $\mathcal{A} \in X_{C'}$ define

$$e_{\mathcal{A}} = a_{\mathcal{A}} + a_{\mathcal{A}_{C'}}.$$

Note that $e_{\mathcal{A}_{C'}} = 0$. Similarly, for each apartment $\mathcal{A}$ of type 3, define

$$e_{\mathcal{A}} = a_{\mathcal{A}_{C'}} + a_{\mathcal{A}} + a_{\mathcal{A}_{C''}}$$

where $C', C'' \in \mathcal{A}$ are of types 1 and 2 respectively, and $\mathcal{A}_{C'}$ and $\mathcal{A}_{C''}$ are the corresponding fixed apartments in $X_{C'}$ and $X_{C''}$ respectively. Finally, for each apartment $\mathcal{A}$ of type 4, define $e_{\mathcal{A}} = a_{\mathcal{A}}$.

Theorem 5.4.6. *Let $\mathcal{A}$ denote an apartment containing the fundamental chamber C. The set $\mathcal{B} = \{e_{\mathcal{A}} \neq 0 \mid \mathcal{A}$ is of type $1, 2, 3$ or $4\}$ forms a basis for $Z_1(\Gamma)$.*

Proof. First observe that $e_{\mathcal{A}} = 0$ if and only if $\mathcal{A} = \mathcal{A}_{C'}$ for some C' of type 1 or 2. Also note that for each apartment $\mathcal{A}$ of type $1, 2, 3$ or 4, the set $\{a_{\mathcal{A}} \mid e_{\mathcal{A}} \in \mathcal{B}\}$ is a linearly independent set. This is due to the fact that $\{a_{\mathcal{A}} \mid e_{\mathcal{A}} \in \mathcal{B}\} \subset \{a_{\mathcal{A}} \mid \mathcal{A} \ni C\}$, which is a basis for $Z_1(\Delta)$ by the Solomon-Tits theorem. It therefore follows that for each apartment $\mathcal{A}$ of type k, $k = 1, 2, 3, 4$, $e_{\mathcal{A}}$ is not in the linear combination of any of the others. Thus, $\mathcal{B}$ is a linearly independent set. It now remains to show that $\mathcal{B}$ spans $Z_1(\Gamma)$.

Suppose $span(\mathcal{B}) \neq Z_1(\Gamma)$ and pick a codeword $x \in Z_1(\Gamma) \setminus span(\mathcal{B})$. Then $x \neq 0$ and by the Solomon-Tits theorem, x can be written as a linear combination of the apartments containing the fundamental chamber C. That is,

$$x = \sum_{\substack{\mathcal{A} \in \Delta \\ \mathcal{A} \ni C}} f_{\mathcal{A}}(x) a_{\mathcal{A}}, \quad f_{\mathcal{A}}(x) \in \mathbb{F} \tag{*}$$

Consider the apartments represented in (*). If $\mathcal{A}$ is such an apartment, that is $f_{\mathcal{A}}(x) \neq 0$ in (*), then $\mathcal{A}$ has type $1, 2, 3$, or 4. If $\mathcal{A}$ has type 4, then add $e_{\mathcal{A}} = a_{\mathcal{A}}$ to x. We do this for each apartment of type 4 represented in

(*). So the resulting codeword x' has no apartment of type 4 represented, furthermore, $x' \in Z(\Gamma) \setminus span(\mathcal{B})$ since $x \notin span(\mathcal{B})$ implies $x + e_{\mathcal{A}} \notin span(\mathcal{B})$ for all apartments $\mathcal{A}$ of type 4 represented in x. Similarly, for any apartment $\mathcal{A}$ of type 3 represented in x' add $e_{\mathcal{A}} = a_{\mathcal{A}_{C'}} + a_{\mathcal{A}} + a_{\mathcal{A}_{C''}}$ to x'. This eliminates $a_{\mathcal{A}}$ but adds $a_{\mathcal{A}_{C'}}$ and $a_{\mathcal{A}_{C''}}$ to x'. Thus, the resulting codeword x'' only has apartments of types 1 or 2 represented. Finally, for each apartment $\mathcal{A}$ of type k represented in x'', $k = 1, 2$, add $e_{\mathcal{A}} = a_{\mathcal{A}} + a_{\mathcal{A}_{C'}}$ to x''. Again, this gets rid of $a_{\mathcal{A}}$ but adds $a_{\mathcal{A}_{C'}}$ to x'', for each $\mathcal{A}$ of type k. Note that for the fixed $\approx_{C'}$-class representatives $\mathcal{A}_{C'}$, $e_{\mathcal{A}_{C'}} = 0$. Hence, the resulting codeword x''' is a sum of the $\mathcal{A}_{C'}$s. Since these contain bad chambers, the only way they can appear in $Z_1(\Gamma)$ is an even number of times, forcing $x''' = 0$. But this implies that the codeword x we started with belongs to $span(\mathcal{B})$, a contradiction to the choice of x. □

Lemma 5.4.7. *Let $\mathcal{A}_{C,C^\star} = \mathcal{A}^\star$ be an apartment of type 3, where $C^\star = p^\star \subset l^\star$ denotes the opposite chamber to C in $\mathcal{A}^\star$. Let C' and C'' be the neighbours of $C^\star$ in $\mathcal{A}^\star$ of types 1 and 2 respectively. Then, if $q \geq 5$, there are at least $(q^2 - 2q - 1)(q^2 - 4q - 3)$ pairs of apartments $\mathcal{A}_1 \in X_{C'}$ and $\mathcal{A}_2 \in X_{C''}$, such that the codeword $a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2}$ can be written as a sum of three good apartments.*

Proof. A pictorial representation of the apartments $\mathcal{A}_1$, $\mathcal{A}^\star$ and $\mathcal{A}_2$ is given in Figure 5.4.

Pick $\mathcal{A}_1 \in X_{C'}$ and let C_1 be the opposite chamber to C in $\mathcal{A}_1$. Then C and C_1 determine $\mathcal{A}_1$. Note that C_1 and $C^\star$ are 1-adjacent and so have the line $l^\star$ in common. Thus $C_1 = p_1 \subset l^\star$ for some good point $p_1 \in l^\star$, $p_1 \neq p^\star$. To

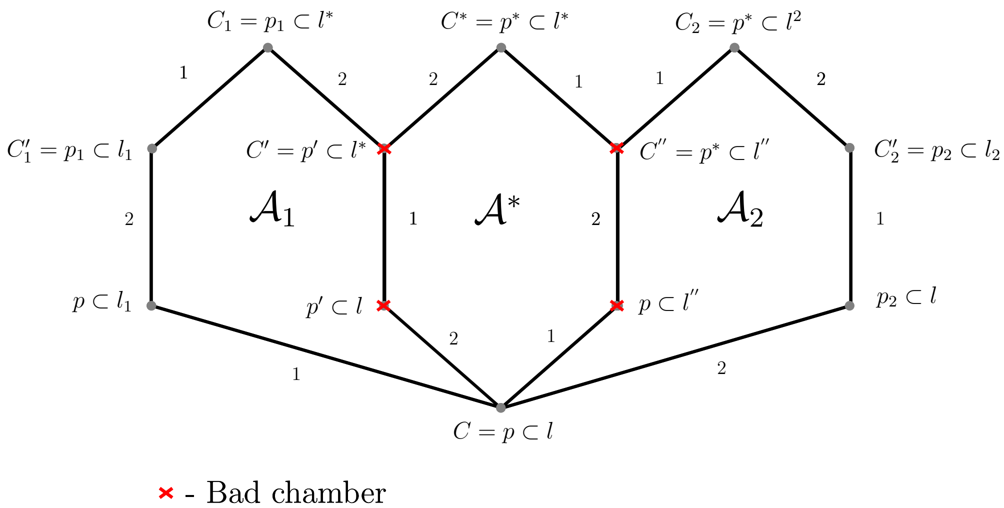

Figure 5.4: Representation of a type 3 apartment

count the number of choices for $\mathcal{A}_1$ is equivalent to counting the number of choices for C_1 (or p_1 to be precise) subject to the condition that $\langle p_1, p \rangle$ is a good line. Now there are $q^2 - q$ good points in $l^\star$ (by Proposition 5.4.1), and $p^\star$ is one of them, so there are at most $q^2 - q - 1$ choices for p_1 in $l^\star$. We want $\langle p_1, p \rangle$ to be a good line. There are $q + 1$ bad lines through p (by Proposition 5.4.1)and hence $q + 1$ points which form a bad line with p. The point $p^\star$ is one of such points, so at most q of the $q^2 - q - 1$ possible choices for p_1 are bad. Thus, there are at least $(q^2 - q - 1) - q = q^2 - 2q - 1$ choices for p_1 and hence at least $q^2 - 2q - 1$ choices for $\mathcal{A}_1$.

Let us fix $\mathcal{A}_1$ (hence $C_1 = p_1 \subset l^\star$) for the moment. We would like to count the number of choices for $\mathcal{A}_2$ such that $a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2}$ can be written as a sum of three good apartments. Let C_2 be the opposite chamber to C in $\mathcal{A}_2$. Then C_2 and $C^\star$ are 2-connected (since C_2 is 2-adjacent to C'' which is also

2-adjacent to $C^\star$) and so have the point $p^\star$ in common. Thus $C_2 = p^\star \subset l_2$ where l_2 is a good line such that $l_2 \cap l$ is good. Again counting the number of choices for $\mathcal{A}_2$ is equivalent to counting the number of choices for l_2, subject to the following conditions:

- $p_2 = l_2 \cap l$ is good
- $\langle p_1, p_2 \rangle$ is good
- $l_2 \cap l_1$ is good.

Now, l_2 passes through $p^\star$ which has $q^2 - q$ good lines through it. The line $l^\star$ is one of them, so there are at most $q^2 - q - 1$ possible choices for l_2. We want $l_2 \cap l$ to be good. There are $q+1$ bad points on l, so at most $q+1$ good lines passing through $p^\star$ intersect l at a bad point and $l^\star$ is one of them. So there at least $(q^2 - q - 1) - q = q^2 - 2q - 1$ choices for l_2 such that $l_2 \cap l$ is good. We also want $\langle p_1, p_2 \rangle$ to be good, where $p_2 = l_2 \cap l$. Observe that each line l_2 determines a unique point p_2. Thus, there are as many choices for p_2 as there are for l_2. For $\langle p_1, p_2 \rangle$ to be good, p_2 cannot lie in the $q + 1$ bad lines through p_1. If p_2 lies in a bad line through p_1, then the line l_2 yielding it is unacceptable. So, there are at least $q^2 - 2q - 1 - (q + 1) = q^2 - 3q - 2$ choices for p_2 and hence at least $q^2 - 3q - 2$ choices for l_2. Finally, we want $l_2 \cap l_1$ to be good. Again, at most $q + 1$ good lines intersect l_1 at a bad point, so the number of choices for l_2 such that $l_2 \cap l_1$ is good is at least $(q^2 - 3q - 2) - (q + 1) = q^2 - 4q - 3$. Hence, for the fixed apartment $\mathcal{A}_1$ there are at least $q^2 - 4q - 3$ choices for the apartment $\mathcal{A}_2$. Since $\mathcal{A}_1$ has at least $q^2 - 2q - 1$ choices, there are at least $(q^2 - 2q - 1)(q^2 - 4q - 3)$ pairs of apartments $\mathcal{A}_1$, $\mathcal{A}_2$ such that the codeword $a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2}$ can be written as a sum of three good apartments. $\square$

Corollary 5.4.8. *Let $\mathcal{A}^\star$, C', C'' and q be as in Lemma 5.4.7. Then for any apartment $\mathcal{A}_1 \in X_{C'}$ and $\mathcal{A}_2 \in X_{C''}$, the codeword $a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2}$ can be written as a sum of good apartments.*

Proof. By Lemma 5.4.7, we can choose $\mathcal{A}_1 \in X_{C'}$ and $\mathcal{A}_2 \in X_{C''}$ such that the codeword $a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2}$ can be written as a sum of three good apartments. Choose and fix such an $\mathcal{A}_1 \in X_{C'}$ and $\mathcal{A}_2 \in X_{C''}$. Then for any $\mathcal{A}_1' \neq \mathcal{A}_1 \in X_{C'}$ and $\mathcal{A}_2' \neq \mathcal{A}_2 \in X_{C''}$ we have,

$$a_{\mathcal{A}_1'} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2'} = (a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2}) + (a_{\mathcal{A}_1} + a_{\mathcal{A}_1'}) + (a_{\mathcal{A}_2} + a_{\mathcal{A}_2'}).$$

By Proposition 5.4.5, there are good apartments $\mathcal{A}'$ and $\mathcal{A}''$ such that

$$(a_{\mathcal{A}_1} + a_{\mathcal{A}_1'}) = a_{\mathcal{A}'} \text{ and } (a_{\mathcal{A}_2} + a_{\mathcal{A}_2'}) = a_{\mathcal{A}''}.$$

Let $\mathcal{B}_1, \mathcal{B}_2,$ and $\mathcal{B}_3$ be three good apartments such that

$$a_{\mathcal{A}_1} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2} = a_{\mathcal{B}_1} + a_{\mathcal{B}_2} + a_{\mathcal{B}_3}.$$

Then, $a_{\mathcal{A}_1'} + a_{\mathcal{A}^\star} + a_{\mathcal{A}_2'} = a_{\mathcal{B}_1} + a_{\mathcal{B}_2} + a_{\mathcal{B}_3} + a_{\mathcal{A}'} + a_{\mathcal{A}''}$, completing the proof. $\square$

Theorem 5.4.9. *Suppose $q \geq 5$. The set $\mathcal{T} = \{a_{\mathcal{A}} \mid \mathcal{A}$ is a good apartment$\}$ spans $Z_1(\Gamma)$.*

Proof. By Lemma 5.4.6, the set

$$\mathcal{B} = \{e_{\mathcal{A}} \neq 0 \mid \mathcal{A} \ni C \text{ and } \mathcal{A} \text{ is of type } 1, 2, 3 \text{ or } 4\}$$

forms a basis for $Z_1(\Gamma)$. If $\mathcal{A}$ is of type k, $k = 1, 2$, then by Proposition 5.4.5, there is a good apartment $\mathcal{A}'$ such that $e_{\mathcal{A}} = a_{\mathcal{A}'}$. If $\mathcal{A}$ is of type 3 then by Lemma 5.4.7 and Corollary 5.4.8, $e_{\mathcal{A}}$ can be written as a sum of good apartments. If $\mathcal{A}$ is of type 4, then $\mathcal{A}$ is good by definition and $e_{\mathcal{A}} = a_{\mathcal{A}}$. It therefore follows that every element in $Z_1(\Gamma)$ can be written as a sum of good apartments. □

Noting that good apartments can be defined for all ranks, a natural question would be; can we find a basis for $Z_{n-1}(\Gamma)$ consisting only of good apartments?

5.5 Submodules in Rank 2

Here, we obtain submodules for the Phan code in the rank 2 case.

Definition 5.5.1. *We say an apartment $\mathcal{A}$ has k* zeros*, $k \geq 0$, if the gram matrix of a basis of V giving $\mathcal{A}$ contains k zeros.*

Note that if the Gram matrix of a basis of V giving an apartment $\mathcal{A}$ contains k number of zeros, then the Gram matrix of any basis of V giving $\mathcal{A}$ contains k zeros.

Lemma 5.5.2. *Let $\mathcal{A}$ denote a good apartment and for $i = 0, 1, 2, 3$, let $B_i = \{\mathcal{A} \mid \mathcal{A}$ has $2i$ zeros$\}$. Set $V_i = \langle a_{\mathcal{A}} \mid \mathcal{A} \in B_i \rangle$. Then V_i is a submodule of $Z_1(\Gamma)$, for all i.*

Proof. By definition, V_i is a subspace of $Z_1(\Gamma)$, for all i. It remains to show that V_i is also a G-set. Suppose an apartment $\mathcal{A} \in B_i$ is given by the basis $\{e_1, e_2, e_3\}$ for V. Then for any $g \in G$, we have

$$(e_i^g, e_j^g) = (e_i, e_j).$$

It therefore follows that the apartment $\mathcal{A}^g$ given by the basis $\{e_1^g, e_2^g, e_3^g\}$ has the same gram matrix as $\mathcal{A}$. Hence, for all i and all $g \in G$, $\mathcal{A}^g \in B_i$ provided $\mathcal{A} \in B_i$. In particular, $V_i^G = V_i$. □

The next result shows that there is some overlapping of the submodules V_i.

Lemma 5.5.3. *Let V_i, B_i be as in Lemma 5.5.2, $i = 2, 3$. Then for each apartment $\mathcal{A} \in B_3$, the codeword $a_{\mathcal{A}}$ can be written as a sum of apartments in B_2. In particular, $V_3 \subsetneqq V_2$.*

Proof. Let $\mathcal{A}$ be a good apartment given by the basis $\{e_1, e_2, e_3\}$ of V and suppose $(e_i, e_i) = 1$ for all i. We consider the different ways by which $\mathcal{A}$ may be written as a symmetric difference of two good apartments $\mathcal{A}_1$ and $\mathcal{A}_2$. There are three possibilities.

(I) The apartments $\mathcal{A}_1, \mathcal{A}_2$ are given by the bases $\{e_1, e_2, e_4\}$ and $\{e_2, e_3, e_4\}$ respectively, with $e_4 \in \langle e_1, e_3 \rangle$ such that $\langle e_4 \rangle$ and $\langle e_2, e_4 \rangle$ are non-degenerate.

(II) The apartments $\mathcal{A}_1, \mathcal{A}_2$ are given by the bases $\{e_1, e_2, e_4\}$ and $\{e_1, e_3, e_4\}$ respectively, with $e_4 \in \langle e_2, e_3 \rangle$ such that $\langle e_4 \rangle$ and $\langle e_1, e_4 \rangle$ are non-degenerate.

(III) The apartments $\mathcal{A}_1, \mathcal{A}_2$ are given by the bases $\{e_1, e_3, e_4\}$ and $\{e_2, e_3, e_4\}$ respectively, with $e_4 \in \langle e_1, e_2 \rangle$ such that $\langle e_4 \rangle$ and $\langle e_3, e_4 \rangle$ are non-degenerate.

Suppose $\mathcal{A} \in B_3$, then $\mathcal{A}$ is special. Thus $\mathcal{A}$ is given by an orthonormal basis $\{e_1, e_2, e_3\}$ which has gram matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We have $e_1^\perp = \langle e_2, e_3 \rangle$, and $e_2^\perp = \langle e_1, e_3 \rangle$ and $e_3^\perp = \langle e_1, e_2 \rangle$. We wish to examine the gram matrices for the bases giving the apartments $\mathcal{A}_1$ and $\mathcal{A}_2$. In (I), we have $e_4 \in \langle e_1, e_3 \rangle$ so $(e_2, e_4) = 0$. Also $(e_1, e_4) = a \neq 0$ and $(e_3, e_4) = b \neq 0$ since $\langle e_1, e_3 \rangle \cap e_1^\perp = \langle e_3 \rangle$ and $\langle e_1, e_3 \rangle \cap e_3^\perp = \langle e_1 \rangle$. So the bases $\{e_1, e_2, e_4\}$ and $\{e_2, e_3, e_4\}$ have gram matrices

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ \bar{a} & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & \bar{b} & 1 \end{pmatrix}.$$

We get similar results in cases (II) and (III) with gram matrices also containing four zeros. Thus, in all three cases, the apartments $\mathcal{A}_1$ and $\mathcal{A}_2$ belong to B_2 and so $V_3 \subseteq V_2$. Now, if $V_2 \subseteq V_3$, then any apartment $\mathcal{A} \in B_2$ can be written as a symmetric difference of apartments in B_3. By Lemma 5.3.6, the apartments in B_3 are pairwise disjoint, which implies their intersection is empty and so the symmetric difference of any two apartments in B_3 is just the (disjoint) union of the two apartments. In particular, the symmetric difference of any two apartments in B_3 cannot yield an apartment in B_2 and hence $V_3 \subsetneq V_2$. $\square$

Chapter 6

Summary and Conjectures

In this thesis, we have defined linear codes based on the Phan geometry $\Gamma = \Gamma(n, q)$ of type A_n. We also investigated the action of the unitary group $G = SU_{n+1}(q)$ on the code and described some of its properties. In particular, we showed that the action of the group on the code is not irreducible. In the rank two case, we obtained a basis for this code and showed that it is spanned by all the good apartments in the associated building of type A_n. In addition, we find some submodules of the code module. We proved that given the sets $B_i = \{\mathcal{A}$ a good apartment $\mid \mathcal{A}$ has a gram matrix having $2i$ zeros$\}$, with $0 \leq i \leq 3$, the spaces defined by

$$V_i = \langle a_{\mathcal{A}} \mid \mathcal{A} \in B_i \rangle$$

are submodules of the code module. We suspect that these spaces would overlap in some way and on close observation we obtained the refinement $V_3 \subsetneqq V_2$. Furthermore, we anticipate that we would have the following result.

Conjecture 6.0.4. *Let V_i be as above, $0 \leq i \leq 3$. Then the following results* *hold.*

(i) $V_3 \subsetneqq V_2 \subsetneqq V_0$

(ii) $V_1 \subsetneqq V_0$

(iii) V_0 *is the code module.*

Drawing from our results in the rank two case, we also make the following speculation regarding a basis of the Phan module in arbitrary rank n.

Conjecture 6.0.5. *The set of good apartments spans the Phan code in any rank* n*. In particular, there is a basis consisting only of good apartments for the Phan code.*

6.1 Coding theory implications

Below, we give a table showing the rate of the Phan code for different ranks. Let G_C denote the stabilizer of a chamber C in Γ.

n	weight	q	dimension	length	rate
	(n+1)!		$\chi(n)$	$\lvert G : G_C \rvert$	$\chi(n)/\lvert G : H \rvert$
2	6	q	polynomial in q	polynomial in q	
			$q^2(q^2-q+1)(q^2-q-2)+1$	$q^3(q-1)(q^2-q+1)$	
		3 4	253 2079	378 2496	253/378 2079/2496
3	24	q	$q^5(q-1)(q^2+1)(q^2-q+1)(q^2-q-3)+q^3(q^2+1)(q^3-q^2+3q-2)-1$	$q^6(q-1)^2(q^2+1)(q^2-q+1)$	
		4	6175487	8146944	6175487/8146944

From the table above, we see that as q increases, asymptotically, the rate tends to 1. This tells us that a high fraction of the code symbols carry information. The code is able to correct $e = \lfloor((n+1)! - 1)/2\rfloor$ errors and detect $(n+1)! - 1$ errors. However, we suspect that its error correcting capability relative to its length would not be as good as that of the Hamming and Golay codes owing to the fact it is less symmetric.

Bibliography

[1] P. Abramenko, K. S. Brown, *Buildings: Theory and Applications*, Springer 2008.

[2] M. Aschbacher, *Notes on the Curtis-Tits-Phan theorems*, unpublished notes.

[3] E. Assmus, J. Keys, *Designs and their Codes*, Cambridge Tracts in Mathematics, Vol 103, Cambridge Univ. Press, Cambridge, 1992.

[4] R. W. Carter, *Simple Groups of Lie type*, John Wiley & Sons Ltd, London,1972.

[5] C. D. Bennett, S. Shpectorov, *A new proof of a theorem of Phan*, J. Group Theory **7** (2004), 287-310.

[6] N. Bourbaki, *Lie Groups and Lie Algebras: Chapters* $4-6$, (trans.), in Elements of Mathematics, Springer-Verlag, Berlin, Heidelberg, 2008.

[7] C. W. Curtis, I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders*, Volume II, John Wiley and sons, New York, 1994.

[8] K. M. Das, *Homotopy and homology of p-group complexes*, Ph.D. thesis, Caltech (1994).

[9] A. Devillers, R. Gramlich, B. Mühlherr, *The Sphericity of the complex of non-degenerate subspaces*, J. Lond. Math. Soc. **79** (2009), 684-700.

[10] K. Phan, *On groups generated by three-dimensional special unitary groups I*, J. Austral. Math. Soc. **23** (Series A) (1977), 67-77.

[11] K. Phan, *On groups generated by three-dimensional special unitary groups II*, J. Austral. Math. Soc. **23** (Series A) (1977), 129-146.

[12] M. Ronan, *Lectures on Buildings*, (Revised), The University of Chicago Press, Chicago, 2009.

[13] S. D. Smith, *On Decomposition of Modular Representations from Cohen-Macaulay geometries*, J. Algebra **131** (1990), 598-625.

[14] S. D. Smith, S. Yoshiara, *Group Geometries and Error Correcting Codes*, Journal of Algebra **175** (1995), 199-211.

[15] L. Solomon, *The Steinberg Character of a Finite Group with a BN-Pair*, in Theory of Finite Groups, (R. Brauer and C. Sah, (Editors)), pp 213-221, Benjamin, New York, 1969.

[16] E. H. Spanier, *Algebraic Topology*, McGraw-Hill Inc., New York, 1966. Berlin, 1963.

[17] R. M. Weiss, *The Structure of Spherical Buildings*, Princeton University Press, Princeton, 2003.