Distinct Difference Configurations in Groups

Royal Holloway, University of London

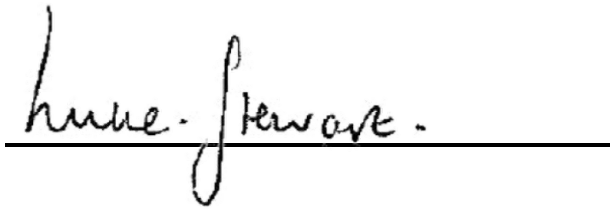
Thesis submitted towards the degree of Doctor of Philosophy

Luke Stewart

For my Parents

Declaration of Authorship

I, Luke Stewart, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed: 

Date: 2nd April 2023

Acknowledgements

Firstly, I would like to thank my supervisor Professor Simon Blackburn, who has devoted a great deal of time and effort to guiding me throughout this project. His patience in addition to his incisive comments have not only had a beneficial effect upon this thesis but also my own mathematical ability. He has shown a great deal of commitment without which the project would not have been possible.

I am enormously grateful to my family, who have been a constant source of support throughout, helping me both deal with frustrations and celebrate the various high points along the way. They were always there when I needed them.

I would like to thank my friends, fellow Centre for Doctoral Training students, my advisor Professor Keith Martin, and the various staff members who have made it such a pleasure to work at Royal Holloway. Special mentions must go to Marcel Armour and Simon Butler, as the many games of tennis and pool made student life that much better!

Finally, I would like to thank the EPSRC for providing me with the opportunity to

carry out this research project.

Abstract

A *distinct difference configuration* is a set of elements contained in a (finite or infinite) group such that the differences between those elements are pairwise distinct. Such configurations may be used to create key predistribution schemes for wireless sensor networks. After detailing preliminary results and describing the applications, we consider distinct difference configurations in the free group. This has applications to networks distributed in a tree-like structure in addition to being an extreme case combinatorially speaking and therefore mathematically interesting in its own right. Furthermore, our results on the free group inform our results on other groups. We provide upper bounds on the number of elements contained in a distinct difference configuration in the free group, in addition to constructions which provide lower bounds. We then consider distinct difference configurations in all groups before looking at the group $\mathbb{Z}^n$, rather than restricting ourselves to the group $\mathbb{Z}^2$ as much of the existing literature does. Next, we consider a natural generalisation of a distinct difference configuration which we call a *difference from unique pair configuration*. We describe the relation between these two objects and their appropriateness for use in key predistribution in wireless sensor networks. Finally, we outline some open problems which are worthy of further study.

Contents

Notation

We provide a table defining the notation used throughout the thesis, including where it first appears.

Notation	Definition	Page
G	An arbitrary group.	22
S	A generating set of a group G.	22
m	The number of elements in a configuration.	11
r	The maximum distance between a pair of elements in a set.	12
n	The cardinality of the generating set (not including inverses).	45
F_n	The free group with n generating elements.	45
X	The generating set of F_n (not including inverses).	45
$X^{\pm 1}$	The generating set of F_n (including inverses).	37
e	The identity element in a group G.	31
$D(x,y)$	The difference between two elements x, y with $D(x,y) = x^{-1}y$.	22
$d(x,y)$	The distance between two elements x, y.	22
$\mathcal{B}_L$	$\mathcal{B}_L = \{g \in G \mid g = g_1 \cdot g_2 \cdots g_k$ where $g_i \in S$ and $k \leq L\}$.	34
$\mathcal{S}_L$	$\mathcal{S}_L = \{g \in G \mid d(e,g) = L\}$.	34
$\mathcal{B}_L(x)$	$\mathcal{B}_L(x) = \{g \in G \mid g = x \cdot g_1 \cdot g_2 \cdots g_k$ where $g_i \in S$ and $k \leq L\}$.	34
$\mathcal{S}_L(x)$	$\mathcal{S}_L(x) = \{g \in G \mid d(x,g) = L\}$.	34
$\mathcal{B}_L(x,y)$	$\mathcal{B}_L(x,y) = \{g \in G \mid g = x \cdot g_1 \cdot g_2 \cdots g_k$ where $g_i \in S$ and $k \leq \lfloor L \rfloor\} \cup \{g \in G \mid y \cdot g_1 \cdot g_2 \cdots g_l$ where $g_i \in S$ and $l \leq \lfloor L \rfloor\}$.	54
$\mathcal{S}_L(x,y)$	$\mathcal{S}_L(x,y) = \{g \in G \mid d(x,g) = \lfloor L \rfloor$ and $d(y,g) = \lfloor L \rfloor + 1\} \cup \{g \in G \mid d(y,g) = \lfloor L \rfloor$ and $d(x,g) = \lfloor L \rfloor + 1\}$.	54

Notation	Definition	Page
$\overline{\mathrm{DD}}(G, S, m, r)$	A set of cardinality m contained in a group G with generating set S such that the distance between a pair of elements in the set is of length at most r and the differences between any two different pairs of distinct elements are pairwise distinct.	24
D_x	In a $\overline{\mathrm{DD}}(G, S, m, 4)$, $D_x = \{x' \in X^{\pm 1} \colon xx' \in D, xx' \text{ reduced}\}$.	59
D_x	In a $\overline{\mathrm{DD}}(G, S, m, r)$, $D_x = \{x' \colon xx' \in D, xx' \text{ reduced}\}$.	79
$\widetilde{\mathrm{DD}}(G, S, m, r)$	A set of cardinality m contained in a group G with generating set S such that the distance between a pair of elements in the set is of length at most r and every difference corresponds to a unique pair of elements.	116

Chapter 1

Introduction

1.1 Wireless Sensor Networks

A wireless sensor network consists of a large number of low-power nodes with limited communication range used to measure and/or analyse complex physical phenomena [38]. Data is typically transmitted frequently between nodes within the network, and cryptography may be used to provide confidentiality, integrity, and authentication for transmitted data. Nodes are generally assumed not to possess enough computational power to perform public-key cryptography, and so symmetric keys must be used. Symmetric keys must therefore be pre-loaded onto the nodes prior to their distribution. This has given rise to a rich body of research literature on key predistribution, discussing issues such as the number of different keys required in a network and how to distribute these keys between the nodes. See [13], [29], [30] for a survey of key predistribution schemes. There are numerous applications of wireless sensor networks, such as monitoring habitat [37]

and weather conditions [23], and tracking animal migration [27].

While it is generally assumed that nodes are randomly distributed (for example, they may be dropped from an aeroplane), there are cases where the distribution is known in advance, and it is these instances that we are concerned with. Furthermore, we assume the nodes to be in a fixed position, rather than mobile. The motivation for exisiting work on this subject has arisen from *grid-based* networks, such as those in [2], [3]. Examples of such networks include those used to develop efficient irrigation techniques [21], monitor air pollution [28], and monitor landslides [25]. Distinct difference configurations can be used to construct key predistribution schemes for grid-based networks, and such networks may be represented by the square model. We now outline how this is done.

1.2 Applications to Grid-Based Networks

Square model: We tile the $\mathbb{Z}^2$ plane with unit squares, and view the points in $\mathbb{Z}^2$ as being the centres of these tiles. We consider two points to be adjacent exactly when their squares share an edge. The distance between neighbouring points is therefore 1, and the neighbourhood of a point $(i, j) \in \mathbb{Z}^2$ is the set of points $\{(i-1, j), (i, j-1), (i+1, j), (i, j+1)\}$. The *Manhattan distance* between two points (i_1, j_1) and (i_2, j_2) is defined as $d((i_1, j_1), (i_2, j_2)) = |i_2 - i_1| + |j_2 - j_1|$.

We follow the notation of [3] in Definition 1.2.1.

Definition 1.2.1. A *distinct difference configuration* $\overline{\mathrm{DD}}(m, r)$ is a set of m dots placed

on a (possibly infinite) square grid such that the following two conditions hold:

1) Any pair of dots in the configuration is of Manhattan distance at most r apart,

2) All $\binom{m}{2}$ straight lines between pairs of dots are distinct in either length or gradient.

If we select a square on the grid to be the origin, then we can consider the dots to be a set of distinct vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ in $\mathbb{Z}^2$. For the dots to form a $\overline{\mathrm{DD}}(m, r)$, we require that for any pairs of vectors $\mathbf{v}_i, \mathbf{v}_j$ and $\mathbf{v}_k, \mathbf{v}_l$ such that $i \neq j$ and $k \neq l$, if $\mathbf{v}_i - \mathbf{v}_j = \mathbf{v}_k - \mathbf{v}_l$ then $i = k$ and $j = l$. Furthermore, $||\mathbf{v}_i - \mathbf{v}_j|| \leq r$. We do not permit the pair $\mathbf{v}_i = \mathbf{v}_j$ in general.[1]

Let K be a finite set, where each element of K corresponds to a key, N a set of nodes (each of which is capable of storing m keys), and W a wireless sensor network formed by the nodes in N after deployment.

Definition 1.2.2. A key predistribution scheme for W is a map $N \to K^m$ that assigns at most m keys in K to each node in N.

In [2] Blackburn et al. create a key predistribution scheme on the $\mathbb{Z}^2$ grid in which $N = \mathbb{Z}^2$ (so that every square in the grid contains a node) as follows:

Construction 1.2.3. **[2]** Let $D = \{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_m\}$ be a distinct difference configuration, and label every node in N by its position. For every shift $\mathbf{u} \in \mathbb{Z}^2$ generate a key $k_{\mathbf{u}}$, and assign $k_{\mathbf{u}}$ to the nodes labelled $\mathbf{u} + \mathbf{d}_i$, where $i = 1, 2, \ldots, m$.

Remark 1.2.4. If the grid is not infinite, 'edge cases' appear. This means that keys are assigned to positions outside the grid, and leads to some nodes storing a key which

[1] Note that there are $m(m-1)$ difference vectors, as order matters when the dots are considered as vectors.

is shared with fewer than $m-1$ (possibly zero) other nodes, leading to inefficient key storage. However, such edge cases will typically represent a very small proportion of the network, and so for the simplification of analysis we ignore such cases.

In Example 1.2.5 below, we give an example of a distinct difference configuration and how it may be used to distribute keys in a grid-based network using Construction 1.2.3.

Example 1.2.5. The set of dots {(1,0), (0,1), (2,2)} forms a $\overline{\mathrm{DD}}(3,3)$.

Vectors	**Manhattan Dist.**	**Grad.**
$(0,1),(1,0)$	2	-1
$(0,1),(2,2)$	3	1/2
$(1,0),(2,2)$	3	2

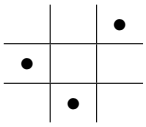


Figure 1.1: A $\overline{\mathrm{DD}}(3,3)$.

S		H	K		M		D
F	Z	Q		C	I	N	O
α			D	H	A		L
C	R	F	P	G		I	B
Q	A	β		T	D	U	
γ		C	B	E		G	J
T			A	X		Y	
P	δ	ϵ	U	V	B	E	W

Figure 1.2: Distribution of keys based on Figure 1.1 and Construction 1.2.3.

We begin by setting the node in the bottom left corner of the grid to be at $(0,0)$ and superimposing the dots in Figure 1.1 onto the grid. Assign the key A to the nodes which coincide with our initial placement of the dots. Shift the dots by $(1,0)$ and assign the key B to the nodes which coincide with the new placement of the dots. We continue in this way for all possible shifts, assigning a different letter to each key. After all such shifts are completed, each node has been assigned 3 keys. The node at $(2,2)$ stores the keys {A, G,

H}, the node at $(3,1)$ stores the keys {G, J, U}, and the node at $(1,3)$ stores the keys {H, K, Q}. Thus, the node at $(2,2)$ can communicate with the nodes at $(1,3)$ and $(3,1)$ as they share the key H and G respectively. However, the nodes at $(1,3)$ and $(3,1)$ cannot communicate with each other as they do not share a key and are at distance 4 apart.

Lemma 1.2.6. **[2]** *Let $D = \{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_m\}$ be the set of positions of dots in a distinct difference configuration. Suppose D is translated by a vector $\mathbf{v}$ in the lattice $\mathbb{Z}^2$ and let $D' = \{\mathbf{d}_1 + \mathbf{v}, \mathbf{d}_2 + \mathbf{v}, \ldots, \mathbf{d}_m + \mathbf{v}\}$ be the set of positions of dots in the translated configuration. Then if $\mathbf{v} \neq 0$, we have $|D \cap D'| \leq 1$.*

This lemma ensures that a pair of nodes share at most one key.

Theorem 1.2.7. **[2]** *If* Construction 1.2.3 *is applied to a $\overline{\mathrm{DD}}(m,r)$, then the resulting key predistribution scheme has the following properties:*

1) *Each node is assigned m different keys.*
2) *Each key is assigned to m different nodes.*
3) *Any two sensors have at most one key in common.*
4) *The distance between two sensors which have a common key is at most r.*
5) *Each node can communicate with at most $m(m-1)$ other nodes.*

Proof.

1) There are m dots in a $\overline{\mathrm{DD}}(m,r)$. For each dot, there is exactly one shift $\mathbf{u} \in \mathbb{Z}^2$ such that the dot is placed over a given node in the network. Placing a dot over a node assigns one key to that node, and so m dots means each node stores m keys. As each shift

corresponds to a different key, the keys assigned to a given node are pairwise distinct, and so each node stores m different keys.

2) A key $k_{\mathbf{u}}$ is assigned to m positions in the grid, namely those that coincide with the dots after a shift by $\mathbf{u}$.

3) Let $D = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ be a $\overline{\mathrm{DD}}(m, r)$. Suppose towards a contradiction that we have two different nodes at positions $\mathbf{x}$ and $\mathbf{y}$ that share two keys, $k_{\mathbf{u}_1}$ and $k_{\mathbf{u}_2}$. Then we have the following:

$$\mathbf{x} = \mathbf{u}_1 + \mathbf{v}_1 \ for\ some\ \mathbf{v}_1 \in D,\ as\ \mathbf{x}\ stores\ k_{\mathbf{u}_1}, \tag{1.1}$$

$$\mathbf{x} = \mathbf{u}_2 + \mathbf{v}_2 \ for\ some\ \mathbf{v}_2 \in D,\ as\ \mathbf{x}\ stores\ k_{\mathbf{u}_2}, \tag{1.2}$$

$$\mathbf{y} = \mathbf{u}_1 + \mathbf{v}_3 \ for\ some\ \mathbf{v}_3 \in D,\ as\ \mathbf{y}\ stores\ k_{\mathbf{u}_1}, \tag{1.3}$$

$$\mathbf{y} = \mathbf{u}_2 + \mathbf{v}_4 \ for\ some\ \mathbf{v}_4 \in D,\ as\ \mathbf{y}\ stores\ k_{\mathbf{u}_2}. \tag{1.4}$$

Therefore, $\mathbf{y} - \mathbf{x} = \mathbf{v}_4 - \mathbf{v}_2$ and $\mathbf{y} - \mathbf{x} = \mathbf{v}_3 - \mathbf{v}_1$. As $\mathbf{u}_1 \neq \mathbf{u}_2$, equations (1.3) and (1.4) imply that $\mathbf{v}_4 \neq \mathbf{v}_3$. Similarly, (1.1) and (1.2) imply that $\mathbf{v}_1 \neq \mathbf{v}_2$. But the distinct difference property implies that if $\mathbf{v}_4 - \mathbf{v}_2 = \mathbf{v}_3 - \mathbf{v}_1$ and $\mathbf{v}_4 \neq \mathbf{v}_2$ and $\mathbf{v}_3 \neq \mathbf{v}_1$, then $\mathbf{v}_4 = \mathbf{v}_3$ and $\mathbf{v}_2 = \mathbf{v}_1$. As $\mathbf{v}_4 \neq \mathbf{v}_3$ and $\mathbf{v}_4 - \mathbf{v}_2 = \mathbf{v}_3 - \mathbf{v}_1$, this implies $\mathbf{v}_4 = \mathbf{v}_2$ or $\mathbf{v}_3 = \mathbf{v}_1$. In either case, we have $\mathbf{x} = \mathbf{y}$. But $\mathbf{x}$ and $\mathbf{y}$ are different nodes, and so we have a contradiction. Thus, any two sensors have at most one key in common.

4) This follows directly from the limit on the distances between dots in a $\overline{\mathrm{DD}}(m, r)$.

5) Each node stores m keys, each of which is shared with at most $(m-1)$ other nodes. We say 'at most' as it is possible that there is an 'edge case', where the key is assigned to a position outside the grid. By 3), any two nodes have at most one key in common. Each node thus shares a key with $m(m-1)$ nodes. By 4), nodes which share a key are within distance r of each other. Therefore, a given node shares a key with $m(m-1)$ different nodes within distance r, and so can communicate securely (due to sharing a key) with $m(m-1)$ other nodes. □

We now explain why the properties in Theorem 1.2.7 are desirable. If the maximum number of keys a node in our network can store is m, then by property 1 we can use a distinct difference configuration with m dots to maximise the number of keys stored whilst increasing the number of nodes each node can communicate with (as this grows with m by property 5). Now, consider property 3. If a pair of nodes have at most one key in common then we don't waste memory space by having a pair of nodes store multiple identical keys when only one shared key is needed to communicate. We get this property from the fact that translated distinct difference configurations overlap in at most one place. Finally, consider property 4. We can set r to be the communication range of the nodes, ensuring two nodes which share a key are never out of communication range. This prevents nodes from needlessly storing keys required to communicate with other nodes which are out of range. So we are storing as many keys as possible in as efficient a manner as possible. Note that we take *optimal* to mean that the value of m is as large as possible given the parameter r. This is because the greater the value of m, the greater the number

of nodes in the network that a given node can communicate with, and we typically wish to maximise this. Our constructions therefore seek to maximise the value of m. Note that there is a trade-off with the amount of memory storage used if we maximise m. However, as very little memory space is generally required to store keys we assume throughout that this is not an issue.

1.3 Other Related Work and our Contribution

There is an extensive body of literature regarding sets with distinct differences. In [5], Bose constructed a set of q elements in a finite field $\mathbb{F}_{q^2}$ whose (additive) differences are distinct. If a subset D of a group G is such that every non-identity element of G occurs an equal number of times as the difference of elements of D, then D is a *difference set*. Difference sets in both the abelian and non-abelian case are studied in [10].

Specific classes of distinct difference configurations have been investigated extensively. In [18], Golomb considers a set of integers $A = \{a_1, a_2, \ldots, a_m\}$ with the property that all differences $a_i - a_j$ with $1 \leq i \leq m$, $1 \leq j \leq m$ and $i \neq j$ and $i, j \in \{1, 2, \ldots, m\}$ are pairwise distinct. Such a set is called a *Golomb ruler*. This is a 1-dimensional distinct difference configuration. If $|A| = k$ then we say the Golomb ruler has *order* k, and the *length* of the Golomb ruler is the largest difference between any two elements of A. A ruler that measures all distances up to its length is said to be *perfect*. It has been proved that no perfect ruler of order 5 or greater exists [9]. A related definition is that of a *Sidon set*, which is a set of positive integers $B = \{b_1, b_2, \ldots ...b_m\}$ such that all sums $b_u + b_v$ with $1 \leq u \leq m$, $1 \leq v \leq m$ and $u \neq v$ and $u, v \in \{1, 2, \ldots, m\}$ are pairwise distinct. The

central problem concerning Sidon sets is to find how many terms a Sidon set may contain for a given upper bound k on the elements in the sequence. This problem is studied (for example) in [14]. All Sidon sets are Golomb rulers, and vice-versa. To see this, suppose towards a contradiction that B is a Sidon set and not a Golomb ruler. Then there exist $b_i, b_j, b_k, b_l \in B$ such that $b_i - b_j = b_k - b_l$. Then we have $b_i + b_l = b_k + b_j$, which contradicts our assumption that B is a Sidon set. Thus, a Sidon set is also a Golomb ruler. A similar argument proves the reverse implication, namely that all Golomb rulers are Sidon sets. In [19], Golomb and Taylor consider an $n \times n$ square grid with exactly one dot in each row and column such that all difference vectors are pairwise distinct (a *Costas array*). Golomb and Taylor showed that Costas arrays exist for $n = p-1, n = q-2, n = q-3$ and sometimes exist when $n = q - 4$ and $n = q - 5$, where p is a prime number and q is the power of a prime. In [15], Erdős et al. consider an $n \times m$ square grid with exactly one point in each column such that all difference vectors are pairwise distinct (a *sonar sequence*). Erdős et al. showed that, for fixed n, the maximal m for which a sonar sequence exists satisfies $n - Cn^{11/20} < m < n + 4n^{2/3}$ for all n and $m > n + c\log n \log\log n$ for infinitely many n.

The square model is not the only model. The *Hexagonal Model*, in which we tile the $\mathbb{R}^2$ plane with regular hexagons with side lengths of $\frac{1}{\sqrt{3}}$, has also been studied (see [2], [3]). Similarly to the square model, the dots are the centre of these hexagons, and two dots are adjacent if and only if their hexagons share an edge and the distance between neighbouring dots is 1. The *hexagonal distance* between two dots x and y is the smallest r such that there exists a path $p_1 p_2 \dots p_{r+1}$, where $x = p_1, y = p_{r+1}$ and p_i and p_{i+1} are adjacent dots. It is shown in [3] that the square model and hexagonal model are isomor-

phic. *Honeycomb arrays*, defined by Golomb and Taylor in [19], are a hexagonal analogue of Costas arrays, and are investigated in [4] and [32]. Additional classes of distinct difference configurations using the square and hexagonal model with different definitions of distance are discussed in [3]. We provide examples of a Golomb ruler, Costas array, sonar sequence, and honeycomb array in Figures 1.3, 1.4, 1.5, and 1.6 respectively.

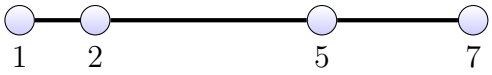


Figure 1.3: A perfect Golomb ruler of order 4.

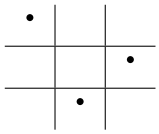


Figure 1.4: A Costas array forming a $\overline{\mathrm{DD}}(3,3)$.

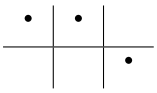


Figure 1.5: A sonar sequence forming a $\overline{\mathrm{DD}}(3,3)$.

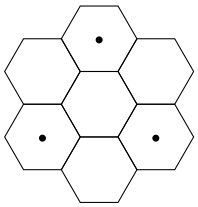


Figure 1.6: A honeycomb array of size 3

In [2], Blackburn et al. consider k-hop coverage in distinct difference configurations using the square model. The k-hop coverage of a distinct difference configuration is the number of distinct vectors that can be expressed as the sum of k or fewer difference vectors. The motivation for considering this parameter stems from its applications in wireless sensor networks. The greater the k-hop coverage, the greater the (expected) number of nodes which can be reached via a path of length k in the network. This has benefits in a wireless sensor network as it increases how efficiently data can be transmitted within a network. If fewer hops are required to transmit data throughout the network,

then fewer transmissions are required – this is particularly useful given our assumption that the nodes have limited power. The case where $k = 2$ has been studied by Stinson and Lee in [26], and in [12] Du et al. consider using two-hop paths as a secure means of data transmission between two nodes out of communication range in a wireless sensor network, rather than simply increasing the communication range of the nodes. In [16], Eschenauer and Gligor describe how multi-hop paths may be used to establish secure connections for the transmission of data where random key distribution is used. Using multi-hop paths with random key distribution as a means of secure communication is also discussed in [8]. In [7], Camtepe et al. consider multi-hop paths in the context of randomly distributed nodes with a deterministic key predistribution scheme.

1.3.1 Structure of the Thesis

The structure of this thesis is as follows. In Chapter 2, we give definitions of difference and distinct difference configurations which are applicable to all groups, rather than $\mathbb{Z}^2$ only. We also outline a key predistribution scheme analogous to that set out in Construction 1.2.3 which may be applied to any distinct difference configuration, rather than restricting ourselves to grid-based configurations. We then provide some preliminary results and background material on Cayley graphs which we make use of throughout the thesis. In Chapters 3, 4, 5, and 6 we consider distinct difference configurations in the free group. We include motivation for focussing on the free group in addition to background material required to understand the results. Our primary result states that for a distinct difference configuration in a free group with n generators and maximum distance r, there exists an upper bound on the number of elements m contained in the

distinct difference configuration such that $m \leq n^2 r(2n-1)^{\frac{r+5}{3}-2} + O(rn^{r/3})$ if r is even and $m \leq n^2(r+1)(2n-1)^{\frac{r+5}{3}-2} + O(rn^{\frac{r+1}{3}})$ if r is odd. In Chapter 7, we provide results which are applicable to distinct difference configurations contained in any given group. In Chapter 8, we consider the group $\mathbb{Z}^n$, and show that results which hold true in $\mathbb{Z}^2$ do not necessarily extend to $\mathbb{Z}^n$, in addition to providing our own results and constructions. These results are then applied to the dihedral group. Chapter 9 introduces the concept of a difference from unique pair configuration, a generalisation of our definition of a distinct difference configuration. We describe the relation between the two concepts, in addition to showing that difference from unique pair configurations are not as appropriate as distinct difference configurations for our applications to wireless sensor networks.

Chapter 2

Preliminaries

This chapter provides results we make use of throughout the thesis, in addition to some notation and background material required to understand the results and their applications. We begin with definitions and results which are a group-theoretic analogue of those which focus on the square grid discussed in Chapter 1.

2.1 Differences and DDCs

Definition 2.1.1. Let G be a group and S a generating set of G that is closed under inverses. For two elements $g_1, g_2 \in G$ we define the *left difference*, denoted $D_L(g_1, g_2)$, between g_1 and g_2 to be $g_1 \cdot g_2^{-1}$, and the *right difference*, denoted $D_R(g_1, g_2)$, to be $g_1^{-1} \cdot g_2$. The *distance* between g_1 and g_2, denoted $d(g_1, g_2)$, is the minimum number of elements (counting multiplicity) of the generating set in the representation of $g_1 \cdot g_2^{-1}$ (when considering left differences) or $g_1^{-1} \cdot g_2$ (when considering right differences) as a product of generators and their inverses.

Remark 2.1.2. While the convention is to consider left differences (see [11], [17], [24], [35], [39], for example), we will typically concern ourselves with right differences. We have a geometric justification for the use of right differences which we provide later in the chapter. We show below in Theorem 2.4.3 that choosing to use left or right differences does not affect any of our results.

Definition 2.1.3. Let G be a group, and let $D \subseteq G$. We say that D is a *distinct difference configuration* if, for every pair of elements $d_1, d_2 \in D$ such that $d_1 \neq d_2$, if there exists another pair of elements $d_3, d_4 \in D$ such that $d_3 \neq d_4$ and $d_3^{-1} \cdot d_4 = d_1^{-1} \cdot d_2$ then $d_3 = d_1$ and $d_4 = d_2$.

We now provide a small example of a distinct difference configuration.

Example 2.1.4. Let $D = \{(0,1,2), (1,2,0), (1,0,2)\} \subseteq \mathbb{Z}^3$ and label these elements as a, b, c respectively. We show that D forms a distinct difference configuration. Observe that $a^{-1} = (-a) = (0,-1,-2), b^{-1} = (-b) = (-1,-2,0), c^{-1} = (-c) = (-1,0,-2)$. The difference between a pair of elements in D is therefore one of the following:

Elements	**Difference Vector**
$a - b$	$(-1,-1,2)$
$a - c$	$(-1,1,0)$
$b - a$	$(1,1,-2)$
$b - c$	$(0,2,-2)$
$c - a$	$(1,-1,0)$
$c - b$	$(0,-2,2)$

These difference vectors are all pairwise distinct, so if for a pair of elements $d_1, d_2 \in D$ where $d_1 \neq d_2$ there exists another pair of elements $d_3, d_4 \in D$ where $d_3 \neq d_4$ such

that $d_3^{-1}d_4 = d_1^{-1}d_2$, then $d_3 = d_1$ and $d_4 = d_2$. Hence, D forms a distinct difference configuration.

We now define some notation. Let S be a generating set of G that is closed under inverses. If $|D| = m$ and D is a distinct difference configuration then we say that D is a $\overline{\mathrm{DD}}(G, S, m)$. Furthermore, if the maximum distance between any pair of elements $d_1, d_2 \in D$ is r, then we say that D is a $\overline{\mathrm{DD}}(G, S, m, r)$. We omit G and S from the notation where they are clear from the context.

Remark 2.1.5. By our definition of 'maximum distance', there is no requirement that a $\overline{\mathrm{DD}}(G, S, m, r)$ actually contains a pair of nodes at distance r apart. A $\overline{\mathrm{DD}}(G, S, m, r)$ is also a $\overline{\mathrm{DD}}(G, S, m, r')$ for all $r' \geq r$.

Before providing our key predistribution scheme, we require some background material on Cayley graphs, which we now provide.

2.2 Cayley Graphs

Definition 2.2.1. A *graph* Γ is a finite, non-empty set of *vertices*, together with a (possibly empty) set of unordered pairs of vertices of Γ, known as *edges*. The vertex set of Γ is denoted $V(\Gamma)$, and the edge set of Γ is denoted by $E(\Gamma)$.[1]

Definition 2.2.2. A graph in which the pairs of vertices corresponding to edges are ordered is a *directed graph*, and the edges are *directed edges*. The first vertex in the pair is called the *initial vertex*, and the second vertex the *terminal vertex*. Furthermore, the

[1]Note that our definition does not allow for loops, which are not needed for our application as a node need not communicate with itself – we therefore consider simple graphs throughout the thesis.

elements in the pair must be pairwise distinct. We also allow pairs of opposite directed edges – that is, edges containing the same pair of vertices but with the order reversed.

Remark 2.2.3. We use the notation (a, b) to denote a directed edge with initial vertex a and terminal vertex b. We do not allow multiple edges with the same initial and terminal vertex.

Let S be a finite generating set for a group G. We can construct a graph $\Gamma_{G,S}$ in which the vertices correspond to elements of G and for each $g \in G$ and $s \in S$, we insert a directed edge with initial vertex g and terminal vertex $g \cdot s$.

Definition 2.2.4. Let S be a finite generating set for a group G. We call the directed graph $\Gamma_{G,S}$ the *Cayley graph of G with respect to S* (or simply *Cayley graph* when G and S are clear from the context).

Sometimes, it will be convenient to draw parallel directed edges (i.e. two directed edges with the same pair of initial and terminal vertices, but opposite orderings) as an undirected edge (as in Figure 2.1).

Remark 2.2.5. Note that as we typically consider finite generating sets which are closed under inverses, if (a, b) is an edge in $\Gamma_{G,S}$ then (b, a) is also an edge. To see this, observe that we must have $a \cdot s = b$ for some $s \in S$ when (a, b) is an edge. As S is closed under inverses, we have $s^{-1} \in S$. Furthermore, $a = b \cdot s^{-1}$ and so $(b, a) \in E(\Gamma)$. We can therefore think of the Cayley graph in this case as a simple graph.

Example 2.2.6. Set $S = \{(12), (123), (132)\}$. This generates the symmetric group $S_3 = \{e, (12), (13), (23), (123), (132)\}$, where e is the identity element. We give the Cayley graph in Figure 2.1.

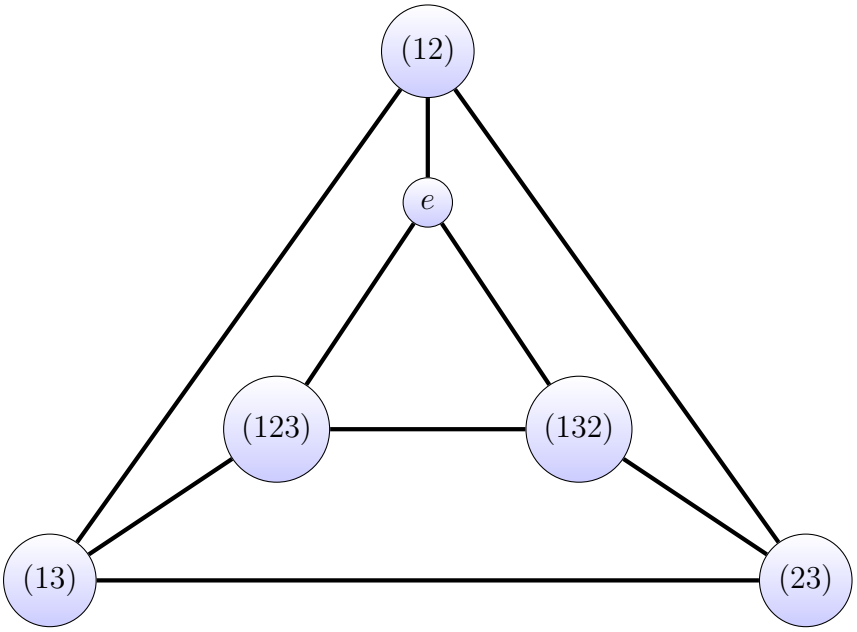


Figure 2.1: Cayley graph of S_3 and generating set $S = \{(12), (123), (132)\}$

Lemma 2.2.7. *Let G be a group and S a finite generating set of G. The Cayley graph $\Gamma_{G,S}$ is connected.*

Proof. Let $u, v \in V(\Gamma_{G,S})$. Observe that $u^{-1}v \in G$, and so can be written as the product of elements of S – say, $u^{-1}v = s_{i_1} \cdot s_{i_2} \cdot \ldots \cdot s_{i_k}$. Now, $u^{-1}v$ corresponds to a path in the Cayley graph from u to v, namely the path with vertex sequence $(u, u \cdot s_{i_1}, u \cdot s_{i_1} \cdot s_{i_2}, \ldots, u \cdot s_{i_1} \cdot s_{i_2} \cdot \ldots \cdot s_{i_k})$. That is, $u(s_{i_1} \cdot s_{i_2} \cdot \ldots \cdot s_{i_k}) = u(u^{-1}v) = v$, and so we have a path from u to v. Thus, the Cayley graph is connected. □

Remark 2.2.8. Note that the case where $G = \mathbb{Z}^2$ and $S = \{(\pm 1, 0), (0, \pm 1)\}$ produces a Cayley graph in the form of a square grid. This is why distinct difference configurations contained in $\mathbb{Z}^2$ have applications in grid-based networks.

2.3 Key Predistribution Scheme

We now provide a key predistribution scheme analogous to Construction 1.2.3. Our scheme is applicable to any distinct difference configuration contained in any group, rather than being restricted to $\mathbb{Z}^2$. A more generalised approach is useful as nodes are not necessarily arranged in a grid-like fashion as is the case with $\mathbb{Z}^2$. For example, a distinct difference configuration contained in $\mathbb{Z}^3$ introduces elevation. It is commonplace for nodes in a network to be at different heights due to the environment they are deployed in (such as hilly terrain), and so a scheme which takes account of this is likely to produce a key distribution which is closer to optimal in some circumstances. Furthermore, nodes may be distributed in a variety of patterns, rather than in the uniform pattern seen in the square grid. We see this in our study of the free group in Chapter 3, in which we consider nodes distributed in a tree-like pattern. A linear distribution of nodes is also plausible (for example, on a bridge) and so a distinct difference configuration in $\mathbb{Z}$ is likely to be a more appropriate group for such an application. Thus, it is useful to have a generalised predistribution scheme which can be adapted to a particular circumstance, rather than relying on the grid-based approach.

We use the following definition. For a group G, we can place a sensor node in every vertex in the Cayley graph of G. Denote the set of nodes by N. Two nodes are adjacent if their corresponding elements are adjacent in the Cayley graph. The distance between adjacent nodes is 1. The distance between a pair of nodes is the length of the shortest path between those nodes. This is equivalent to the definition of distance given in Definition 2.1.1.

Construction 2.3.1. Let G be a group and let $D = \{d_1, d_2, \ldots, d_m\}$ be a $\overline{\mathrm{DD}}(G, S, m, r)$. Label every node in N by its corresponding element in G. For every element $g \in G$, generate a key k_g and assign k_g to the nodes labelled $g \cdot d_i$ where $i \in \{1, 2, \ldots, m\}$.

Theorem 2.3.2. *If* Construction 2.3.1 *is applied to a* $\overline{\mathrm{DD}}(G, S, m, r)$*, then the resulting key predistribution scheme has the following properties:*

1) *Each node is assigned* m *different keys.*

2) *Each key is assigned to* m *different nodes.*

3) *Any two sensors have at most one key in common.*

4) *The distance between two sensors which have a common key is at most* r*.*

5) *Each node can communicate with at most* $m(m-1)$ *other nodes.*

Proof. The proof is similar to that of Theorem 1.2.7, however we include it for completeness.

1) There are m elements in a $\overline{\mathrm{DD}}(G, S, m, r)$. For each element, there is exactly one shift $g \in G$ such that the element is mapped to a given node in the network. Mapping an element of the configuration to a node assigns one key to that node, and so m elements means each node stores m keys. As each shift corresponds to a different key, the keys assigned to a given node are pairwise distinct, and so each node stores m different keys.

2) A key k_g is assigned to m positions in the network, namely those that coincide with the elements in the $\overline{\mathrm{DD}}(G, S, m, r)$ after multiplication by g (which are pairwise distinct).

3) Let $D = \{d_1, d_2, \ldots, d_m\}$ be a $\overline{\mathrm{DD}}(G, S, m, r)$. Suppose towards a contradiction that there are two different nodes corresponding to $x, y \in G$ that share two keys k_{g_1} and k_{g_2}. Then we have the following equations:

$$x = g_1 \cdot d_1 \text{ for some } d_1 \in D \text{ as } x \text{ stores } k_{g_1}, \tag{1}$$

$$x = g_2 \cdot d_2 \text{ for some } d_2 \in D \text{ as } x \text{ stores } k_{g_2}, \tag{2}$$

$$y = g_1 \cdot d_3 \text{ for some } d_3 \in D \text{ as } y \text{ stores } k_{g_1}, \tag{3}$$

$$y = g_2 \cdot d_4 \text{ for some } d_4 \in D \text{ as } y \text{ stores } k_{g_2}. \tag{4}$$

Therefore, $y^{-1}x = d_4^{-1}g_2^{-1}g_2d_2 = d_4^{-1}d_2$ and $y^{-1}x = d_3^{-1}g_1^{-1}g_1d_1 = d_3^{-1}d_1$. As $g_1 \neq g_2$, equations (3) and (4) imply that $d_3 \neq d_4$. Similarly, (1) and (2) imply that $d_1 \neq d_2$. But the distinct difference property implies that if $d_4^{-1}d_2 = d_3^{-1}d_1$ and $d_4 \neq d_2$ and $d_3 \neq d_1$, then $d_4 = d_3$ and $d_2 = d_1$. As $d_4 \neq d_3$ and $d_4^{-1}d_2 = d_3^{-1}d_1$, this implies $d_4 = d_2$ or $d_3 = d_1$. In both cases, we have $x = y$. But x and y are different nodes, and so we have a contradiction. Thus, any two sensors have at most one key in common.

4) This follows directly from the limit on the distances between elements in a $\overline{\mathrm{DD}}(G, S, m, r)$.

5) Each node stores m keys, each of which is shared with at most $(m-1)$ other nodes. By property 3, any two nodes have at most one key in common. Each node thus shares a key with $m(m-1)$ other nodes. By property 4, nodes which share a key are within distance r of each other. Therefore, a given node shares a key with $m(m-1)$ different nodes within distance r, and so can communicate with $m(m-1)$ other nodes. □

These properties are desirable for precisely the same reasons as in the grid-based case.

Note that with infinite groups, there are no 'edge cases'.

2.4 Preliminary Results

Theorem 2.4.1. *Let G be a group, $g \in G$, and $D \subseteq G$. Then D is a distinct difference configuration if and only if gD is a distinct difference configuration.*

Proof. We firstly prove the forward implication. Suppose $D = \{d_1, d_2, \ldots, d_m\}$ is a distinct difference configuration. Then $gD = \{g \cdot d_1, g \cdot d_2, \ldots, g \cdot d_m\}$. Suppose two differences in gD are equal. Then there exist $g \cdot d_i, g \cdot d_j, g \cdot d_k, g \cdot d_l \in gD$ such that $(g \cdot d_i)^{-1} g \cdot d_j = (g \cdot d_k)^{-1} g \cdot d_l$ where $i, j, k, l \in \{1, 2, \ldots, m\}$. Then $d_i^{-1} d_j = d_k^{-1} d_l$. But $d_i, d_j, d_k, d_l \in D$. As D is a distinct difference configuration, d_i, d_j, d_k, d_l must be such that $d_i = d_k$ and $d_j = d_l$ or $d_i = d_j$ and $d_k = d_l$ (in which case we have the trivial difference). If $d_i = d_k$ and $d_j = d_l$, then $g \cdot d_i = g \cdot d_k$ and $g \cdot d_j = g \cdot d_l$. Thus, if the differences between two pairs of elements in gD are equal, then either the pairs are the same or each pair consists of the same element twice, and so gD is a distinct difference configuration.

We now prove the reverse implication. Suppose $D = \{d_1, d_2, \ldots, d_m\}$ and that $gD = \{g \cdot d_1, g \cdot d_2, \ldots, g \cdot d_m\}$ is a distinct difference configuration. By the forward implication, if gD is a distinct difference configuration, then $g^{-1}(gD) = D$ is also a distinct difference configuration. Hence, if gD is a distinct difference configuration then D is a distinct difference configuration and the result follows. □

Theorem 2.4.1 ensures that when we translate a distinct difference configuration by multiplying every element in the configuration by an element g of the group it is contained

in, the set gD forms a distinct difference configuration. This is analogous to performing 'shifts' in the grid case. Note that we use e to denote the identity element.

Theorem 2.4.2. *Let $D = \{d_1, d_2, \ldots, d_m\}$ be a $\overline{\mathrm{DD}}(G, m, r)$. Suppose D is translated by an element $g \in G$ to produce a distinct difference configuration $gD = \{g \cdot d_1, g \cdot d_2, \ldots, g \cdot d_m\}$. If $g \neq e$, then $|D \cap gD| \leq 1$.*

Proof. Suppose there exists $d_i, d_j, d_k, d_l \in D$ such that $gd_k = d_i$ and $gd_l = d_j$, so that $|D \cap gD| \geq 2$ and $gd_i, gd_j, gd_k, gd_l \in gD$. Then we have $D(gd_k, gd_l) = D(d_i, d_j) = d_i^{-1}d_j$ and $D(gd_i, gd_j) = d_i^{-1}g^{-1}gd_j = d_i^{-1}d_j$. So $D(gd_k, gd_l) = D(gd_i, gd_j)$. By Theorem 2.4.1, gD is a distinct difference configuration. So $gd_i = gd_k$ and $gd_j = gd_l$. Then $d_i = d_k$ and $d_j = d_l$, and so $g = e$. □

Theorem 2.4.2 shows that when we translate a distinct difference configuration D, the resulting distinct difference configuration gD overlaps in at most one element. This is analogous to Lemma 1.2.6 in the context of groups. As in the $\mathbb{Z}^2$ case, this ensures that a pair of nodes share at most one key after distribution. A pair of nodes need share only one key in order to communicate, and so this ensures that storage is not wasted by allowing a pair of nodes to share multiple identical keys.

We now provide a theorem which shows that a set of elements is a distinct difference configuration with respect to left differences if and only if it is a distinct difference configuration with respect to right differences. This means that the bound on the number of elements contained in a distinct difference configuration is unaffected by whether we consider right or left differences, and constructions which produce a distinct difference

configuration with respect to right differences also produce a distinct difference configuration with respect to left differences.

Lemma 2.4.3. *Let G be a group, and let $D \subseteq G$. Then D is a distinct difference configuration with respect to left differences if and only if D is a distinct difference configuration with respect to right differences.*

Proof. We firstly prove the forward implication. Suppose D is a distinct difference configuration with respect to left differences. Let $d_1, d_2, d_3, d_4 \in D$ such that $d_1^{-1}d_2 = d_3^{-1}d_4$ so that two pairs of elements in D have equal differences with respect to right differences. Then $d_3d_1^{-1}d_2 = d_4$ and so $d_3d_1^{-1} = d_4d_2^{-1}$. But D is a distinct difference configuration with respect to left differences, and so either $d_3 = d_4$ and $d_1 = d_2$ or $d_1 = d_3$ and $d_2 = d_4$. Thus, if the differences between two pairs of elements in D are equal with respect to right differences, then either the pairs are the same or the difference between the elements in each pair is the trivial difference e. Thus, if D forms a distinct difference configuration with respect to left differences, then D forms a distinct difference configuration with respect to right differences.

The proof of the converse implication is similar. □

The following example illustrates why right difference is the more 'natural' definition from a geometric perspective.

Example 2.4.4. Let G be a group, S a generating set of G, and let $a, b, c \in S$ where $a \neq b, a \neq c, b \neq c$ and $a \neq b^{-1}, a \neq c^{-1}, b \neq c^{-1}$. Then we have the subgraph of the Cayley graph $\Gamma_{G,S}$ shown in Figure 2.2.

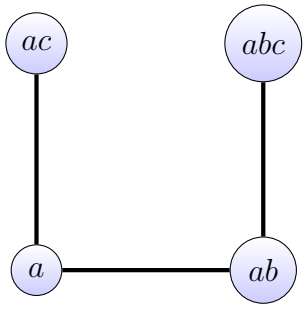


Figure 2.2: Subgraph of $\Gamma_{G,S}$

We have the following differences:

$$D_R(ac, abc) = c^{-1}a^{-1}abc = c^{-1}bc$$

$$D_R(abc, ac) = c^{-1}b^{-1}a^{-1}ac = c^{-1}b^{-1}c$$

$$D_L(ac, abc) = acc^{-1}b^{-1}a^{-1} = ab^{-1}a^{-1}$$

$$D_L(abc, ac) = abcc^{-1}a^{-1} = aba^{-1}.$$

When considering right differences, the difference formed by a pair of elements corresponds to the edges in the path from the first element in the pair to the second. When considering left differences, the difference between a pair of elements corresponds to a path from the second element to the first. Thus, we see from the Cayley graph that from a geometric perspective it is more intuitive to consider right differences.

Remark 2.4.5. Observe that the size of the balls and spheres of radius r are unaffected by where the centre of the ball or sphere is.

2.5 Maximum Distance and Balls of Radius r

We finish with a result that shows that a distinct difference configuration with maximum distance r is contained in a ball of radius r about an element of the group. We make use of this result in forming upper bounds on the number of elements m contained in a distinct difference configuration, and hence the number of nodes each node can communicate with and the number of keys assigned to each node. We begin by defining a sphere of radius L, and a related object, a ball of radius L.

Definition 2.5.1. Let G be a group, S a generating set of G, and $x \in G$. The *sphere of radius L about x* is defined as $\mathcal{S}_L(x) = \{g \in G | d(x, g) = L\}$.

Definition 2.5.2. Let G be a group, S a generating set of G, and $x \in G$. The *ball of radius L about x* is defined as $\mathcal{B}_L(x) = \{g \in G | d(x, g) \leq L\}$.

Note that we use $\mathcal{S}_L$ and $\mathcal{B}_L$ to denote the sphere of radius L about the identity element and ball of radius L about the identity element respectively.

Lemma 2.5.3. *Let G be a group and $D \subseteq G$ where the maximum distance between a pair of elements in D is r. Then D is contained in a ball of radius r.*

Proof. Consider an element $d \in D$. As the maximum distance between a pair of elements in D is r, every element in D is at distance at most r from d. Thus, every element in D is contained in the ball of radius r with centre d. □

Corollary 2.5.4. *Let G be a group and S a generating set of G. If D is a $\overline{\mathrm{DD}}(G, S, m, r)$, then D is contained in a ball of radius r.*

Proof. As D is a subset of G the result follows immediately from Lemma 2.5.3. □

Remark 2.5.5. Observe that for all vertices x, y in a Cayley graph, we have $|\mathcal{S}_L(x)| = |\mathcal{S}_L(y)|$ and $|\mathcal{B}_L(x)| = |\mathcal{B}_L(y)|$.

Chapter 3

The Free Group

We now consider distinct difference configurations in the free group. A widely known theorem states that the Cayley graph of a free group (on a free generating set) is a tree (see 3.1.20). Thus, if we wish to distribute the sensors in our network in the form of a tree (or a tree-like structure), then it is natural to consider free groups. A further motivation for the study of free groups is the following. In Chapter 6, we use the fact that all finitely generated groups can be written as the quotient of a free group to show that given a distinct difference configuration in a non-free group, we can produce a distinct difference configuration containing at least an equal number of elements in the free group. Finally, the free group is an 'extreme' case, combinatorially. So looking at the free group and understanding the tree structure is a natural combinatorial problem to consider when trying to understand distinct difference configurations in all finitely generated groups. We therefore focus on distinct difference configurations in free groups, before considering other types of groups.

We begin by providing some background material on the free group in Section 3.1. We then provide some preliminary results on the free group before considering configurations in which the maximum distance is small in Chapters 4 and 5. Finally, we consider the case where the maximum distance is of arbitrary size and provide upper and lower bounds on the number of elements contained in an optimal distinct difference configuration, in addition to providing a construction for a distinct difference configuration with $2n(2n-1)^{\lfloor \frac{r}{4} \rfloor - 1}$ elements in Chapter 6.

3.1 Background on the Free Group

We now provide some standard facts of the free group, some of which are taken from [34].

Definition 3.1.1. Let X be a non-empty set, and choose a set $X^{-1} = \{x^{-1} | x \in X\}$ which is disjoint from X with $|X^{-1}| = |X|$ where x^{-1} denotes the formal inverse of x. A *word* in X is a finite sequence $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}$ where $x_i \in X$ and $\varepsilon_i = \pm 1$ for $i \in \{1, 2, \ldots, r\}$, and $r \geq 0$. If $r = 0$ then this is the *empty word*, denoted e.

We denote the set $X \cup X^{-1}$ by $X^{\pm 1}$. Two words $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}$ and $v = y_1^{\mu_1} y_2^{\mu_2} \cdots y_s^{\mu_s}$ are equal if and only if elements in corresponding positions are equal – that is, $w = v$ if and only if $x_i^{\varepsilon_i} = y_i^{\mu_i}$ for all $i \in \{1, 2, \ldots, r\}$ and $r = s$.

The product of two words is defined by concatenation. So, $wv = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r} y_1^{\mu_1} y_2^{\mu_2} \cdots y_s^{\mu_s}$ with $we = ew = w$. Furthermore, the inverse of w, denoted w^{-1}, is given by $w^{-1} = x_r^{-\varepsilon_r} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1}$, and $e^{-1} = e$.

Let W denote the set of all words in X. We now define an equivalence relation on W. Two words $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}$, $v = y_1^{\mu_1} y_2^{\mu_2} \cdots y_s^{\mu_s}$ are equivalent if it is possible to transform one to the other by applying a finite sequence of the following operations:

i) insertion of xx^{-1} or $x^{-1}x$ where $x \in X$ as consecutive elements of a word,
ii) deletion of xx^{-1} or $x^{-1}x$ as consecutive elements.

We denote such a relation by $w \sim v$.

Theorem 3.1.2. *The relation $w \sim v$ is an equivalence relation.*

Proof. We first show that the relation is reflexive – that is, $w \sim w$. Applying the empty sequence of the above operations transforms w to w, and so $w \sim w$.

We now show that the relation is symmetric – that is, if $w \sim v$, then $v \sim w$. If $w \sim v$, then we can apply some finite sequence of the above operations to transform w to v. If we now replace every instance of an insertion of xx^{-1} in the sequence with a deletion of xx^{-1} (and vice-versa) and every instance of an insertion of an $x^{-1}x$ in the sequence with a deletion of $x^{-1}x$ (and vice-versa), and reverse the order in which the operations were applied, we obtain a sequence which transforms v to w. Therefore, $v \sim w$.

We now show that the relation is transitive – that is, if $w \sim v$ and $v \sim u$, then $w \sim u$. If $w \sim v$, then there is some finite sequence of the above operations $o_{i_1} o_{i_2} \cdots o_{i_k}$ that transforms w to v. If $v \sim u$, then there exists some finite sequence of the above operations

$o_{j_1}o_{j_2}\cdots o_{j_l}$ that transforms v to u. If we concatenate these two sequences to obtain $o_{i_1}o_{i_2}\cdots o_{i_k}o_{j_1}o_{j_2}\cdots o_{j_l}$ and apply this sequence of operations to w, then w is transformed to u via v, and so $w{\sim}u$.

The relation $w{\sim}v$ is therefore reflexive, symmetric, and transitive. Thus, it is an equivalence relation. □

The equivalence class to which a word w belongs is the set of all words which are equivalent to w, and is denoted $[w]$.

Definition 3.1.3. Let X be a non-empty set, F a group, $\sigma\colon X \to F$ a function, and G a group. Then (F, σ) (or simply 'F') is *free* on X if for each function $\alpha\colon X \to G$ there is a unique corresponding homomorphism $\beta\colon F \to G$ such that $\alpha = \sigma\beta$. A group which is free on some set is a *free group*.

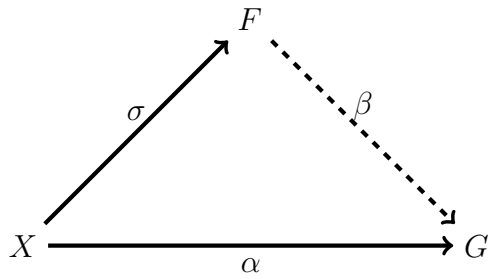


Figure 3.1: The relationship between sets and functions in a free group.

Theorem 3.1.4. *The function $\sigma\colon X \to F$ is injective.*

Proof. Suppose towards a contradiction that σ is not injective, so there exist $x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $\sigma(x_1) = \sigma(x_2)$. Let G be a group with at least two distinct elements

g_1, g_2 and choose a function $\alpha\colon X \to G$ such that $\alpha(x_1) = g_1$ and $\alpha(x_2) = g_2$. Then $\beta(\sigma(x_1)) = \beta(\sigma(x_2))$, and $\beta(\sigma(x_1)) = \alpha(x_1)$ and $\beta(\sigma(x_2)) = \alpha(x_2)$, and so $\alpha(x_1) = \alpha(x_2)$. But then $g_1 = g_2$, a contradiction. Thus, σ is injective. □

Definition 3.1.5. Let A and B be sets with $A \subseteq B$. The injection $f\colon A \to B$ defined by $f(a) = a$ for all $a \in A$ is the *inclusion map*, denoted Im f.

Theorem 3.1.6. [34] *If X is a non-empty set, then there exists a group F and a function $\sigma\colon X \to F$ such that (F, σ) is free on X and $F = \langle \text{Im } \sigma \rangle$.*

Proof. Define F to be the set of all equivalence classes of words in X. We now make F into a group. Observe that if $w{\sim}w'$ and $v{\sim}v'$, then $wv{\sim}w'v'$. We can therefore define the product of $[w]$ and $[v]$ as $[w][v] = [wv]$. Then we have $[w][e] = [e][w] = [w]$ and $[w][w^{-1}] = [ww^{-1}] = [e]$, and so $[e]$ is the identity and the inverse of $[w]$ is $[w^{-1}]$. We now show that the product is associative. As concatenation is associative, we have $(wv)u = w(vu)$ and so $([w][v]) \cdot [u] = [(wv)u] = [w(vu)] = [w] \cdot ([v][u])$. Thus, F is a group with respect to this binary operation.

Now, define a function $\sigma\colon X \to F$ by $\sigma(x) = [x]$. Let G be a group and suppose $\alpha\colon X \to G$ is a function. Construct a function $\overline{\beta}$ with domain the set of all words in X and range G which maps $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}$ to $g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_r^{\varepsilon_r}$ where $g_i = \alpha(x_i)$. If $w{\sim}v$, then $\overline{\beta}(w) = \overline{\beta}(v)$, as $gg^{-1} = g^{-1}g = e_G$, where e_G denotes the identity element in G. Therefore, we can now define a function $\beta\colon F \to G$ by $\beta([w]) = \overline{\beta}(w)$. Then $\beta(([w][v])) = \beta([wv]) = \overline{\beta}(wv) = \overline{\beta}(w)\overline{\beta}(v)$. Hence, $\beta([w][v]) = \beta([w])\beta([v])$ and β is a homomorphism from F to G. Furthermore, $\beta(\sigma(x)) = \beta([x]) = \overline{\beta}(x) = \alpha(x)$ for all

$x \in X$.

We now show that β is unique. If $\phi\colon F \to G$ is a homomorphism such that $\phi\sigma = \alpha$, then $\phi\sigma = \beta\sigma$ and ϕ and β agree on Im σ. By Theorem 3.1.2, every word in X generates the equivalence class it is contained in through a finite sequence of insertions or deletions of xx^{-1} or $x^{-1}x$ as consecutive elements with $x \in X$, and so $F = \langle \text{Im } \sigma \rangle$. Thus, $\phi = \beta$ and so β is unique. Therefore, (F, σ) is free on X. □

Definition 3.1.7. Let X be a non-empty set, and w a word in X. We say that w is *reduced* if it does not contain a pair of consecutive symbols of the form xx^{-1} or $x^{-1}x$ where $x \in X$. The empty word is considered reduced.

Example 3.1.8. Let X be a non-empty set, and let $x, y \in X$ with $x \neq y$. The word $xyx^{-1}y^{-1}$ is reduced, but the word $xyy^{-1}x$ is not.

Theorem 3.1.9. [34] *Let X be a non-empty set. Each equivalence class of words in X contains a unique reduced word.*

Proof. Let w be a word in X. We can delete all consecutive pairs of symbols xx^{-1} or $x^{-1}x$ in w (if any exist) to obtain an equivalent word. As words are of finite length, we can repeat this procedure finitely many times to obtain a reduced word equivalent to w. Thus, each equivalence class contains at least one reduced word. We now show that such a word is unique.

Let R be the set of all reduced words, $u \in X^{\pm 1}$, and define a function $u'\colon R \to R$

by:

$$u'(x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_r^{\varepsilon_r}) = \begin{cases} x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_r^{\varepsilon_r}u & \text{if } u \neq x_r^{-\varepsilon_r} \\ x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_{r-1}^{\varepsilon_{r-1}} & \text{if } u = x_r^{-\varepsilon_r} \end{cases}$$

where $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_r^{\varepsilon_r}$ is reduced.

Observe that as $(u^{-1})'$ is the inverse of u', we have that u' is a permutation of R. Consider the function from X to S_R (the symmetric group of R) defined by $x \mapsto x'$, and let F be the free group on R. Then by the defining property of a free group there exists a unique homomorphism $\theta\colon F \to S_R$ such that $\theta([x]) = x'$.

Let w and v be equivalent reduced words. Then $[w] = [v]$ and $\theta([w]) = \theta([v])$. If $w = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_r^{\varepsilon_r}$, then $[w] = [x_1^{\varepsilon_1}][x_2^{\varepsilon_2}]\cdots[x_r^{\varepsilon_r}]$ and $\theta([w]) = (x_1^{\varepsilon_1})'(x_2^{\varepsilon_2})'\cdots(x_r^{\varepsilon_r})'$. If we apply $\theta([w])$ to the empty word, then we obtain $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_r^{\varepsilon_r} = w$, as this is reduced. Similarly, $\theta([v])$ maps the empty word to v. Therefore $v = w$, and so the reduced word must be unique. □

By Theorem 3.1.9, every element of the constructed free group F can be written in the form $[w]$, where $w = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_r^{\varepsilon_r}$, with $\varepsilon_i = \pm 1, i \in \{1, 2, \ldots, r\}, r \geq 0$ is a reduced word. By the definition of multiplication in F, we have $[w] = [x_1]^{\varepsilon_1}[x_2]^{\varepsilon_2}\cdots[x_r]^{\varepsilon_r}$. If we multiply consecutive terms involving the same element x_i, then after relabelling the x_i's we see that $[w]$ can be written in the form

$$[w] = [x_1]^{l_1}[x_2]^{l_2}\cdots[x_s]^{l_s}$$

where $s \geq 0, x_i \neq x_{i+1}$, and l_i is a non-zero integer. As the original reduced word can be reassembled from this, this expression is unique.

Simplifying notation, identify w with $[w]$. By this convention, each element of F can be uniquely written in the form

$$w = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s}$$

where $s \geq 0, l_i \neq 0$, and $x_i \neq x_{i+1}$. This is the *normal form* of w.

Example 3.1.10. Let X be a non-empty set, and $x, y \in X$ with $x \neq y$. Consider the word $w = xxxyyx^{-1}x^{-1}$ in X. The normal form of w is $x^4y^2x^{-2}$.

Theorem 3.1.11. [34] *Let G be a group and X a set with $X \subseteq G$, and assume that each element $g \in G$ can be uniquely written in the form $g = x_1^{l_1} x_2^{l_2} \cdots x_s^{l_s}$, where $x_i \in X, l_i \neq 0, x_i \neq x_{i+1}, i \in \{1, 2, \ldots, s\}$, and $s \geq 0$. Then G is free on X.*

Proof. Let F be a free group on X with $\sigma \colon X \to F$ the associated injection. By the mapping property, there is a homomorphism $\beta \colon F \to G$ such that $\sigma\beta \colon X \to G$ is the inclusion map. As $G = \langle X \rangle$ and F contains all reduced words in X, we have that β is surjective. The function β is injective as each reduced word has a unique corresponding normal form. □

We now provide an example of a free group.

Example 3.1.12. [34] Consider the functions α, β on the set $\mathbb{C} \cup \{\infty\}$ defined by

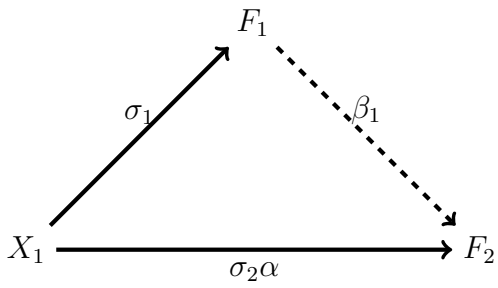
$$\alpha(x) = x + 2 \quad \textit{and} \quad \beta(x) = \frac{x}{2x + 1},$$

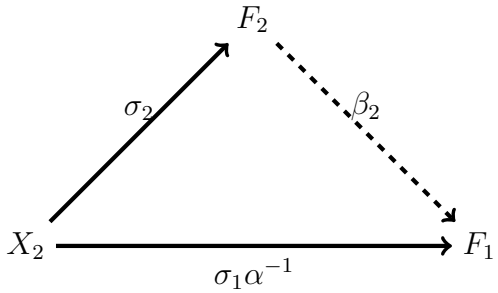
where ∞ is subject to the rules $1/0 = \infty$ and $\infty/\infty = 1$. As α and β have inverses, namely $\alpha^{-1}(x) = x - 2$ and $\beta^{-1}(x) = x/(1-2x)$, they are bijections. Therefore, α and β generate a group of permutations F of $\mathbb{C} \cup \{\infty\}$.

See page 48 of [34] for a geometric argument that no word can equal 1, and that every element of F has a unique expression as a reduced word. By Theorem 3.1.11, F is free on $\{\alpha, \beta\}$.

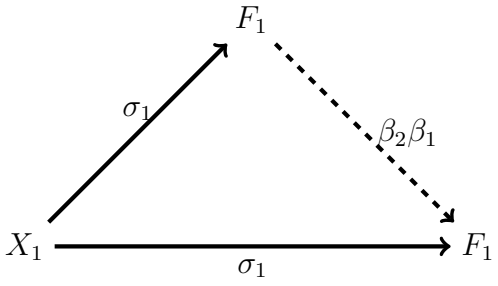
Theorem 3.1.13. [34] *Let F_1 be free on X_1 and F_2 be free on X_2 (where F_1 and F_2 denote arbitrary free groups). If $|X_1| = |X_2|$, then $F_1 \cong F_2$.*

Proof. Let $\sigma_1 \colon X_1 \to F_1$ and $\sigma_2 \colon X_2 \to F_2$ be the given injections and $\alpha \colon X_1 \to X_2$ be a bijection. Then we have the following commutative diagrams:





where β_1, β_2 are homomorphisms. Hence, $\sigma_1\beta_1\beta_2 = \alpha\sigma_2\beta_2 = \alpha\alpha^{-1}\sigma_1 = \sigma_1$. We therefore have the following commutative diagram:



Replacing $\beta_2\beta_1$ with the identity map e_{F_1} will make this diagram commute. As F_1 is free on X, the map $\beta_2\beta_1$ is the unique map such that $\beta_2\beta_1\sigma_1 = \sigma_1$, and so $\beta_2\beta_1 = e_{F_1}$. By a similar argument, $\beta_1\beta_2 = e_{F_2}$. Thus, β_1 is an isomorphism and $F_1 \cong F_2$. □

Theorem 3.1.14. *Let F_1 be free on X_1 and F_2 be free on X_2 (where F_1 and F_2 denote arbitrary free groups). If $F_1 \cong F_2$, then $|X_1| = |X_2|$.*

Remark 3.1.15. We assume throughout that the generating set of a free group F is the standard one – that is, for each element x in the generating set there is a unique corresponding formal inverse x^{-1}, and each inverse element corresponds to a single generating element.

Definition 3.1.16. Let F be a group which is free on a set X, with $|X| = n$. Then F has n generating elements, and we say that F has *rank* n. We denote this by F_n.

Remark 3.1.17. Note that in the case of the free group F_n, we can replace G and S in our $\overline{\mathrm{DD}}(G, S, m, r)$ notation and instead use $\overline{\mathrm{DD}}(F_n, m, r)$.

Theorem 3.1.18. *For $l \geq 1$, the number of reduced words of length l in F_n is $2n(2n-1)^{l-1}$.*

Proof. We have $2n$ 'letters' – n generators, and n inverses. The first letter of a word can be any of these $2n$ letters, and the only condition on each subsequent letter is that it must not be the inverse of the letter immediately before it (in order for the word to be reduced). Therefore, at each position in the word after the first letter there are $(2n-1)$ possibilities – we may have any letter except the inverse of the letter in the position immediately before. In a reduced word of length l, therefore, we have one letter (the first) for which

there are $2n$ possibilities, and $(l-1)$ letters for which there are $(2n-1)$ possibilities. Thus, the number of reduced words of length l is $2n(2n-1)^{l-1}$. □

Remark 3.1.19. Every vertex in the Cayley graph of a free group F_n has $2n$ 'in' edges and $2n$ 'out' edges – one for each generator, and one for each generator's inverse. To see this, observe that for a pair of vertices v_1 and $v_2 = v_1x$ where $x \in X^{\pm 1}$, there is an edge with initial vertex v_1 and terminal vertex v_2, and a corresponding edge with v_2 as the initial vertex and v_1 as the terminal vertex which represents multiplication of v_2 by x^{-1}. Therefore, each vertex is incident to exactly $4n$ directed edges. See Figure 3.2 as an example of this.

Lemma 3.1.20. *Let F be a group and X a generating set of F. If F is a free group then the Cayley graph $\Gamma_{F,X}$ is a tree.*

Proof. If F is a group which is free on a set X, then every element $g \in F$ may be written in the form $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_k^{\varepsilon_k}$ where $x_i \in X$, $\varepsilon_i = \pm 1$, $i \in \{1, 2, \dots, k\}$, $k \geq 0$, and $\varepsilon_i = \varepsilon_{i+1}$ if $x_i = x_{i+1}$. By Lemma 2.2.7, the Cayley graph $\Gamma_{F,X}$ is connected as X generates F.

Suppose towards a contradiction that $\Gamma_{F,X}$ is not a tree. Then $\Gamma_{F,X}$ contains a circuit, and so for some vertex $v_1 \in V(\Gamma_{F,X})$ there is a non-trivial path from v_1 to v_1, say $v_1v_2\dots v_lv_1$ where $l \geq 2$, which corresponds to $v_1 \cdot x_{j_1}x_{j_2}\cdots x_{j_{l-1}}$ where $x_{j_t} \in X^{\pm 1}, x_{j_t} \neq x_{j_{t+1}}^{-1}, t \in \{1, 2, \dots, l-1\}$.

As edges come in pairs, there are two different paths from v_1 to v_l – namely $v_1v_2\dots v_l$ and v_1v_l, so that $v_1 \cdot y = v_l$ for some $y \in X^{\pm 1}$ where $y \neq x_{j_1}$. Then we have the following

equation:

$$v_1 x_{j_1} x_{j_2} \cdots x_{j_{l-1}} = v_1 \cdot y.$$

Left multiplying by $(v_1)^{-1}$, we obtain

$$x_{j_1} x_{j_2} \cdots x_{j_{l-1}} = y.$$

Left multiplying by y^{-1}, we obtain

$$y^{-1} x_{j_1} x_{j_2} \cdots x_{j_{l-1}} = e.$$

Then as $y \neq x_{j_1}$ we have a non-empty reduced word which is equivalent to the empty word. As each equivalence class has a unique reduced word in the free group, the group is not free, a contradiction. Thus, the graph $\Gamma_{F,X}$ must be a tree. □

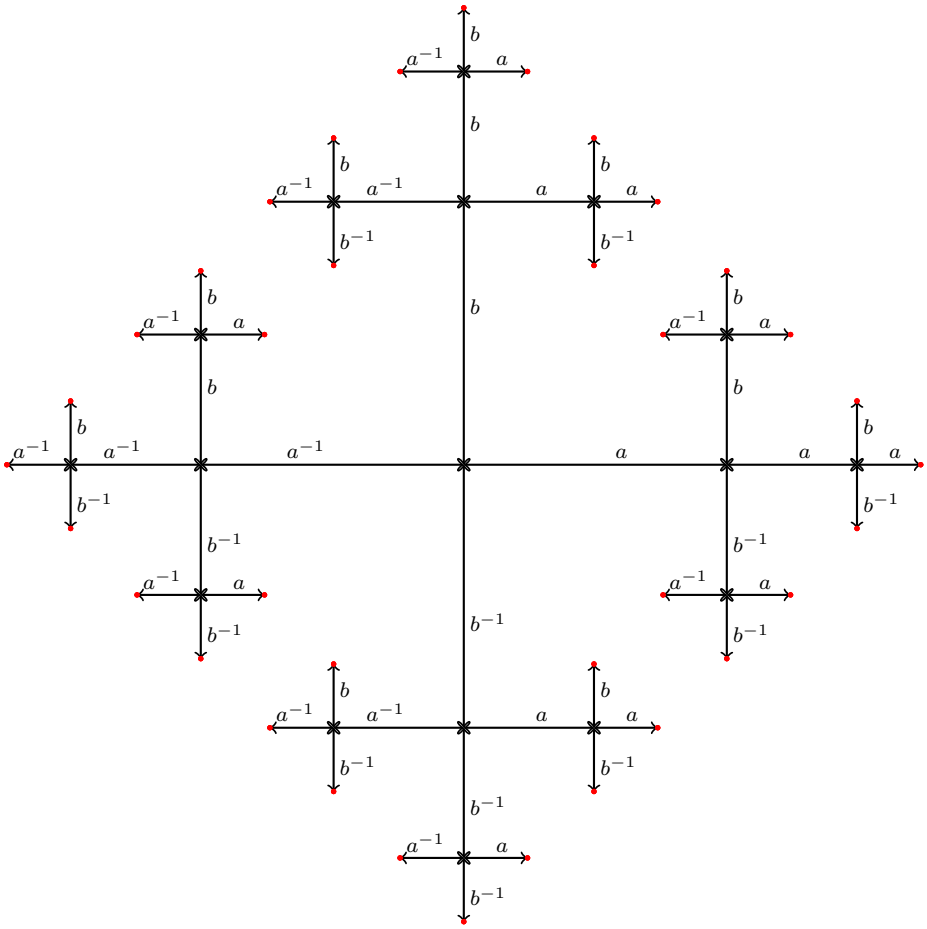


Figure 3.2: The Cayley graph of F_2

Chapter 4

Small Maximum Distances in the Free Group

We now consider distinct difference configurations contained in the free group. This chapter is concerned with distinct difference configurations in which the maximum distance between a pair of points is small. Considering configurations in which the maximum distance is small has applications in wireless sensor networks in which the communication range of the sensors is small. In addition to being interesting in their own right, the results for small distances can typically be extended to configurations with larger (including arbitrarily large) maximum distances. Note that the distance between a pair of nodes corresponds to the number of nodes on the unique shortest path between the nodes in the pair, and so smaller distances equates to fewer 'hops'.

4.1 Maximum Distance 2 in the Free Group

This section is concerned with the case where the maximum distance between a pair of points in a distinct difference configuration contained in the free group is 2 (note that the cases where the maximum distances are 0 and 1 are trivial as these produce configurations of a single element and a single pair of elements respectively). We show that a distinct difference configuration where the maximum distance between a pair of points is r is contained in a ball of radius $r/2$, and so a distinct difference configuration with maximum distance 2 is contained in a ball of radius 1. Furthermore, we provide an upper bound on the number of elements contained in such a configuration and describe the structure of a distinct difference configuration which meets this bound.

Theorem 4.1.1. *Let D be a $\overline{\mathrm{DD}}(F_n, m, r)$. Then D is contained in a ball of radius $r/2$.*

Proof. We can assume there exists a pair of elements $(d_1, d_2) \in D$ such that $d(d_1, d_2) = r$ (if no such pair exists then we are in the maximum distance $r-1$ case). Denote the unique shortest path from d_1 to d_2 by P_{d_1,d_2}, and label the mid-point of P_{d_1,d_2} as α so that $d(d_1, \alpha) = d(d_2, \alpha) = \frac{r}{2}$. Note that α is the centre of an edge if r is odd. We regard paths as a subset of vertices (so edges are not counted).

Let $d_3 \in D$ be such that $d_1 \neq d_3$ and $d_2 \neq d_3$. If $|P_{d_1,d_2} \cap P_{d_1,d_3}| = r+1$ or $|P_{d_1,d_2} \cap P_{d_2,d_3}| = r+1$, then $d_2 = d_3$ and $d_1 = d_3$ respectively, a contradiction. Furthermore, if $|P_{d_1,d_2} \cap P_{d_1,d_3}| = 0$, then d_3 is only reachable from d_2 via d_1 and so $d(d_2, d_3) > r$, a contradiction. Similarly, if $|P_{d_1,d_2} \cap P_{d_2,d_3}| = 0$, then $d(d_1, d_3) > r$, a contradiction. Thus, $r > |P_{d_1,d_2} \cap P_{d_1,d_3}| > 0$.

Let $|P_{d_1,d_2} \cap P_{d_1,d_3}| = k+1$, and p be the point such that $d(d_1, p) = k$ and $p \in P_{d_1,d_2}$. There are two possibilities: either $0 < k \leq r/2$ or $r/2 < k \leq r$. We consider each of these in turn.

$0 < k \leq r/2$: As $k \leq r/2$, we have $d(d_2, p) \geq r/2$ and $\alpha \in P_{d_2,d_3}$ (note that α is the mid-point of an edge between two points on the path if r is odd). As $\alpha \in P_{d_2,d_3}$ and $d(d_2, d_3) \leq r$ and $d(d_2, \alpha) = r/2$, we have $d(d_3, \alpha) \leq r/2$. Thus, if $0 < k \leq r/2$ then $d_3 \in \mathcal{B}_{r/2}(\alpha)$.

$r/2 < k \leq r$: We employ a similar argument. As $k > r/2$, we have $d(d_1, p) > r/2$ and $\alpha \in P_{d_1,d_3}$ (again, α is the centre of an edge on the path if r is odd). As $\alpha \in P_{d_1,d_3}$ and $d(d_1, d_3) \leq r$ and $d(d_1, \alpha) = r/2$, we have $d(d_3, \alpha) \leq r/2$. Thus, if $r/2 < k \leq r$ then $d_3 \in \mathcal{B}_{r/2}(\alpha)$.

Hence, $d_3 \in \mathcal{B}_{r/2}(\alpha)$, and so $D \subseteq \mathcal{B}_{r/2}(\alpha)$. □

We now present a lemma which states that if a $\overline{\mathrm{DD}}(F_n, m, 2)$ contained in a ball of radius 1 about an element $g \in F_n$ contains g (the element at the centre of the ball), then the upper bound on the number of elements in the configuration m is $n+1$. Furthermore, distinct difference configurations which meet this bound exist.

Lemma 4.1.2. *Let D be a $\overline{\mathrm{DD}}(F_n, m, 2)$ where $D \subseteq \mathcal{B}_1(g)$ and $g \in F_n$. If $g \in D$, then $m \leq n + 1$, where the bound is tight.*

Proof. We begin by showing that $m \leq n + 1$. By Theorem 2.4.1 we can translate any $\overline{\mathrm{DD}}(F_n, m, 2)$ contained in $\mathcal{B}_1(e)$ so that it is contained in $\mathcal{B}_1(g)$ (and vice-versa), whilst

retaining the distinct difference property. We can therefore assume without loss of generality that the centre of the ball is the identity element e. We have $\mathcal{B}_1(e) = e \cup X^{\pm 1}$. Consider $a, a^{-1} \in X^{\pm 1}$. We have $D(e, a) = a$ and $D(a^{-1}, e) = a$. Thus, for every generating element and it's corresponding inverse, D can contain at most one of those elements. As there are n generating elements (and inverses) in $X^{\pm 1}$, D can contain at most n elements from $X^{\pm 1}$, in addition to e. Hence, if D contains the element at the centre of the ball then D contains at most $n + 1$ elements and so $m \leq n + 1$.

We now prove that there exists a $\overline{\mathrm{DD}}(F_n, m, 2)$, say D^*, contained in $\mathcal{B}_1(g)$ with $g \in D^*$ and $|D^*| = n + 1$. Again, we can assume $g = e$. Set $D^* = e \cup X$, so that $|D^*| = n + 1$. We now show that D^* forms a $\overline{\mathrm{DD}}(F_n, m, 2)$. A pair of elements in D^* is either of the form (e, a) where $a \in X$ or (b, c) where $b, c \in X$. As above, we have $D(e, a) = a$ and $D(a, e) = a^{-1}$. Thus, the difference between a pair of elements containing e is of length 1 and uniquely defined by the corresponding generating element. Therefore, the difference between two different pairs of elements where both pairs contain e cannot be equal. Now, we have $D(b, c) = b^{-1}c$ and $D(c, b) = c^{-1}b$. Thus, the difference between a pair of distinct generating elements is of length 2, and so cannot be equal to the difference between a pair of elements containing e. Finally, consider the case in which two pairs of elements in X are equal where each pair consists of two distinct elements. Then for some $p, q, r, s \in X$ we have $D(p, q) = D(r, s)$. Then $p^{-1}q = r^{-1}s$. Left multiplying by p, we obtain $q = pr^{-1}s$. As $q \in X$, we have that q is of length 1. Thus, either $p = r$ or $r = s$. If $p = r$, then $q = s$, and so $(p, q) = (r, s)$ and the pairs are the same. If $r = s$, then $p = q$ and so we have the trivial difference in both pairs. Thus, D^* forms a $\overline{\mathrm{DD}}(F_n, m, 2)$. As $|D^*| = n + 1$ the

bound is tight. □

We now show that a large $\overline{\mathrm{DD}}(F_n, m, 2)$ is contained in the sphere $\mathcal{S}_1(g)$ for some $g \in F_n$.

Theorem 4.1.3. *Let D be a $\overline{\mathrm{DD}}(F_n, m, 2)$ where $n > 1$. Then $m \leq 2n$, and $m = 2n$ if and only if $D = \mathcal{S}_1(g)$ for some $g \in F_n$. Furthermore, if $n + 1 < m \leq 2n$ then $D \subseteq \mathcal{S}_1(g)$ for some $g \in F_n$.*

Proof. We first prove that $m \leq 2n$. By Theorem 4.1.1, $D \subseteq \mathcal{B}_1(g)$ for some $g \in F_n$. By Lemma 4.1.2, if $g \in D$ then $m \leq n + 1$. We have $\mathcal{B}_1(g) = g \cup \mathcal{S}_1(g)$, and so if $m > n + 1$ we must have $g \notin D$ and so $D \subseteq \mathcal{S}_1(g)$. As $|\mathcal{S}_1(g)| = 2n$, we have $m \leq 2n$ and equality can hold only if $D = \mathcal{S}_1(g)$.

We now show that $\mathcal{S}_1(g)$ forms a $\overline{\mathrm{DD}}(F_n, m, 2)$. If $\mathcal{S}_1(g)$ does not form a $\overline{\mathrm{DD}}(F_n, m, 2)$, then there exist two pairs of elements $(a, b) \in \mathcal{S}_1(g)$ and $(c, d) \in \mathcal{S}_1(g)$ such that $D(a, b) = D(c, d)$ where $a \neq b$ and $c \neq d$. By Theorem 2.4.1 we can assume without loss of generality that $g = e$, so $a, b, c, d \in X^{\pm 1}$. We have $a^{-1}b = c^{-1}d$. Left multiplying by a we obtain $b = ac^{-1}d$. As $b \in X^{\pm 1}$, we have that b is of length 1. Thus, either $a = c$ or $c = d$. If $a = c$ then $b = d$ and so $(a, b) = (c, d)$ and the pairs are the same. If $c = d$ then $a = b$ and so we have the trivial difference in both pairs. Thus, $\mathcal{S}_1(e)$ (and therefore $\mathcal{S}_1(g)$) forms a $\overline{\mathrm{DD}}(F_n, m, 2)$ with $m = 2n$. □

Remark 4.1.4. Note that in Theorem 4.1.3 we restrict ourselves to the case where $n > 1$ as we have $n + 1 = 2n$ when $n = 1$. If $n = 1$, then inspection of the Cayley graph will show that a $\overline{\mathrm{DD}}(F_1, m, 2)$ is such that $m \leq 2$. If $n = 1$ and $m = 2$ then the configuration

consists of a pair of nodes at distance either 1 or 2 apart. Furthermore, note that in the proof of Lemma 4.1.2 we have an example of a $\overline{\mathrm{DD}}(F_n, m, 2)$ where $m = n + 1$ such that $D \notin \mathcal{S}_1(e)$ but $D \subseteq \mathcal{B}_1(e)$ as $e \in D$. This is in contrast to the result for larger values of m in Theorem 4.1.3.

4.2 Maximum Distance 3 in a Free Group

This section is concerned with the case where the maximum distance between a pair of points in a distinct difference configuration contained in the free group is 3. We begin by providing an upper bound on the number of elements contained in such a configuration. We then provide some results describing the form of a configuration with size close to this bound.

We first define what we mean by a ball which has centre the mid-point of an edge contained in a group G with generating set S. The ball of radius L with centre the mid-point of the edge (a, b), denoted $\mathcal{B}_L(a, b)$, is defined as $\mathcal{B}_L(a, b) = \{g \in G | a \cdot g_1 \cdot g_2 \cdots g_k$ where $g_i \in S$ and $k \leq \lfloor L \rfloor\} \cup \{g \in G | b \cdot g_1 \cdot g_2 \cdots g_l$ where $g_i \in S$ and $l \leq \lfloor L \rfloor\}$. Similarly, we define the sphere of radius L about the mid-point of the edge (a, b), denoted $\mathcal{S}_L(a, b)$, as $\mathcal{S}_L(a, b) = \{g \in G | d(a, g) = \lfloor L \rfloor$ and $d(b, g) = \lfloor L \rfloor + 1\} \cup \{g \in G | d(b, g) = \lfloor L \rfloor$ and $d(a, g) = \lfloor L \rfloor + 1\}$.

Theorem 4.2.1. *Let D be a $\overline{\mathrm{DD}}(F_n, m, 3)$. Then $m \leq 2n + 1$, and the bound is tight.*

Proof. By Theorem 2.4.1 and Theorem 4.1.1 we can assume without loss of generality that D is contained in $\mathcal{B}_{1.5}(e, a)$ for some $a \in X^{\pm 1}$. We first show that $m \leq 2n + 1$. We

have that $\mathcal{B}_{1.5}(e,a) = X^{\pm 1} \cup aX^{\pm 1}$, and so $|\mathcal{B}_{1.5}(e,a)| = 4n$. We can therefore partition $\mathcal{B}_{1.5}(e,a)$ into n quadruples of the form $\{x, x^{-1}, ax, ax^{-1}\}$ where $x \in X$. Observe that $D(x, x^{-1}) = x^{-1}x^{-1} = D(ax, ax^{-1})$. Thus, D cannot contain such a quadruple, and so must contain at most 3 elements from every such quadruple. As there are n such quadruples and D can contain at most 3 elements from every quadruple, it follows that $m \leq 3n$. Now, observe that for $y, z \in X^{\pm 1}$ where $y \neq z$, we have $D(y,z) = y^{-1}z = D(ay, az)$. Therefore, D can contain at most one pair of elements of the form $\{y, ay\}$. For every quadruple $\{y, y^{-1}, ay, ay^{-1}\}$, any subset of size 3 contained in this quadruple contains either $\{y, ay\}$ or $\{y^{-1}, ay^{-1}\}$. As D can contain at most one such pair of elements, D must contain at most 2 elements from every such quadruple but one, which contains at most 3 elements. As there are n quadruples, we have $m \leq 2(n-1) + 3 = 2n + 1$. This establishes the upper bound. We now show that a configuration with $m = 2n + 1$ exists, and so the bound is tight.

Consider the set $X^{\pm 1} \cup \{aa\}$, which has size $2n + 1$. We show that this set forms a $\overline{\mathrm{DD}}(F_n, m, 3)$ with $m = 2n + 1$. The only differences of length 1 are $D(a, aa) = a$ and $D(aa, a) = a^{-1}$, which are pairwise distinct. The differences of length 2 are between pairs of elements (u, v) where $u, v \in X^{\pm 1}$. By Theorem 4.1.3, we have that all the differences of length 2 are pairwise distinct. The differences of length 3 are between pairs of elements of the form (u, aa) where $u \in X \backslash \{a\}$. Suppose towards a contradiction that there exist two different such pairs whose differences are equal. Then we have $u, v \in X^{\pm 1}$ with either $D(u, aa) = D(v, aa)$ or $D(u, aa) = D(aa, v)$. If $D(u, aa) = D(v, aa)$ then $u^{-1}aa = v^{-1}aa$ and so $u = v$. But then the pairs are not different, a contradiction. If $D(u, aa) = D(aa, v)$

then $u^{-1}aa = a^{-1}a^{-1}v$. Left multiplying by aa we obtain $aau^{-1}aa = v$. But the reduced form of $aau^{-1}aa$ is of length at least 3, whereas v is of length 1 as $v \in X^{\pm 1}$, and so we have a contradiction. Thus, two differences of length 3 formed by two different pairs of elements cannot be equal. Hence, $X^{\pm 1} \cup aa$ forms a $\overline{\mathrm{DD}}(F_n, m, 3)$ with $m = 2n + 1$, and so the bound is tight. □

We now provide a theorem which describes a condition that a large $\overline{\mathrm{DD}}(F_n, m, 3)$ must satisfy. Our proof of this theorem outlines the form a $\overline{\mathrm{DD}}(F_n, m, 3)$ must take.

Theorem 4.2.2. *Let D be a $\overline{\mathrm{DD}}(F_n, m, 3)$ where $D \subseteq \mathcal{B}_{1.5}(g_1, g_2)$ and $m > n + 1$. Then either $g_1 \notin D$ or $g_2 \notin D$.*

Proof. By Theorem 2.4.1 and Theorem 4.1.1 we can assume without loss of generality that D is contained in $\mathcal{B}_{1.5}(e, a)$ for some $a \in X^{\pm 1}$. This is because by Theorem 4.1.1 D is contained in a ball of radius 1.5 about the mid-point of an edge. Furthermore, by Theorem 2.4.1 we can translate a distinct difference configuration contained in $\mathcal{B}_{1.5}(g_1, g_2)$ so that it is contained in $\mathcal{B}_{1.5}(e, a)$ (without affecting the distinct difference property), with g_1 translated to e and g_2 translated to a. We have that $\mathcal{B}_{1.5}(e, a) = X^{\pm 1} \cup aX^{\pm 1}$, and so $|\mathcal{B}_{1.5}(e, a)| = 4n$. We can therefore partition $\mathcal{B}_{1.5}(e, a)$ into n quadruples of the form $\{x, x^{-1}, ax, ax^{-1}\}$ where $x \in X$. Suppose towards a contradiction that $e, a \in D$ and $m > n+1$. We now show that for each such quadruple (except $\{a, a^{-1}, aa, e\}$), if $e, a \in D$ then D can contain at most one element from that quadruple.

For each quadruple, there are $\binom{4}{2} = 6$ subsets of size 2. We consider each of these in turn:

(x, ax): $D(a, ax) = x = D(e, x)$. Therefore D cannot contain both x and ax.

(x, x^{-1}): $D(e, x) = x = D(x^{-1}, e)$. Therefore D cannot contain both x and x^{-1}.

(x, ax^{-1}): $D(a, ax^{-1}) = x^{-1} = D(x, e)$. Therefore D cannot contain both x and ax^{-1}.

(ax, x^{-1}): $D(x^{-1}, e) = x = D(a, ax)$. Therefore D cannot contain both ax and x^{-1}.

(ax, ax^{-1}): $D(a, ax) = x = D(ax^{-1}, a)$. Therefore D cannot contain both ax and ax^{-1}.

(x^{-1}, ax^{-1}): $D(e, x^{-1}) = x^{-1} = D(a, ax^{-1})$. Therefore D cannot contain both x^{-1} and ax^{-1}.

Hence, D cannot contain any subsets of size 2 contained in any of the $n-1$ quadruples. Therefore D contains at most one element from each of the $n-1$ such quadruples. Now, we have that $D(a, e) = a^{-1} = D(e, a^{-1})$, and so if $e, a \in D$ then D cannot contain a^{-1}. Similarly, we have $D(e, a) = a = D(a, aa)$, and so if $e, a \in D$ then $aa \notin D$. Thus, if $e, a \in D$ then D contains at most $n - 1 + 2 = n + 1$ elements, a contradiction. Hence, if $m > n + 1$ then either $e \notin D$ or $a \notin D$. The result follows by Theorem 2.4.1. □

Remark 4.2.3. The proof of Theorem 4.2.1 shows the form that every $\overline{\mathrm{DD}}(F_n, m, 3)$ with $m = 2n + 1$ must take. Suppose such a configuration is contained in $\mathcal{B}_{1.5}(e, a)$ for some $a \in X^{\pm 1}$. Then the configuration consists of at most $n - 1$ pairs of elements from $n - 1$ disjoint quadruples of the form $\{x, x^{-1}, ax, ax^{-1}\}$ for some $x \in X^{\pm 1}$ and one triple from the quadruple $\{y, y^{-1}, ay, ay^{-1}\}$ for some $y \in X^{\pm 1}$.

Chapter 5

Maximum Distance 4 in a Free Group

This chapter is concerned with the case where the maximum distance between a pair of points in a distinct difference configuration contained in the free group is 4. We separate this from the cases where the maximum distance is 2 or 3 as having a larger maximum distance allows us to formulate results and constructions which were either not possible with, or not applicable to, smaller distances. These results can also be extended to larger maximum distances. We begin with a theorem which states an if and only if condition a subset contained in a sphere of radius 2 about an element of the group must satisfy in order to form a distinct difference configuration. We use this condition in tandem with an upper bound on the number of edges in a bipartite graph with no 4-cycles to give an upper bound on the number of elements contained in such a configuration. We briefly describe affine planes and their properties as these are needed for our construction. We

then provide our construction, which we show produces a distinct difference configuration with the number of elements m close to the upper bound. Our construction is therefore useful for distributing keys in a network where we wish to maximise the number of nodes each node in the network can communicate with, as each node can communicate with $m(m-1)$ other nodes. Thus, it gives near-maximum connectivity.

We now introduce some notation. Let D be a $\overline{\mathrm{DD}}(F_n, m, 4)$. By Theorem 4.1.1, we have $D \subseteq \mathcal{B}_2(g)$ for some $g \in F_n$. Let $D \subseteq \mathcal{S}_2(g) = \mathcal{B}_2(g) \backslash \mathcal{B}_1(g)$. Define the following for every $x \in \mathcal{B}_1(g)$:

$$D_x = \{x' \in X^{\pm 1} \colon xx' \in D, xx' \textit{ reduced}\}.$$

Theorem 5.0.1. *Let $D \subseteq \mathcal{S}_2(g)$ for some $g \in F_n$. Then D is a distinct difference configuration if and only if $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_1(g)$ where $x \neq y$.*

Proof. We first prove the forward implication. That is, if $|D_x \cap D_y| \geq 2$ for some $x, y \in \mathcal{B}_1(g)$ where $x \neq y$, then D does not form a distinct difference configuration. If $|D_x \cap D_y| \geq 2$, then there exist elements $xz, xw, yz, yw \in D$ where $w, z \in D_x$ and $w, z \in D_y$ and $w \neq z$. As these words are reduced, they are pairwise distinct. But $D(xz, xw) = z^{-1}w = D(yz, yw)$, so the differences are not pairwise distinct and D does not form a distinct difference configuration. Thus, if $|D_x \cap D_y| \geq 2$ then D does not form a distinct difference configuration.

We now prove the reverse implication. That is, if $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_1(g)$ then D forms a distinct difference configuration. Note that D_g is the empty set, and so $|D_g \cap D_h| = 0$ for all $h \in \mathcal{B}_1(g)$. We now consider the elements in $\mathcal{S}_1(g)$. Every pair of elements in D is of the form (xx', yy') where $x', y' \in X^{\pm 1}$. There are three possible cases.

(i) If $x = y$ and $x' \neq y'$, then $D(xx', yy') = D(xx', xy') = x'^{-1}xxy' = x'^{-1}y'$, which has length 2.

(ii) If $x \neq y$, then $D(xx', yy') = x'^{-1}x^{-1}yy'$, which has length 4.

(iii) If $x = y$ and $x' = y'$, then $D(xx', yy') = e$, the trivial difference.

We now consider when a pair of differences can be equal. There are three possibilities; two differences of the form (i) are equal, one difference of the form (i) and one difference of the form (ii) are equal, or two differences of the form (ii) are equal. We consider each of these cases in turn. Note that if two different pairs of elements produce the trivial difference, this does not prevent D being a distinct difference configuration.

1 – two differences from (i): If two differences of the form (i) are equal, then for some $x, z \in \mathcal{B}_1(g)$ and $x', y', z', w' \in X^{\pm 1}$ we have $D(xx', xy') = x'^{-1}y' = z'^{-1}w' = D(zz', zw')$. Left multiplying by x', we obtain $y' = x'z'^{-1}w'$. As y' is of length 1, either $x' = z'$ or $z' = w'$. We consider each of these possibilities in turn.

If $x' = z'$, then $y' = w'$. Therefore $x', y' \in D_x \cap D_z$. As $|D_x \cap D_z| \leq 1$ if $x \neq z$, we must have either $x = z$ or $x' = y'$. If $x = z$ then since $x' = z'$ and $y' = w'$ we see that $xx' = zz'$ and $xy' = zw'$, and so the pairs are equal. If $x' = y'$, then $x' = y' = z' = w'$ and $D(xx', xy') = D(xx', xx') = D(zz', zw') = D(zz', zz') = e$, the trivial difference.

If $z' = w'$, then $x' = y'$ and so $xx' = xy'$ and $zz' = zw'$. Therefore $D(xx', xy') = D(zz', zw') = e$, the trivial difference.

Thus, if the differences between two pairs of elements of the form (i) are equal, then either the pairs must be equal or the difference between each pair of elements is the identity.

2 – one from (i) and one from (ii): Differences of the form in (i) are of length 2, and differences of the form (ii) are of length 4. Therefore, two such differences cannot be equal.

3 – two from (ii): Recall that g is the centre of the sphere with $D \subseteq \mathcal{S}_2(g)$, and so for a pair of elements $xx' \in D$ and $yy' \in D$ we have $xx' \in \mathcal{S}_2(g)$ and $yy' \in \mathcal{S}_2(g)$. We therefore have $d(g, xx') = d(g, yy') = 2$, and so $xx' = gx^*x'$ and $yy' = gy^*y'$ for some $x^*, y^* \in X^{\pm 1}$ with $x^* \neq y^*$. We therefore have $D(xx', yy') = x'^{-1}x^{*-1}g^{-1}gy^*y' = x'^{-1}x^{*-1}y^*y$, and this is reduced as the difference is of length 4. This difference therefore corresponds uniquely to the ordered pair of elements $gx^*x' = xx'$ and $gy^*y' = yy'$. Thus, every difference of length 4 between elements in D corresponds to a unique ordered pair of elements, and so the differences are pairwise distinct.

Hence, if $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_1(g)$ with $x \neq y$, then the differences formed by distinct pairs of elements in D are pairwise distinct, and so D forms a distinct difference configuration.

Hence, D is a distinct difference configuration if and only if $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_1(g)$ where $x \neq y$. $\square$

We now state a preliminary theorem we make use of in giving our upper bound.

Theorem 5.0.2. [33] *Let Γ be a bipartite graph with parts A and B where $|A| = |B| = k$. If Γ contains no 4-cycles, then $|E(\Gamma)| \leq \frac{k}{2}(1 + \sqrt{4k-3})$.*

Theorem 5.0.3. *If D is a $\overline{\mathrm{DD}}(F_n, m, 4)$, then $m \leq n(3 + \sqrt{8n-3})$.*

Proof. By Theorem 4.1.1, D is contained in $\mathcal{B}_2(g)$ for some $g \in F_n$. The number of elements contained in $\mathcal{B}_2(g) \backslash \mathcal{S}_2(g)$ (that is, $\mathcal{B}_1(g)$) is $2n+1$. By Theorem 4.1.3, the maximum number of elements in a distinct difference configuration contained in $\mathcal{B}_1(g)$ is $2n$. Thus, if M is an upper bound on the number of elements in a distinct difference configuration contained in $\mathcal{S}_2(g)$, then the number of elements m in a $\overline{\mathrm{DD}}(F_n, m, 4)$ has an upper bound of at most $M + 2n$. We now show that $n(1 + \sqrt{8n-3})$ is an upper bound on M.

Construct a bipartite graph β with parts A and B where $|A| = |B| = 2n$ as follows. Label the vertices in A by the elements in $X^{\pm 1}$, and label the vertices in B by the sets D_x, where $x \in \mathcal{S}_1(g)$. Insert an (undirected) edge incident to a vertex $v \in A$ and a vertex $D_x \in B$ if $xv \in D$. Note that $xv \in D$ if and only if $v \in D_x$. The number of edges in β is therefore equal to $|D \cap \mathcal{S}_2(g)|$. Now, by Theorem 5.0.1, we must have $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{S}_1(g)$ where $x \neq y$. Observe that there exists a 4-cycle in β if and only if $|D_x \cap D_y| = 2$ for some $x, y \in \mathcal{S}_1(g)$ where $x \neq y$. As D is a $\overline{\mathrm{DD}}(F_n, m, 4)$, there does not exist such a pair of elements x and y. Thus, β contains no 4-cycles. By Theorem 5.0.2,

we have $|E(\beta)| \leq \frac{2n}{2}(1+\sqrt{4(2n)-3}) = n(1+\sqrt{8n-3})$. Thus, $M \leq n(1+\sqrt{8n-3})$. As $m \leq M+2n$, we have $m \leq n(1+\sqrt{8n-3})+2n = n(3+\sqrt{8n-3})$. □

Remark 5.0.4. For sufficently large n, the upper bound in Theorem 5.0.3 approximates to $n\sqrt{8n}+3n = 2\sqrt{2}n^{3/2}+3n$.

Our construction makes use of affine planes. We therefore provide some background on affine planes, including some standard results and notation which we make use of in our construction.

Definition 5.0.5. Let $\mathcal{A}$ consist of a set of points P and a set of blocks which are subsets of P, and let two blocks be parallel if they are equal or disjoint. We say that $\mathcal{A}$ forms an *affine plane* if the following conditions are satisfied:

- Any two distinct points lie in a unique block,
- Each block contains at least two points,
- Given a point and a block, there is a unique block which contains that point and is parallel to the given block,
- There exist three points such that no block contains all three points.

Lemma 5.0.6. [6] *Let $\mathcal{A}$ be an affine plane containing a finite number of points. If there exists a block containing k points in $\mathcal{A}$, then the following are true:*

- *Each block contains k points,*
- *Each point is contained in $k+1$ blocks,*
- *There are k^2 points in $\mathcal{A}$,*
- *There are a total of k^2+k blocks.*

We refer to the number k in Lemma 5.0.6 as the *order* of $\mathcal{A}$.

Lemma 5.0.7. [6] *Let k be a prime power. Then there exists an affine plane of order k.*

5.1 Construction for $2n = q^2$

We begin with our construction for the case where $2n = q^2$. This is the ideal case, and we present a more complex version of this construction in the following section which produces a distinct difference configuration for the case where $2n \geq q^2$.

We now define some notation. Let $\mathcal{A}$ be an affine plane of order q, where q is a prime power. So $\mathcal{A}$ contains q^2 points and $q(q+1)$ blocks of size q. Let P denote the set of points and $\mathcal{L}$ denote the set of blocks. Choose a class of parallel blocks, call these the *blocks of infinite gradient*, and denote the class by $\mathcal{L}_\infty$. Let $\mathcal{L}\backslash\mathcal{L}_\infty$ denote $\mathcal{L}$ minus the blocks of infinite gradient. So $|\mathcal{L}\backslash\mathcal{L}_\infty| = q^2$.

Lemma 5.1.1. *If $\mathcal{A}$ is an affine plane of order q with q^2 points where $q^2 = 2n$ for some $n \in \mathbb{Z}$, then $n \geq q$.*

Proof. Suppose towards a contradiction that $n < q$. Then, as $2n = q^2$, we have $q^2 < 2q$, and so $q < 2$. Then q is at most 1. But $n < q$, and so $n < 1$. Then $n = 0$ and $q^2 = 0$ and so $n = q = 0$, a contradiction. Thus, $n \geq q$. □

We now define further notation before providing our construction. Let $\gamma\colon P \to X^{\pm 1}$ and $\varphi\colon X^{\pm 1} \to \mathcal{L}\backslash\mathcal{L}_\infty$ be bijections; note that $\varphi(x)$ is a block in $\mathcal{A}$, so $\varphi(x) \subseteq P$. As each point in the block is mapped to an element of $X^{\pm 1}$ by γ, we have the set $\gamma(\varphi(x)) \subseteq X^{\pm 1}$.

We say that a pair of bijections (γ, φ) is *inverse-avoiding* if $x^{-1} \notin \gamma(\varphi(x))$ for all $x \in X^{\pm 1}$. We show below in Theorem 5.1.4 that an inverse-avoiding pair (γ, φ) always exists.

Construction 5.1.2. Let (γ, φ) be inverse-avoiding. Set $D = \bigcup_{x \in X^{\pm 1}} x \cdot \gamma(\varphi(x))$.[1]

Theorem 5.1.3. Construction 5.1.2 *produces a* $\overline{\mathrm{DD}}(F_n, 2\sqrt{2}n^{3/2}, 4)$.

Proof. We first prove that our construction produces a distinct difference configuration D. As $\gamma(\varphi(x)) \subseteq X^{\pm 1}$ and all elements in $X^{\pm 1}$ are of length 1, and $x^{-1} \notin \gamma(\varphi(x))$, all elements in the set $x \cdot \gamma(\varphi(x))$ are of length 2. Thus, $D \subseteq \mathcal{S}_2(e)$. Note that $D_x = \varphi(B)$ where $B = \varphi(x)$ is a block. As the points contained in a pair of blocks intersect in at most one place in an affine plane, and γ is a bijection, $|D_x \cap D_y| \leq 1$ for all $x, y \in X^{\pm 1}$ where $x \neq y$. By Theorem 5.0.1, D forms a distinct difference configuration.

We now show that D has size $2\sqrt{2}n^{3/2}$. For each $x \in X^{\pm 1}$, we have $D_x = \gamma(\varphi(x))$. As each block in $\mathcal{A}$ is of size $q = \sqrt{2n}$, we have $|\gamma(\varphi(x))| = |D_x| = \sqrt{2n}$ for all $x \in X^{\pm 1}$. As $|X^{\pm 1}| = 2n$ and the sets xD_x are disjoint, D contains $|\bigcup_{x \in X^{\pm 1}} x \cdot D_x| = q^3 = 2n\sqrt{2n} = 2\sqrt{2}n^{3/2}$ elements. □

Theorem 5.1.4. *A pair of inverse-avoiding bijections* (γ, φ) *with* $\gamma \colon P \to X^{\pm 1}$ *and* $\varphi \colon X^{\pm 1} \to \mathcal{L} \backslash \mathcal{L}_\infty$ *always exists.*

Proof. We begin by providing an outline of the proof, which is in several stages. We first define a set Q which consists of q different pairs of elements of the form $\{x, x^{-1}\}$ and

[1] During the thesis examination, it was pointed out that it is possible to use a projective plane rather than an affine plane for our construction. As projective planes have greater intersection, for many values of n they will produce a larger distinct difference configuration. However, they never have an even number of points, and so this may not be the case for all values of n.

$Q \subseteq X^{\pm 1}$. We then show that there exist q pairs of distinct points $\{p, p'\} \in P$ where no pairs have a point in common such that the points p, p' are contained in a block of infinite gradient (and therefore not contained together in any other blocks). Further, using the fact that there exists a subset $Q \subseteq X^{\pm 1}$ containing q different pairs of elements of the form $\{x, x^{-1}\}$, there exists a bijection $\gamma : P \to X^{\pm 1}$ such that $\gamma(p) = x$ and $\gamma(p') = x^{-1}$ for some $x \in X^{\pm 1}$ for each of the q pairs of distinct points $\{p, p'\}$. We then seek to show that once we have a map γ with this property, we can find a map φ such that (γ, φ) is inverse-avoiding. We do this by partitioning $X^{\pm 1}$ and forming a preliminary bijection $\widehat{\varphi}$ which makes use of our partition. We can then use $\widehat{\varphi}$ to formulate a bijection φ such that (γ, φ) is inverse-avoiding. The maps $\widehat{\varphi}$ and φ are essentially similar as they map the elements of $X^{\pm 1}$ to the same parallel classes, however φ maps the elements of $X^{\pm 1}$ to the blocks within the parallel classes using a matching method which we describe in the proof.

Define $Q = \{x_1, x_2, \ldots, x_q, x_1^{-1}, x_2^{-1}, \ldots, x_q^{-1}\}$, so that Q consists of q different pairs of distinct elements of the form $\{x, x^{-1}\}$ and $Q \subseteq X^{\pm 1}$. As q is a prime power we have $q \geq 2$, so each block contains at least one pair of points. As the blocks in $\mathcal{L}_\infty$ are disjoint, we can choose a pair of points $\{p, p'\}$ from each of the q blocks in $\mathcal{L}_\infty$ and set $\gamma(p) = x$ and $\gamma(p') = x^{-1}$, where $x, x^{-1} \in Q$ and different pairs of points are mapped to different pairs of elements in Q. By the definition of an affine plane, if a pair of points $\{p, p'\}$ are contained together in a block then that block has infinite gradient. As each block in $\mathcal{L}_\infty$ intersects each block in $\mathcal{L} \backslash \mathcal{L}_\infty$ in at most one point, blocks in $\mathcal{L} \backslash \mathcal{L}_\infty$ contain at most one point in each of the q pairs of points in Q.

We now show that there exists a bijection $\varphi\colon X^{\pm 1} \to \mathcal{L}\backslash\mathcal{L}_\infty$ such that $x^{-1} \notin \gamma(\varphi(x))$ for all $x \in X^{\pm 1}$, where γ is as above.

As there are q pairs of elements of the form $\{x, x^{-1}\}$ in Q, we can partition $X^{\pm 1}$ into subsets $R_1, R_2, \ldots, R_q$ such that for all $i \in \{1, 2, \ldots, q\}$, the set R_i contains a pair of elements of the form $x, x^{-1} \in Q$ and $|R_i| = q$. Label the parallel classes in $\mathcal{A}$ not of infinite gradient (of which there are q) as $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_q$. We now define a bijection $\widehat{\varphi}$ which can be thought of as an approximation to φ, which we then use to show how to construct a map φ such that (γ, φ) is inverse-avoiding. Define $\widehat{\varphi}\colon X^{\pm 1} \to \mathcal{L}\backslash\mathcal{L}_\infty$ by requiring $\widehat{\varphi}(R_i) = \mathcal{C}_i$, so that each element in R_i is mapped to a block in $\mathcal{C}_i$, where different elements are mapped to different blocks so that $\widehat{\varphi}$ is a bijection.

Fix $R \in \{R_1, R_2, \ldots, R_q\}$ and let $\mathcal{C}$ denote the parallel class such that $\widehat{\varphi}(R) = \mathcal{C}$, so $\mathcal{C} \in \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_q\}$. Construct a bipartite graph with bipartitions of R and $\mathcal{C}$ as follows. The vertices in $\mathcal{C}$ are the blocks in $\mathcal{C}$, and the vertices in R are the elements of R. Join $x \in R$ to a block $B \in \mathcal{C}$ if $x^{-1} \notin \gamma(B)$. Consider $x \in R$, and recall that as the blocks in $\mathcal{C}$ are disjoint they partition the q^2 points in $X^{\pm 1}$. Thus, there exists a unique $B' \in \mathcal{C}$ such that $x^{-1} \in \gamma(B')$ for all $x \in X^{\pm 1}$. Hence, x is adjacent to all $B \in \mathcal{C}$ with $B \neq B'$. As $|\mathcal{C}| = q$, we have that every $x \in R$ has degree $q - 1$.

We now show that an R-saturating matching in our bipartite graph exists. By Hall's Marriage Theorem [22], such a matching exists if and only if for any subset $W \subseteq R$, we have $|N(W)| \geq |W|$, where $N(W)$ denotes the neighbourhood of W.

Trivially, $|N(\emptyset)| = |\emptyset|$. As every $x \in R$ has degree $q-1$, if W is a proper subset of R so that $|W| \leq q-1$, then we have $|N(W)| \geq |W|$. If $W = R$, then R contains a pair of elements $\{y, y^{-1}\} \in Q$ by our partition of $X^{\pm 1}$. Recall that no block in $\mathcal{L} \backslash \mathcal{L}_\infty$ contains the pair of points $\{p, p'\} \in P$ such that $\gamma(p) = y$ and $\gamma(p') = y^{-1}$. So, every block in $\mathcal{C}$ is adjacent to either y or y^{-1}. Recall that every point is contained in precisely one block per parallel class. Let $B_1 \in \mathcal{C}$ be a block such that $p \in B_1$, and let $B_2 \in \mathcal{C}$ be a block such that $p' \in B_2$. So $B_1 \neq B_2$. As $|N(y)| = |N(y)^{-1}| = q-1$ and $N(y) \neq N(y^{-1})$ and $|\mathcal{C}| = q$, we have $N(y) \cup N(y^{-1}) = \mathcal{C}$. Thus, if $W = R$ then W contains a pair of points $\{y, y^{-1}\}$ and $|N(W)| = q$. Hence $|N(W)| \geq |W|$ for all $W \subseteq R$, and so an R-saturating matching exists by Hall's Marriage Theorem. This matching produces the following condition. For all $x \in R$, we have $x^{-1} \notin B^*$, where $B^* \in \mathcal{C}$ is the block adjacent to x in the matching. Furthermore, this matching gives a bijection between R and $\mathcal{C}$ with that property. As every $R_i \in \{R_1, R_2, \ldots, R_q\}$ contains a pair of elements of the form $\{x, x^{-1}\}$ for some $x \in Q$, such a matching exists in every graph bipartitioned into $R_i, \mathcal{C}_i$ in this way.

We can construct φ from these matchings as follows: if there exists an edge from an element $x \in R_i$ to a block $B \in \mathcal{C}_i$, set $\varphi(x) = B$. Hence, for any $x \in X^{\pm 1}$, there is a unique $R_i \in \{R_1, R_2, \ldots, R_q\}$ such that $x \in R_i$, and, by our construction of φ and γ, we have $x^{-1} \notin \gamma(\varphi(x))$. Thus, there exists φ such that $x^{-1} \notin \gamma(\varphi(x))$ for all $x \in X^{\pm 1}$ – that is, there exists a pair of inverse-avoiding bijections (γ, φ) where $\gamma \colon P \to X^{\pm 1}$ and $\varphi \colon X^{\pm 1} \to \mathcal{L} \backslash \mathcal{L}_\infty$. $\square$

5.2 Construction for $2n \geq q^2$

We now assume that q is the largest prime power such that $2n \geq q^2$ throughout, as we make use of this in our construction.

Lemma 5.2.1. *Let $\mathcal{A}$ be an affine plane of order q, so that $\mathcal{A}$ has q^2 points. If q^2 is even, then $q \leq \frac{q^2}{2}$. If q^2 is odd, then $q < \frac{q^2-1}{2}$.*

Proof. Suppose q is even and suppose towards a contradiction that $\frac{q^2}{2} < q$. Then $q^2 < 2q$ and so $q < 2$. But q is a prime power, and so $q \geq 2$, a contradiction. Thus, $\frac{q^2}{2} \geq q$.

Suppose q is odd. The lowest odd prime power is 3, so $q \geq 3$. If $q = 3$, then $\frac{q^2-1}{2} = 4$, so $\frac{q^2-1}{2} > q$. As $q \geq 3$ and $\frac{q^2-1}{2}$ grows faster than q, we have $\frac{q^2-1}{2} > q$ for all odd q. □

If q is even, set $Z = \{x_1, x_2, \ldots, x_{q^2/2}, x_1^{-1}, x_2^{-1}, \ldots, x_{q^2/2}^{-1}\}$, and if q is odd, set $Z = \{x_1, x_2, \ldots, x_{(q^2+1)/2}, x_1^{-1}, x_2^{-1}, \ldots, x_{(q^2-1)/2}^{-1}\}$, so that $|Z| = q^2$ and $Z \subseteq X^{\pm 1}$. Note that it is always possible to construct a set Z in this way as $X^{\pm 1}$ consists of n pairs of elements of the form (x, x^{-1}) and $n \geq \frac{q^2}{2}$.

We now give a definition and some notation before providing our construction. As before, let $\mathcal{A}$ be an affine plane of order q, let$P$ denote the set of points in $\mathcal{A}$ and denote the set of blocks by $\mathcal{L}$. We choose a class of parallel blocks and call these the *blocks of infinite gradient*, denoted by $\mathcal{L}_\infty$. Let $\mathcal{L}\backslash\mathcal{L}_\infty$ denote $\mathcal{L}$ minus the blocks of infinite gradient. Now, let $\gamma\colon P \to Z$ and $\varphi\colon Z \to \mathcal{L}\backslash\mathcal{L}_\infty$ be bijections; note that $\varphi(x)$ is a block in $\mathcal{A}$, so $\varphi(x) \subseteq P$. As each point in the block is mapped to an element of Z by γ, we have the set $\gamma(\varphi(x)) \subseteq Z$. We say that a pair of bijections (γ, φ) is *inverse-avoiding* if

$x^{-1} \notin \gamma(\varphi(x))$ for all $x \in Z$. We show below in Theorem 5.2.6 that there always exists an inverse-avoiding pair (γ, φ).

Construction 5.2.2. Let (γ, φ) be inverse-avoiding. Set $D = \bigcup_{x \in Z} x \cdot \gamma(\varphi(x))$.

We now provide a lemma we make use of in showing that our construction produces a distinct difference configuration of size at least $2\sqrt{2}n^{3/2} - O(n^{1.2625})$.

Theorem 5.2.3. [1] *For sufficiently large c, the interval $[c - c^{0.525}, c]$ contains a prime number.*

Theorem 5.2.4. *For sufficiently large n,* Construction 5.2.2 *produces a distinct difference configuration of size at least $2\sqrt{2}n^{3/2} - O(n^{1.2625})$.*

Proof. We firstly prove that our construction produces a distinct difference configuration D. As $\gamma(\varphi(x)) \subseteq Z$ for all $x \in Z$ and all elements in Z are of length 1, and $x^{-1} \notin \gamma(\varphi(x))$ as (γ, φ) is inverse-avoiding, all elements in the set $x \cdot \gamma(\varphi(x))$ are of length 2. Thus, $D \subseteq \mathcal{S}_2(e)$.

As the points contained in a pair of blocks intersect in at most one place in an affine plane, and γ is a bijection, we have $|D_x \cap D_y| \leq 1$ for all $x, y \in Z$ where $x \neq y$. By Theorem 5.0.1, D forms a distinct difference configuration.

We now show that D has size at least $2\sqrt{2}n^{3/2} - O(n^{1.2625})$. For each $x \in Z$, we have $D_x = \gamma(\varphi(x))$. As each block in $\mathcal{A}$ is of size q, we have $|\gamma(\varphi(x))| = |D_x| = q$ for all $x \in Z$. As $|Z| = q^2$ and the sets xD_x are disjoint, we have $|\bigcup_{x \in Z} D_x| = q^3$ elements.

By Theorem 5.2.3, $q \geq \sqrt{2n} - \sqrt{2n}^{0.525}$, and so $q^2 \geq 2n - O(n^{0.7625})$. Therefore,

$q^3 \geq 2\sqrt{2}n^{3/2} - O(n^{1.2625})$. Thus, D forms a distinct difference configuration of size at least $2\sqrt{2}n^{3/2} - O(n^{1.2625})$. □

Remark 5.2.5. Construction 5.2.2 produces a distinct difference configuration in which the leading term of the size of the configuration is equal to the size of the leading term in the upper bound in Theorem 5.0.3. Indeed, in the case where $2n = q^2$ the configuration produced has size $2\sqrt{2}n^{3/2}$. Construction 5.2.2 therefore produces a configuration of close to optimal size.

We now provide a theorem which shows that the bijections required by our construction always exist, so our construction can be used for any value of n.

Theorem 5.2.6. *A pair of inverse-avoiding bijections (γ, φ) with $\gamma\colon P \to Z$ and $\varphi\colon Z \to \mathcal{L}\backslash\mathcal{L}_\infty$ always exists.*

Proof. The proof is similar to that of Theorem 5.1.4, with the key difference being the use of Z in place of $X^{\pm 1}$ to account for the fact that we no longer necessarily have $|X^{\pm 1}| = 2n = q^2$. Our use of Z ensures that all bijections and partitions can be defined analagously to the use of $X^{\pm 1}$ in Theorem 5.1.4, as we are using a subset $Z \subseteq X^{\pm 1}$ such that $|Z| = q^2$.

We begin by providing an outline of the proof, which is in several stages. We first define a set Q which consists of q different pairs of elements of the form $\{x, x^{-1}\}$ and $Q \subseteq Z$. We then show that there exist q pairs of distinct points $\{p, p'\} \in P$ where no pairs have a point in common such that the points p, p' are contained in a block of infinite gradient (and therefore not contained together in any other blocks). Further, using

the fact that there exists a subset $Q \subseteq Z$ containing q different pairs of elements of the form $\{x, x^{-1}\}$, there exists a bijection $\gamma : P \to Z$ such that $\gamma(p) = x$ and $\gamma(p') = x^{-1}$ for some $x \in Z$ for each of the q pairs of distinct points $\{p, p'\}$. We then seek to show that once we have a map γ with this property, we can find a map φ such that (γ, φ) is inverse-avoiding. We do this by partitioning Z and forming a preliminary bijection $\widehat{\varphi}$ which makes use of our partition. We can then use $\widehat{\varphi}$ to formulate a bijection φ such that (γ, φ) is inverse-avoiding. The maps $\widehat{\varphi}$ and φ are essentially similar as they map the elements of Z to the same parallel classes, however φ maps the elements of Z to the blocks within the parallel classes using a matching method which we describe in the proof.

By our construction of Z and Lemma 5.2.1, Z contains at least q pairs of elements of the form $\{x, x^{-1}\}$. Define $Q = \{x_1, x_2, \ldots, x_q, x_1^{-1}, x_2^{-1}, \ldots, x_q^{-1}\}$, so that Q consists of q different pairs of distinct elements of the form $\{x, x^{-1}\}$ and $Q \subseteq Z$. As q is a prime power we have $q \geq 2$, so each block contains at least one pair of points. As the blocks in $\mathcal{L}_\infty$ are disjoint, we can choose a pair of points $\{p, p'\}$ from each of the q blocks in $\mathcal{L}_\infty$ and set $\gamma(p) = x$ and $\gamma(p') = x^{-1}$, where $x, x^{-1} \in Q$ and different pairs of points are mapped to different pairs of elements in Q. As each block in $\mathcal{L}_\infty$ intersects each block in $\mathcal{L} \backslash \mathcal{L}_\infty$ in at most one point, blocks in $\mathcal{L} \backslash \mathcal{L}_\infty$ contain at most one point in each of the q pairs of points in Q.

We now show that there exists a bijection $\varphi \colon Z \to \mathcal{L} \backslash \mathcal{L}_\infty$ such that $x^{-1} \notin \gamma(\varphi(x))$ for all $x \in Z$, where γ is as above.

As there are q pairs of elements of the form $\{x, x^{-1}\}$ in Q, we can partition Z into subsets $R_1, R_2, \ldots, R_q$ such that for all $i \in \{1, 2, \ldots, q\}$, the set R_i contains a pair of elements of the form $\{x, x^{-1}\} \in Q$ and $|R_i| = q$. Label the parallel classes in $\mathcal{A}$ not of infinite gradient (of which there are q) as $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_q$. We now define a bijection $\widehat{\varphi}$ which can be thought of as an approximation to φ, which we then use to show how to construct a map φ such that (γ, φ) is inverse-avoiding. Define $\widehat{\varphi}\colon Z \to \mathcal{L}\backslash\mathcal{L}_\infty$ by requiring $\widehat{\varphi}(R_i) = \mathcal{C}_i$, so that each element in R_i is mapped to a block in $\mathcal{C}_i$, where different elements are mapped to different blocks so that $\widehat{\varphi}$ is a bijection.

Fix $R \in \{R_1, R_2, \ldots, R_q\}$ and let $\mathcal{C}$ denote the parallel class such that $\widehat{\varphi}(R) = \mathcal{C}$, so $\mathcal{C} \in \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_q\}$. Construct a bipartite graph with bipartitions of R and $\mathcal{C}$ as follows. The vertices in $\mathcal{C}$ are the blocks in $\mathcal{C}$, and the vertices in R are the elements of R. Join $x \in R$ to a block $B \in \mathcal{C}$ if $x^{-1} \notin \gamma(B)$. Consider $x \in R$, and recall that as the blocks in $\mathcal{C}$ are disjoint they partition the q^2 points in Z. Thus, if $x^{-1} \in Z$ then there exists a unique $B' \in \mathcal{C}$ such that $x^{-1} \in \gamma(B')$. Hence, x is adjacent to all $B \in \mathcal{C}$ with $B \neq B'$. As $|\mathcal{C}| = q$, if $x^{-1} \in Z$ then $x \in R$ has degree $q - 1$. Note that by our construction of Z, if q even then if $x \in Z$ we also have $x^{-1} \in Z$. If q is odd and $x^{-1} \notin Z$, then x is adjacent to all blocks in $\mathcal{C}$ and so has degree q.

We now show that an R-saturating matching in our bipartite graph exists. By Hall's Marriage Theorem [22], such a matching exists if and only if for any subset $W \subseteq R$, we have $|N(W)| \geq |W|$, where $N(W)$ denotes the neighbourhood of W.

Trivially, $|N(\emptyset)| = |\emptyset|$. As every $x \in R$ has degree $q-1$, if W is a proper subset of R so that $|W| \leq q-1$, then we have $|N(W)| \geq |W|$. If $W = R$, then R contains a pair of elements $\{y, y^{-1}\} \in Q$ by our partition of Z. Recall that no block in $\mathcal{L}\backslash\mathcal{L}_\infty$ contains the pair of points $\{p, p'\} \in P$ such that $\gamma(p) = y$ and $\gamma(p') = y^{-1}$. So, every block in $\mathcal{C}$ is adjacent to either y or y^{-1}. Recall that every point is contained in precisely one block per parallel class. Let $B_1 \in \mathcal{C}$ be a block such that $p \in B_1$, and let $B_2 \in \mathcal{C}$ be a block such that $p' \in B_2$. So $B_1 \neq B_2$. As $|N(y)| = |N(y)^{-1}| = q-1$ and $N(y) \neq N(y^{-1})$ and $|\mathcal{C}| = q$, we have $N(y) \cup N(y^{-1}) = \mathcal{C}$. Thus, if $W = R$ then W contains a pair of points $\{y, y^{-1}\}$ and $|N(W)| = q$. Hence $|N(W)| \geq W$ for all $W \subseteq R$, and so an R-saturating matching exists by Hall's Marriage Theorem. This matching produces the following condition. For all $x \in R$, we have $x^{-1} \notin B^*$, where $B^* \in \mathcal{C}$ is the block adjacent to x in the matching. Furthermore, this matching gives a bijection between R and $\mathcal{C}$ with that property. As every $R_i \in \{R_1, R_2, \ldots, R_q\}$ contains a pair of elements of the form $\{x, x^{-1}\}$ for some $x \in Q$, such a matching exists in every graph bipartitioned into $R_i, \mathcal{C}_i$ in this way.

We can construct φ from these matchings as follows: if there exists an edge from an element $x \in R_i$ to a block $B \in \mathcal{C}_i$, set $\varphi(x) = B$. Hence, for any $x \in Z$, there is a unique $R_i \in \{R_1, R_2, \ldots, R_q\}$ such that $x \in R_i$, and, by our construction of φ and γ, we have $x^{-1} \notin \gamma(\varphi(x))$. Thus, there exists φ such that $x^{-1} \notin \gamma(\varphi(x))$ for all $x \in Z$ – that is, there exists a pair of inverse-avoiding bijections (γ, φ) where $\gamma\colon P \to Z$ and $\varphi\colon Z \to \mathcal{L}\backslash\mathcal{L}_\infty$. $\square$

Remark 5.2.7. We can add elements to Construction 5.2.2 as follows. Set $A = \{a_1, a_2, \ldots, a_{2n-q^2}\}$ where $a_i \subseteq Z$ for all $i \in \{1, 2, \ldots, 2n-q^2\}$ so that $|A| = |X^{\pm 1}\backslash Z|$. Label the elements of $X^{\pm 1}\backslash Z$ as $\{y_1, y_2, \ldots, y_{2n-q^2}\}$ and set $D_{y_i} = \{y_i, a_i\}$. As the y_i

are not involved in our construction, this ensures that the property in Theorem 5.0.1 of $|D_x \cap D_y| \leq 1$ for all $x, y \in X^{\pm 1}$ where $x \neq y$ is retained and so D is a distinct difference configuration.

This increases the size of our configuration by $2(2n - q^2) \leq 4n$. Thus, this still produces a distinct difference configuration of size at least $2\sqrt{2}n^{3/2} - O(n^{1.2625})$, however the precise size of our configuration has increased.

Remark 5.2.8. Note that if the upper bound on the gap between consecutive primes is shown to be smaller than in Lemma 5.2.3, then the lower bound on the size of a distinct difference configuration produced by Construction 5.2.2 will increase. The gap between consecutive primes produces the $O(n^{1.2625})$ term, and so if the upper bound on the gap between consecutive primes decreases then so will the size of the term we subtract from $2\sqrt{2}n^{3/2}$ in the lower bound on the size of a configuration produced by Construction 5.2.2.

Chapter 6

Arbitrary Maximum Distance in a Free Group

This chapter is concerned with the case where the maximum distance between a pair of points in a distinct difference configuration contained in the free group is an arbitrary value r. The reults in this chapter therefore hold for any (finite) distinct difference configuration contained in the free group. We begin by presenting a construction which produces a distinct difference configuration with maximum distance r which has size approximately equal to the fourth root of the number of elements in a ball of radius r. This in turn provides a lower bound on the number of elements contained in an optimal distinct difference configuration with maximum distance r contained in the free group. This construction also provides a method for constructing a network of nodes distributed in the form of a tree with a maximum distance of r between any pair of nodes with the distinct difference property. Furthermore, the number of nodes in the network will be

approximately equal to the fourth root of the number of elements contained in the ball of radius r in the free group. We show that this number is reasonable in comparison to the upper bound later in the chapter. We then extend Theorem 5.0.1 to provide a necessary and sufficient condition which a set of elements contained in a sphere of radius $r/2$ must satisfy in order to form a distinct difference configuration with maximum distance r. We use this condition to provide an upper bound on the number of elements contained in such a configuration. This upper bound in tandem with our construction shows that the maximum number of elements K contained in a distinct difference configuration which is contained in the free group is between approximately the cube root and fourth root of the number of elements contained in the ball of radius r. This shows that the number of nodes in a network which is distributed in the form of a tree corresponding to the Cayley graph of a free group with the distinct difference property and maximum distance r between any pair of nodes can contain at most K nodes and K keys. Furthermore, each node in the network can communicate with $K(K-1)$ other nodes.

We now present a construction which produces a $\overline{\mathrm{DD}}(F_n, m, r)$ with $m = 2n(2n-1)^{\lfloor \frac{r}{4} \rfloor - 1}$ for any given r and n.

Construction 6.0.1. Let W be the set of words of length $\lfloor \frac{r}{4} \rfloor$ and W^* be the set of words of length $\lceil \frac{r}{4} \rceil$. Let $\pi \colon W \to W^*$ be an injection where for all $w \in W$ the word $w \cdot \pi(w)$ is reduced (see below for a proof this exists). Set $D = \bigcup_{w \in W} w \cdot \pi(w)$.

Theorem 6.0.2. Construction 6.0.1 *produces a* $\overline{\mathrm{DD}}(F_n, m, r)$ *of size* $2n(2n-1)^{\lfloor \frac{r}{4} \rfloor - 1}$.

Proof. We firstly show that such an injection π exists for all values of r. For a word $w \in W$ where $w = w_1 w_2 \dots w_{\lfloor \frac{r}{4} \rfloor}$, if $\lfloor \frac{r}{4} \rfloor = \lceil \frac{r}{4} \rceil$ then set $\pi(w) = w_{\lfloor \frac{r}{4} \rfloor} w_{\lfloor \frac{r}{4} \rfloor - 1} \dots w_2 w_1$. Oth-

erwise, set $\pi(w) = w_{\lfloor \frac{r}{4} \rfloor} w_{\lfloor \frac{r}{4} \rfloor - 1} \dots w_2 w_1 w_1$. In both cases, as w is reduced, so is $\pi(w)$. As $\pi(w)$ is of length $\lceil \frac{r}{4} \rceil$ we have $\pi(w) \in W^*$. As $w_{\lfloor \frac{r}{4} \rfloor} \neq e$, we have $w^{-1}_{\lfloor \frac{r}{4} \rfloor} \neq w_{\lfloor \frac{r}{4} \rfloor}$. Similarly, as $w_1 \neq e$, we have $w_1^{-1} \neq w_1$. Therefore, $w \cdot \pi(w) = w_1 w_2 \dots w_{\lfloor \frac{r}{4} \rfloor} w_{\lfloor \frac{r}{4} \rfloor} w_{\lfloor \frac{r}{4} \rfloor - 1} \dots w_2 w_1$ and $w \cdot \pi(w) = w_1 w_2 \dots w_{\lfloor \frac{r}{4} \rfloor} w_{\lfloor \frac{r}{4} \rfloor} w_{\lfloor \frac{r}{4} \rfloor - 1} \dots w_2 w_1 w_1$ are reduced. Thus, we can always construct an injection π with the property that for all $w \in W$ the word $w \cdot \pi(w)$ is reduced.

As π is an injection, we have $|W| = |D|$. We therefore have $|W| = 2n(2n-1)^{\lfloor \frac{r}{4} \rfloor - 1} = |D|$.

We now show that D forms a distinct difference configuration. Suppose towards a contradiction that D does not form a distinct difference configuration. Then there exist $x, y, z, w \in D$ such that $x^{-1}y = z^{-1}w$ where it is not true that both $x = z$ and $y = w$ or that both $x = y$ and $z = w$. If there is no reduction in $x^{-1}y$, then $x^{-1}y$ and $z^{-1}w$ are the same length and equal in every position when written as a minimum length product of generating elements and their inverses. As x, y, z, w are all of length $(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)$, we have $x = z$ and $y = w$. So there must be reduction. Let $x = x_1 x_2 \cdots x_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)}$, and represent y, z, w similarly. As x, y, z, w are reduced, we must have $x_1 x_2 \cdots x_s = y_1 y_2 \cdots y_s$ and $z_1 z_2 \cdots z_s = w_1 w_2 \cdots w_s$ for some $s \geq 1$ where $x_{s+1} \neq y_{s+1}$ and $z_{s+1} \neq w_{s+1}$. As $x \neq y$, we have $s < \lfloor \frac{r}{4} \rfloor$, the length of words in W. Then we have $x^{-1}_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)} \cdots x^{-1}_{s+1} y_{s+1} \cdots y_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)} = z^{-1}_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)} \cdots z^{-1}_{s+1} w_{s+1} \cdots w_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)}$. Then $x_{s+1} \cdots x_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)} = z_{s+1} \cdots z_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)}$ and $y_{s+1} \cdots y_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)} = w_{s+1} \cdots w_{(\lfloor \frac{r}{4} \rfloor + \lceil \frac{r}{4} \rceil)}$. But as π is an injection and x, z and y, w are equal in the final $\lceil \frac{r}{4} \rceil$ positions, this implies that $x = z$ and $y = w$, a contradiction. Thus, if the differences between two pairs of elements in D are equal, then either both pairs contains a single element twice or both pairs are

equal. Hence, D forms a distinct difference configuration. $\square$

We now provide a definition and preliminary lemma we make use of when giving the if and only if condition a distinct difference configuration contained in the free group must satisfy. Let D be a $\overline{\mathrm{DD}}(F_n, m, r)$. By Theorem 4.1.1, we have $D \subseteq \mathcal{B}_{r/2}(g)$ where $g \in F_n$ if r is even and g is the mid-point of an edge if r is odd. Let $D \subseteq \mathcal{S}_{r/2}(g) = \mathcal{B}_{r/2}(g) \backslash \mathcal{B}_{r/2-1}(g)$. Define the following for every $x \in \mathcal{B}_{r/2-1}(g)$:

$$D_x = \{x' \colon xx' \in D, xx' \text{ reduced}\}.$$

Lemma 6.0.3. *Let $D \subseteq \mathcal{S}_{r/2}(g)$ where $g \in F_n$ if r is even and g is the mid-point of an edge if r is odd. If $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$ and there exists a set of elements $a, b, c, d \in D$ such that $a^{-1}b = c^{-1}d$ and a, b, c, d are of equal length, then either $a = c$ and $b = d$ or $a = b$ and $c = d$.*

Proof. Let $a = a_1 a_2 \cdots a_k, b = b_1 b_2 \cdots b_k, c = c_1 c_2 \cdots c_k, d = d_1 d_2 \cdots d_k$, and suppose that a and b are equal in the first s positions but not $s+1$, so that $a_1 a_2 \cdots a_s = b_1 b_2 \cdots b_s$. As both $a^{-1}b$ and $c^{-1}d$ are of length r prior to reduction and reduce to the same length, we have $c_1 c_2 \cdots c_s = d_1 d_2 \cdots d_s$. Note that if $s = k$ then $a = b$ and $c = d$, so $D(a, b) = D(c, d) = e$, the trivial difference. So we now consider the case where $s < k$.

We have $a_k^{-1} \cdots a_{s+1}^{-1} b_{s+1} \cdots b_k = c_k^{-1} \cdots c_{s+1}^{-1} d_{s+1} \cdots d_k$, where both sides of the equation are reduced. Then $a_{s+1} \cdots a_k = c_{s+1} \cdots c_k$ and $b_{s+1} \cdots b_k = d_{s+1} \cdots d_k$. Therefore, we have the following:

$$a = a_1 a_2 \cdots a_s a_{s+1} \cdots a_k$$

$$b = a_1 a_2 \cdots a_s b_{s+1} \cdots b_k$$

$$c = c_1 c_2 \cdots c_s a_{s+1} \cdots a_k$$

$$d = c_1 c_2 \cdots c_s b_{s+1} \cdots b_k$$

So $a_{s+1} \cdots a_k, b_{s+1} \cdots b_k \in D_{a_1 a_2 \cdots a_s}$ and $a_{s+1} \cdots a_k, b_{s+1} \cdots b_k \in D_{c_1 \cdots c_s}$. By definition of s, we have $a_{s+1} \cdots a_k \neq b_{s+1} \cdots b_k$. Then either $a_1 a_2 \cdots a_s = c_1 \cdots c_s$ or $|D_{a_1 a_2 \cdots a_s} \cap D_{c_1 \cdots c_s}| \geq 2$. If $a_1 a_2 \cdots a_s = c_1 \cdots c_s$ then $a = c$ and $b = d$, so the pairs (a, b) and (c, d) are equal. Thus, if $a^{-1}b = c^{-1}d$ and $s < k$ then $a = c$ and $b = d$. □

Theorem 6.0.4. *Let $D \subseteq \mathcal{S}_{r/2}(g)$ where $g \in F_n$ if r is even and g is the mid-point of an edge if r is odd. Then D is a distinct difference configuration if and only if $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$.*

Proof. We begin with the forward implication – that is, if D is such that $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$, then D forms a distinct difference configuration. We prove the result for even r and odd r separately.

Suppose r is even and that there exist $a, b, c, d \in D$ such that $D(a, b) = a^{-1}b = c^{-1}d = D(c, d)$. Note that a, b, c, d are all of length $r/2$.

By Lemma 6.0.3, as a, b, c, d are of equal length and $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$, either $a = b$ and $c = d$ or $a = c$ and $b = d$. If $a = b$ and $c = d$ then $D(a, b) = D(c, d) = e$, the trivial difference. If $a = c$ and $b = d$ then the pairs (a, b) and (c, d) are equal.

Thus, if r is even and D is such that $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$, then D forms a distinct difference configuration.

We now consider the case where r is odd. By Theorem 2.4.1 we can assume without loss of generality that the centre of the sphere D is the edge (e, z), so that all elements in D are of the form ei or zi, where i is of length $\lfloor \frac{r}{2} \rfloor$. So all elements in D are contained either in D_e and zD_z or in D_e only. There are therefore three possibilities for a pair of elements $a, b \in D$:

(i) If a, b are both contained in D_e but not zD_z then a, b are of length $\lfloor \frac{r}{2} \rfloor$ and $d(a, b) \leq r - 1$.

(ii) If $a, b \in zD_z$ then $a = za'$ and $b = zb'$, where a', b' are of length $\lfloor \frac{r}{2} \rfloor$. We have $d(a, b) \leq r - 1$.

(iii) Precisely one of a and b is contained in both D_e and zD_z, and the other in D_e but not zD_z. We have $d(a, b) = r$.

Differences in (iii) are of length r, so cannot be equal to differences in (i) or (ii). There are therefore four possible ways for the differences between different pairs of elements in D to be equal: two pairs of the form in (i), two from (ii), two from (iii), one from (i) and one from (ii). We consider each of these below. We use the following definition: if an element $a \in D$ is such that $a \in D_e$ and $a \notin zD_z$, then set $a = a_1 a_2 \cdots a_{\lfloor r/2 \rfloor}$, where

$a_1, a_2, \ldots, a_{\lfloor r/2 \rfloor} \in X^{\pm 1}$ and $a_1 a_2 \cdots a_{\lfloor r/2 \rfloor}$ is reduced. If $a \in D_e$ and $a \in zD_z$, then set $a = z a_1 a_2 \cdots a_{\lfloor r/2 \rfloor}$, where $z, a_1, a_2, \ldots, a_{\lfloor r/2 \rfloor} \in X^{\pm 1}$ and $z a_1 a_2 \cdots a_{\lfloor r/2 \rfloor}$ is reduced.

1 – two differences from (i) are equal: If two differences in (i) are equal, then there exist $a, b, c, d \in D$ such that $a, b, c, d \in D_e$ and $a^{-1}b = c^{-1}d$ and a, b, c, d are of length $\lfloor \frac{r}{2} \rfloor$.

By Lemma 6.0.3, as a, b, c, d are of equal length and $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(e, z)$ where $x \neq y$, either $a = b$ and $c = d$ or $a = c$ and $b = d$. If $a = b$ and $c = d$ then $D(a, b) = D(c, d) = e$, the trivial difference. If $a = c$ and $b = d$ then the pairs (a, b) and (c, d) are equal. So the differences between two different pairs of elements in (i) cannot be equal unless it is the trivial difference.

2 – two differences from (ii) are equal: If two differences in (ii) are equal, then there exist $a, b, c, d \in D$ such that $a = za', b = zb', c = zc', d = zd'$ and $a^{-1}b = c^{-1}d$, where a, b, c, d are of length $\lfloor \frac{r}{2} \rfloor + 1$.

By Lemma 6.0.3, as a, b, c, d are of equal length and $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(e, z)$ where $x \neq y$, either $a = b$ and $c = d$ or $a = c$ and $b = d$. If $a = b$ and $c = d$ then $D(a, b) = D(c, d) = e$, the trivial difference. If $a = c$ and $b = d$ then the pairs (a, b) and (c, d) are equal. So the differences between two different pairs of elements in (ii) cannot be equal unless it is the trivial difference.

3 – two differences from (iii) are equal: If two differences in (iii) are equal, then there exist $a, b, c, d \in D$ such that precisely one element from each of the pairs a, b and c, d are contained in zD_z and $a^{-1}b = c^{-1}d$. There are four possible such pairs of differences. We consider each of these in turn. Suppose $a, c \in zD_z$, so that $b, d \in D_e$ and $b, d \notin zD_z$. Then $a^{-1}b = a_{\lfloor r/2 \rfloor}^{-1} \cdots a_2^{-1}a_1^{-1}z^{-1}b_1b_2 \cdots b_{\lfloor r/2 \rfloor} = c_{\lfloor r/2 \rfloor}^{-1} \cdots c_2^{-1}c_1^{-1}z^{-1}d_1d_2 \cdots d_{\lfloor r/2 \rfloor} = c^{-1}d$. As $b_1, d_1 \neq z$ and a, b, c, d are reduced, both sides of the equation are reduced. As they are of equal length, they are equal in every position. Therefore, we have $a = c$ and $b = d$, so the pairs (a, b) and (c, d) are equal. A similar argument shows that if $b, d \in zD_z$ and $a, c \in D_e$ and $a, c \notin zD_z$ then $a = c$ and $b = d$, so the pairs (a, b) and (c, d) are equal. If $a, d \in zD_z$ and $b, c \notin zD_z$, then $a^{-1}b = a_{\lfloor r/2 \rfloor}^{-1} \cdots a_2^{-1}a_1^{-1}z^{-1}b_1b_2 \cdots b_{\lfloor r/2 \rfloor} = c_{\lfloor r/2 \rfloor}^{-1} \cdots c_2^{-1}c_1^{-1}zd_1d_2 \cdots d_{\lfloor r/2 \rfloor} = c^{-1}d$. But as both sides of the equation are reduced we have $z = z^{-1}$, which is impossible as $z \neq e$. Thus, no such differences can be equal. A similar argument shows that a pair of differences where $b, c \in zD_z$ and $a, d \notin zD_z$ cannot be equal.

4 – one difference from (i) and one difference from (ii) are equal: If a difference from (i) and a difference from (ii) are equal, then without loss of generality there exist $a, b, c, d \in D$ such that $a, b \in D_e$ and $a, b \notin zD_z$ and $c, d \in zD_z$ and $a^{-1}b = c^{-1}d$. Then $a^{-1}b = a_{\lfloor r/2 \rfloor}^{-1} \cdots a_2^{-1}a_1^{-1}b_1b_2 \cdots b_{\lfloor r/2 \rfloor}$ and $c^{-1}d = c_{\lfloor r/2 \rfloor}^{-1} \cdots c_2^{-1}c_1^{-1}z^{-1}zd_1d_2 \cdots d_{\lfloor r/2 \rfloor} = c_{\lfloor r/2 \rfloor}^{-1} \cdots c_2^{-1}c_1^{-1}d_1d_2 \cdots d_{\lfloor r/2 \rfloor}$. So we have
$a_{\lfloor r/2 \rfloor}^{-1} \cdots a_2^{-1}a_1^{-1}b_1b_2 \cdots b_{\lfloor r/2 \rfloor} = c_{\lfloor r/2 \rfloor}^{-1} \cdots c_2^{-1}c_1^{-1}d_1d_2 \cdots d_{\lfloor r/2 \rfloor}$.

A similar argument to that in Lemma 6.0.3 shows that either $a = b$ and $c = d$ so

that $D(a,b) = D(c,d) = e$, or we have $a_{s+1}\cdots a_{\lfloor r/2\rfloor}, b_{s+1}\cdots b_{\lfloor r/2\rfloor} \in D_{a_1a_2\cdots a_s}$ and $a_{s+1}\cdots a_{\lfloor r/2\rfloor}, b_{s+1}\cdots b_{\lfloor r/2\rfloor} \in D_{zc_1c_2\cdots c_s}$. As $a_1a_2\cdots a_s$ and $zc_1c_2\cdots c_s$ are reduced words of different lengths, they cannot be equal. Moreover, $a_{s+1}\cdots a_{\lfloor r/2\rfloor} \neq b_{s+1}\cdots b_{\lfloor r/2\rfloor}$ by definition of s. So $|D_{a_1a_2\cdots a_s} \cap D_{zc_1c_2\cdots c_s}| \geq 2$, a contradiction.

Thus, if r is odd and D is such that $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(e,z)$ where $x \neq y$, then D forms a distinct difference configuration.

Hence, if D is such that $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$, then D forms a distinct difference configuration.

We now prove the reverse implication – that is, if $|D_x \cap D_y| \geq 2$ for some $x, y \in \mathcal{B}_{r/2-1}(g)$ where $x \neq y$, then D does not form a distinct difference configuration. If $|D_x \cap D_y| \geq 2$ then there exist $z, w \in D_x$ and $z, w \in D_y$ where $z \neq w$ such that $xz, xw, yz, yw \in D$ and xz, xw, yz, yw are reduced. We have $D(xz, xw) = z^{-1}x^{-1}xw = z^{-1}w$ and $D(yz, yw) = z^{-1}y^{-1}yw = z^{-1}w$. But then $D(xz, xw) = D(yz, yw)$ and so D does not form a distinct difference configuration. Thus, D must be such that $|D_x \cap D_y| \leq 1$. □

We now use Theorem 6.0.4 to provide an upper bound on the number of elements m contained in a $\overline{\mathrm{DD}}(F_n, m, r)$.

Theorem 6.0.5. *Let D be a $\overline{\mathrm{DD}}(F_n, m, r)$. If r is even and $r+i = 6a$ for some $a \in \mathbb{Z}$ and some $i \in \{0,1,2,3,4,5\}$, then $m \leq n^2 r(2n-1)^{\frac{r+i}{3}-2} + nr(2n-1)^{\frac{2r-i}{6}-1} - \frac{nr}{2}(2n-1)^{\frac{r+i}{6}-1}$. If r is odd and $r+1+j = 6b$ for some $b \in \mathbb{Z}$ and some $j \in \{0,1,2,3,4\}$, then $m \leq n^2(r+1)(2n-1)^{\frac{r+1+j}{3}-2} + n(r+1)(2n-1)^{\frac{2(r+1)-j}{6}-1} - \frac{n(r+1)}{2}(2n-1)^{\frac{r+1+j}{6}-1}$.*

Proof. We first consider the case where r is even. By Theorem 4.1.1, D is contained in a ball of radius $r/2$. By Theorem 2.4.1, we can assume without loss of generality that the centre of the ball is e. Consider the elements of D contained in $\mathcal{S}_{r/2}(e)$, and label the set of these elements by D^*. By the definition of D_x, we have $D^* = \bigcup_{x \in \mathcal{B}_{r/2-1}(e)} x \cdot D_x$ where elements in D_x are of length $r/2 - \text{len}(x)$.

Consider the case where r is a multiple of 6 and x is a word of length $r/6$, so that any words contained in D_x are of length $r/2 - r/6 = r/3$. There are $2n(2n-1)^{r/6-1}$ (possibly empty) sets D_x, and $2n(2n-1)^{r/3-1}$ words of length $r/3$. Observe that if each of these words is contained in exactly one set D_x, then $|D_x \cap D_y| = 0$ for all x, y of length $r/6$ where $x \neq y$. This gives $2n(2n-1)^{r/3-1}$ elements.

By Theorem 6.0.4, D must satisfy $|D_x \cap D_y| \leq 1$ for all $x, y \in \mathcal{B}_{r/2-1}(e)$ where $x \neq y$. If any word of length $r/3$ is contained in more than one of these sets, then there exists x, y such that $|D_x \cap D_y| \geq 1$. Thus, in addition to the $2n(2n-1)^{r/3-1}$ elements from above, D can contain at most one additional element for every pair of sets D_x, D_y where x, y are of length $r/6$. The number of such pairs is $\binom{2n(2n-1)^{r/6-1}}{2} = 2n^2(2n-1)^{r/3-2} - n(2n-1)^{r/6-1}$ elements. The subset D^* can therefore contain at most $2n(2n-1)^{r/3-1} + 2n^2(2n-1)^{r/3-2} - n(2n-1)^{r/6-1}$ elements.

We have $\mathcal{B}_{r/2}(e) = \mathcal{S}_{r/2}(e) \cup \mathcal{S}_{r/2-1}(e) \cup \ldots \cup \mathcal{S}_0(e)$. Clearly, the bound on the number of elements in D contained in each of these spheres is not greater than the bound on $\mathcal{S}_{r/2}(e)$, and so the upper bound on the number of elements contained in each sphere

is at most $2n(2n-1)^{r/3-1} + 2n^2(2n-1)^{r/3-2} - n(2n-1)^{r/6-1}$. As there are $r/2$ such spheres, the bound on the size m of a distinct difference configuration contained in $\mathcal{B}_{r/2}(e)$ is $\frac{r}{2}(2n(2n-1)^{r/3-1} + 2n^2(2n-1)^{r/3-2} - n(2n-1)^{r/6-1}) = nr(2n-1)^{r/3-1} + n^2r(2n-1)^{r/3-2} - \frac{nr}{2}(2n-1)^{r/6-1}$.

If r is not divisible by 6, then $r+i$ is divisible by 6 for some $i \in \{1,2,3,4,5\}$. A similar argument which considers the case where x is of length $\frac{r+i}{6}$ provides the bound $m \leq n^2r(2n-1)^{\frac{r+i}{3}-2} + nr(2n-1)^{\frac{2r-i}{6}-1} - \frac{nr}{2}(2n-1)^{\frac{r+i}{6}-1}$. Thus, if $r+i$ is divisible by 6 for some $i \in \{0,1,2,3,4,5\}$ then $m \leq n^2r(2n-1)^{\frac{r+i}{3}-2} + nr(2n-1)^{\frac{2r-i}{6}-1} - \frac{nr}{2}(2n-1)^{\frac{r+i}{6}-1}$.

We now consider the case where r is odd. Clearly, the upper bound on the number of elememts m contained in a $\overline{\mathrm{DD}}(F_n, m, r)$ is at most the upper bound on the number of elements m' contained in a $\overline{\mathrm{DD}}(F_n, m', r+1)$. Thus, we can apply the bound on the number of elements in a distinct difference configuration contained in F_n with maximum distance $r+1$ (as $r+1$ is even) to obtain an upper bound on m. Observe that as r is odd, we have $r+1+j = 6b$ for some $b \in \mathbb{Z}$ and $j \in \{0,1,2,3,4\}$. Using the upper bound found above, this gives an upper bound of $m \leq n^2(r+1)(2n-1)^{\frac{r+1+j}{3}-2} + n(r+1)(2n-1)^{\frac{2(r+1)-j}{6}-1} - \frac{n(r+1)}{2}(2n-1)^{\frac{r+1+j}{6}-1}$. This gives the result. □

Remark 6.0.6. We now explain the reasoning for our consideration of words of length $r/6$ in our proof of Theorem 6.0.5. Observe that for some $k \leq r/2$, the number of words of length $r/2-k$ is $2n(2n-1)^{r/2-k-1}$, which has a leading term of order $r/2-k$. Furthermore, the number of pairs of words of length k is $\frac{(2n(2n-1)^{k-1})(2n(2n-1)^{k-1})}{2}$, which has a leading term of order $2k$. In order to minimise the upper bound in Theorem 6.0.5, we make these

terms as close as possible. If $k = r/6$, then $2k = r/2 - k$. Clearly, $r + i$ where $i \leq 5$ is close to $r/6$ for sufficiently large r, and so these terms are close in size (if not equal).

Corollary 6.0.7. *Let D be a $\overline{\mathrm{DD}}(F_n, m, r)$. If r is even then $m \leq n^2 r(2n-1)^{\frac{r+5}{3}-2} + O(rn^{r/3})$ for sufficiently large r. If r is odd then $m \leq n^2(r+1)(2n-1)^{\frac{r+5}{3}-2} + O(n^{\frac{r+1}{3}})$.*

Proof. We first consider the case where r is even. By Theorem 6.0.5, we have $m \leq n^2 r(2n-1)^{\frac{r+i}{3}-2} + nr(2n-1)^{\frac{2r-i}{6}-1} - \frac{nr}{2}(2n-1)^{\frac{r+i}{6}-1}$ where $i \in \{0,1,2,3,4,5\}$. We have $n^2 r(2n-1)^{\frac{r+i}{3}-2} \leq n^2 r(2n-1)^{\frac{r+5}{3}-2}$ for all $i \in \{0,1,2,3,4,5\}$ and $nr(2n-1)^{\frac{2r-i}{6}-1} \leq nr(2n-1)^{\frac{2r}{6}-1} = O(rn^{r/3})$ for all $i \in \{0,1,2,3,4,5\}$. Furthermore, $\frac{nr}{2}(2n-1)^{\frac{r+i}{6}-1} \leq nr(2n-1)^{\frac{2r-i}{6}-1}$ where $i \in \{0,1,2,3,4,5\}$ for sufficiently large r. We therefore have $m \leq n^2 r(2n-1)^{\frac{r+i}{3}-2} + nr(2n-1)^{\frac{2r-i}{6}-1} - \frac{nr}{2}(2n-1)^{\frac{r+i}{6}-1} \leq n^2 r(2n-1)^{\frac{r+5}{3}-2} + O(rn^{r/3})$ where $i \in \{0,1,2,3,4,5\}$.

We now consider the case where r is odd. By Theorem 6.0.5, we have $m \leq n^2(r+1)(2n-1)^{\frac{r+1+j}{3}-2} + n(r+1)(2n-1)^{\frac{2(r+1)-j}{6}-1} - \frac{n(r+1)}{2}(2n-1)^{\frac{r+1+j}{6}-1}$ for some $j \in \{0,1,2,3,4\}$. We have $n^2(r+1)(2n-1)^{\frac{r+1+j}{3}-2} \leq n^2(r+1)(2n-1)^{\frac{r+5}{3}-2}$ for all $j \in \{0,1,2,3,4\}$ and $n(r+1)(2n-1)^{\frac{2(r+1)-j}{6}-1} \leq n(r+1)(2n-1)^{\frac{r+1}{3}-1} = O(n^{\frac{r+1}{3}})$ for all $j \in \{0,1,2,3,4\}$. Furthermore, $\frac{n(r+1)}{2}(2n-1)^{\frac{r+1+j}{6}-1} \leq n(r+1)(2n-1)^{\frac{2(r+1)-j}{6}-1}$ for sufficiently large r. We therefore have $m \leq n^2(r+1)(2n-1)^{\frac{r+1+j}{3}-2} + n(r+1)(2n-1)^{\frac{2(r+1)-j}{6}-1} - \frac{n(r+1)}{2}(2n-1)^{\frac{r+1+j}{6}-1} \leq n^2(r+1)(2n-1)^{\frac{r+5}{3}-2} + O(n^{\frac{r+1}{3}})$ for sufficiently large r. □

Corollary 6.0.8. *Let K be the upper bound on the number of elements m contained in a $\overline{\mathrm{DD}}(F_n, m, r)$ for given n and r where $r > 0$. If r is even then $2n(2n-1)^{\lfloor \frac{r}{4} \rfloor - 1} \leq K \leq$*

$n^2r(2n-1)^{\frac{r+5}{3}-2}+O(n^{r/3})$ *for sufficiently large* r*. If* r *is odd then* $2n(2n-1)^{\lfloor\frac{r}{4}\rfloor-1} \leq K \leq n^2(r+1)(2n-1)^{\frac{r+5}{3}-2}+O(n^{\frac{r+1}{3}})$ *for sufficiently large* r*.*

Proof. We first consider the case where r is even. By Corollary 6.0.7, we have $K \leq n^2r(2n-1)^{\frac{r+5}{3}-2}+O(n^{r/3})$ for all n and r with r sufficiently large. By Theorem 6.0.2, there exists a $\overline{\mathrm{DD}}(F_n, m, r)$ of size $2n(2n-1)^{\lfloor\frac{r}{4}\rfloor-1}$ for all values of r and n. So $K \geq 2n(2n-1)^{\lfloor\frac{r}{4}\rfloor-1}$. Thus, $2n(2n-1)^{\lfloor\frac{r}{4}\rfloor-1} \leq K \leq n^2r(2n-1)^{\frac{r+5}{3}-2}+O(n^{r/3})$.

A similar argument for odd r gives $2n(2n-1)^{\lfloor\frac{r}{4}\rfloor-1} \leq K \leq n^2(r+1)(2n-1)^{\frac{r+5}{3}-2}+O(n^{\frac{r+1}{3}})$. □

Chapter 7

Arbitrary Groups

In this chapter we consider distinct difference configurations contained in any group, rather than restricting ourselves to the free group. We first provide an upper bound on the number of elements contained in a distinct difference configuration with maximum distance r. We then give a lower bound on the number of elements m contained in a distinct difference configuration contained in a group G where G contains no elements of order 2 and m is maximal. We subsequently show that if for some group the number of elements contained in the ball of radius r with centre e grows exponentially as r grows, then the number of elements m in a distinct difference configuration where m is maximal grows exponentially also. Finally, we show how, given a distinct difference configuration contained in a group H where H is a quotient group of G, we can construct a distinct difference configuration in G where the maximum distance is at most double that of the configuration in H. We begin with our upper bound on the number of elements contained in a distinct difference configuration with maximum distance r.

Theorem 7.0.1. *Let G be a group and S a generating set of G. If D is a $\overline{\mathrm{DD}}(G, S, m, r)$ then $m(m-1) \leq |\mathcal{B}_r(e)|$.*

Proof. The differences formed by pairs of distinct elements of D are of length at most r, and so each difference is an element in G which is contained in $\mathcal{B}_r(e)$. As the differences are pairwise unique, there are at most $|\mathcal{B}_r(e)|$ differences formed by pairs of distinct elements of D. As D contains m distinct elements, there are $m(m-1)$ differences formed by pairs of distinct elements in D. We therefore have $m(m-1) \leq |\mathcal{B}_r(e)|$. □

The following result shows that a distinct difference configuration of size m with maximum distance r must exist in a group G if the given conditions are satisfied.

Theorem 7.0.2. *Let G be a group and S a generating set of G where S is closed under inverses. Define $p_{r/2}$ to be the probability that an element in $\mathcal{B}_{r/2}(e)$ has order 2. There exists a distinct difference configuration $D \subseteq \mathcal{B}_{r/2}(e)$ with maximum distance r and size m if the inequality $\frac{m^4}{|\mathcal{B}_{r/2}(e)|} + m^2 p_{r/2} < 1$ is satisfied.*

Proof. Fix $r > 0$ and $m > 0$ where $r, m \in \mathbb{N}$. Construct a set $D \subseteq \mathcal{B}_{r/2}(e)$ as follows. Choose m elements $x_1, x_2, \ldots, x_m$ uniformly and independently from $\mathcal{B}_{r/2}(e)$. The possible outcomes of this are the m-tuples of $\mathcal{B}_{r/2}(e)$, where the probability of each m-tuple being chosen is $\frac{1}{|\mathcal{B}_{r/2}(e)|^m}$. Let $i, j, k, l \in \{1, 2, \ldots, m\}$, and let $E_{i,j,k,l}$ be the event that $x_i^{-1} x_j = x_k^{-1} x_l$. This is a bad event unless $i = k$ and $j = l$ or $i = j$ and $k = l$, as the set $\{x_1, x_2, \ldots, x_m\}$ does not form a distinct difference configuration if this event occurs. Note that $i = j$ and $k \neq l$ is the event that we have picked x_k and x_l to be equal, as it implies $x_k^{-1} x_l = x_i^{-1} x_j = e$, so $x_l = x_k$. There are at most m^4 bad events, as there are fewer than m^4 choices for i, j, k, l in each m-tuple.

Observe that if i, j, k, l are all distinct, then $P(E_{i,j,k,l}) = P(x_l = x_k x_i^{-1} x_j) = \frac{1}{|\mathcal{B}_{r/2}(e)|}$. We now consider the cases where $l = i$ or $l = j$ or $l = k$.

$l = k$: We have $P(E_{i,j,k,l}) = P(x_l = x_l x_i^{-1} x_j) = P(x_i = x_j) = \frac{1}{|\mathcal{B}_{r/2}(e)|}$.

$l = j$: We have $P(E_{i,j,k,l}) = P(x_l = x_k x_i^{-1} x_l) = P(x_i = x_k) = \frac{1}{|\mathcal{B}_{r/2}(e)|}$.

$l = i$: We have $P(E_{i,j,k,l}) = P(x_l = x_k x_l^{-1} x_j) = P(x_j = x_l x_k^{-1} x_l) = \frac{1}{|\mathcal{B}_{r/2}(e)|}$ unless $j = l$ or $j = k$. If $j = l$ then $P(E_{i,j,k,l}) = P(x_l = x_l x_k^{-1} x_l) = P(x_k = x_l) = \frac{1}{|\mathcal{B}_{r/2}(e)|}$ unless $k = l$. If $k = l$ then $i = j = k = l$, which is not a bad event. If $l = i$ and $j = k$ then $P(E_{i,j,k,l}) = P(x_l^{-1} x_k = x_k^{-1} x_l) = P((x_k^{-1} x_l)^2 = 1) = p_{r/2}$.

As there are fewer than m^4 quadruples $\{i, j, k, l\}$ and fewer than m^2 pairs of elements in an m-tuple, if the inequality $\frac{m^4}{|\mathcal{B}_{r/2}(e)|} + m^2 p_{r/2} < 1$ is satisfied then there exists a distinct difference configuration of size m contained in $\mathcal{B}_{r/2}(e)$. As the maximum distance between a pair of elements in $\mathcal{B}_{r/2}(e)$ is at most r, the maximum distance in the distinct difference configuration is at most r. □

Corollary 7.0.3. *Let G be a group containing no elements of order 2, and S a generating set of G. Then there exists a $\overline{\mathrm{DD}}(G, S, m, r)$ such that $m = \lceil |\mathcal{B}_{r/2}(e)|^{1/4} \rceil - 1$.*

Proof. By Theorem 7.0.2, there exists a $\overline{\mathrm{DD}}(G, S, m, r)$ if m satisfies $\frac{m^4}{|\mathcal{B}_{r/2}(e)|} + m^2 p_{r/2} < 1$. As G contains no elements of order 2, we have $p_{r/2} = 0$. Thus, m must satisfy $m^4 < |\mathcal{B}_{r/2}(e)|^{1/4}$. Setting $m = \lceil |\mathcal{B}_{r/2}(e)|^{1/4} \rceil - 1$ satisfies this requirement. Furthermore, the

maximum distance between a pair of elements in $\mathcal{B}_{r/2}(e)$ is at most r, and so the maximum distance in the distinct difference configuration is at most r. Thus, a $\overline{\mathrm{DD}}(G, S, m, r)$ with $m = \lceil |\mathcal{B}_{r/2}(e)|^{1/4} \rceil - 1$ exists. □

The following corollary shows that if for a group G the number of elements in $\mathcal{B}_k(e)$ grows exponentially as k increases, then the number of elements contained in a distinct difference configuration of maximal size contained in $\mathcal{B}_k(e)$ also grows exponentially.

Corollary 7.0.4. *Let G be a group that contains no elements of order 2, and S a generating set of G. If $|\mathcal{B}_{r/2}(e)| \geq a^{r/2}$ for some $a > 1$, then a distinct difference configuration D of maximal size contained in $\mathcal{B}_{r/2}(e)$ is such that $|D| \geq \lfloor b^{r/2} \rfloor$ for some $b > 1$. Indeed, we may take $b = a^{1/4-\varepsilon}$ for some $0 < \varepsilon < \frac{1}{4}$.*

Proof. Let $|D| = m$. By Theorem 7.0.2, there exists a distinct difference configuration of size m contained in $\mathcal{B}_{r/2}(e)$ if m satisfies $\frac{m^4}{|\mathcal{B}_{r/2}(e)|} + m^2 p_{r/2} < 1$. As G contains no elements of order 2, we have $p_{r/2} = 0$. Thus, $\frac{m^4}{|\mathcal{B}_{r/2}(e)|} < 1$, and so $m^4 < |\mathcal{B}_{r/2}(e)|$. We have $|\mathcal{B}_{r/2}(e)| \geq a^{r/2}$. So a distinct difference configuration of size m exists if m satisfies $m < (a^{1/4})^{r/2}$. Set $b = a^{1/4-\varepsilon}$ where $0 < \varepsilon < \frac{1}{4}$. As $a > 1$, we have $b > 1$. Furthermore, $(a^{1/4})^{r/2} > b^{r/2}$. Set $m = \lfloor b^{r/2} \rfloor$ and the result follows. □

Corollary 7.0.5. *Let G be a group containing no elements of order 2, and S a generating set of G. Then a $\overline{\mathrm{DD}}(G, S, m, r)$ where m is of maximal size is such that $\lceil |\mathcal{B}_r(e)|^{1/4} \rceil - 1 \leq m \leq \sqrt{|\mathcal{B}_{r/2}(e)|} + 1$, where $0 < \varepsilon < \frac{1}{4}$.*

Proof. By Corollary 7.0.3, there exists a $\overline{\mathrm{DD}}(G, S, m, r)$ such that $m \geq \lceil |\mathcal{B}_{r/2}(e)|^{1/4} \rceil - 1$. By Theorem 7.0.1, we have $m(m-1) \leq |\mathcal{B}_r(e)|$. Therefore, $(m-1)^2 \leq |\mathcal{B}_r(e)|$ and so it follows that $m - 1 \leq \sqrt{|\mathcal{B}_r(e)|}$ and thus $m \leq \sqrt{|\mathcal{B}_r(e)|} + 1$. □

7.1 Quotient Group Construction

We now show that if a group H is a quotient group of a group G, then given a distinct difference configuration contained in H, we can construct a distinct difference configuration in G. We first provide some definitions.

Let G be a group, S a generating set of G, and H a quotient group of G. Let $\phi : G \to H$ be a surjective homomorphism. Given a subset $D \subseteq H$, we can construct a set $\widehat{D}$ in bijection with D as follows. Choose an element $d \in D$ and represent d as a product of generators. So $d = d_1 d_2 \dots d_k$ where for all $i \in \{1, 2, \dots, k\}$ we have $d_i \in S$. For every element $d^* \in D$, write d^* as $d \cdot w$, where w is of minimal length. Set $\widehat{d^*} = \phi^{-1}(d_1^*)\phi^{-1}(d_2^*) \dots \phi^{-1}(d_l^*)$. Then, set $\widehat{D} = \bigcup_{d^* \in D} \widehat{d^*}$.

Theorem 7.1.1. *Let D be a $\overline{\mathrm{DD}}(H, S, m, r)$. Then $\widehat{D}$ is a $\overline{\mathrm{DD}}(G, S, m, 2r)$.*

Proof. We firstly prove that $\widehat{D}$ forms a distinct difference configuration.

Suppose towards a contradiction that $\widehat{D}$ is not a distinct difference configuration. Then there exist $\widehat{d_1}, \widehat{d_2}, \widehat{d_3}, \widehat{d_4} \in \widehat{D}$ such that $\widehat{d_1}^{-1}\widehat{d_2} = \widehat{d_3}^{-1}\widehat{d_4}$ and it is not true that both $\widehat{d_1} = \widehat{d_3}$ and $\widehat{d_2} = \widehat{d_4}$. Furthermore, $\widehat{d_1} \neq \widehat{d_2}$ and $\widehat{d_3} \neq \widehat{d_4}$.

As ϕ is a homomorphism and $\phi(\widehat{d_i}) = d_i$, then $\phi(\widehat{d_1}^{-1}\widehat{d_2}) = \phi(\widehat{d_3}^{-1}\widehat{d_4})$ implies that $\phi(\widehat{d_1}^{-1})\phi(\widehat{d_2}) = \phi(\widehat{d_3}^{-1})\phi(\widehat{d_4})$.

As $\phi(\widehat{d_j})^{\pm 1} = d_j^{\pm 1}$ for all $j \in \{1, 2, \dots, m\}$, we have $d_1^{-1}d_2 = d_3^{-1}d_4$. As $d_1, d_2, d_3, d_4 \in D$,

it follows that D is not a distinct difference configuration, a contradiction. Thus, we must have $\widehat{d_1} = \widehat{d_3}$ and $\widehat{d_2} = \widehat{d_4}$ or $\widehat{d_1} = \widehat{d_2}$ and $\widehat{d_3} = \widehat{d_4}$ (or both), and so $\widehat{D}$ is a distinct difference configuration.

We now prove that the maximum distance between any pair of elements in $\widehat{D}$ is at most $2r$.

Let $\widehat{d_5}, \widehat{d_6} \in \widehat{D}$. By the construction of $\widehat{D}$, we have $\widehat{d_5} = \phi^{-1}(d)\phi^{-1}(x)$ and $\widehat{d_6} = \phi^{-1}(d)\phi^{-1}(y)$ for some $d \in D$ and $x, y \in H$. As the maximum distance in D is r, the lengths of x and y are at most r. Then we have:

$$D(\widehat{d_5}, \widehat{d_6}) = (\phi^{-1}(d)\phi^{-1}(x))^{-1}\phi^{-1}(d)\phi^{-1}(y) = \phi^{-1}(x^{-1})\widehat{d}^{-1}\widehat{d}\phi^{-1}(y) = \phi^{-1}(x^{-1})\phi^{-1}(y).$$

As x, y are of length at most r, we have $\phi^{-1}(x^{-1})\phi^{-1}(y)$ is of length at most $r + r = 2r$. Thus, the maximum distance between a pair of elements in $\widehat{D}$ is at most $2r$.

Thus, $\widehat{D}$ forms a $\overline{\mathrm{DD}}(G, S, m, 2r)$. □

Corollary 7.1.2. *Let G be a group and H a quotient group of G. Let K be the upper bound on the size of a distinct difference configuration with maximum distance $2r$ contained in G. Then K is an upper bound on the size of a distinct difference configuration with maximum distance r contained in H.*

Proof. By Theorem 7.1.1, if a subset $D \subseteq H$ is a distinct difference configuration with maximum distance r, then $\widehat{D}$ is a distinct difference configuration with maximum distance $2r$. Recall that $|D| = |\widehat{D}|$. Therefore, given a distinct difference in H with max-

imum distance r, there exists a distinct difference configuration of equal size in G with maximum distance $2r$. Thus, if K is an upper bound on the size of a distinct difference configuration with maximum distance $2r$ contained in G, then K is an upper bound on the size of a distinct difference configuration with maximum distance r contained in any quotient group H of G. □

Corollary 7.1.2 has the following implication. Suppose a set of nodes in a network are distributed in the form of a subgraph of the Cayley graph of a group H where H is a quotient group of a group G, and the maximum communication range of each node is r. Then the upper bound on the number of elements in a distinct difference configuration with maximum distance $2r$ contained in G is also an upper bound on the number of nodes in a distinct difference configuration within the network.

We now describe the applications of Theorem 7.1.1 to the free group. We begin with a preliminary lemma.

Lemma 7.1.3. [31] *Let G be a finitely generated group, and S a finite generating set of G. Then G is isomorphic to a quotient group of a free group of rank $|S|$.*

We now define some notation. Let G be a finitely generated group, let S be a finite generating set of G, and let $F(S)$ be the free group with generating set S. By Lemma 7.1.3, there exists a surjective homomorphism $\phi\colon F(S) \to G$.

Given a subset $D \subseteq G$, we can construct a set $\widehat{D} \subseteq F(S)$ in bijection with D as follows. Choose an element $d \in D$ and represent d as a product of generators. So $d = d_1 d_2 \dots d_k$

where for all $i \in \{1, 2, \ldots, k\}$ we have $d_i \in S$. For every element $d^* \in D$, write d^* as $d \cdot w$, where w is of minimal length. Set $\widehat{d^*} = \phi^{-1}(d_1^*)\phi^{-1}(d_2^*)\ldots\phi^{-1}(d_l^*)$. Then, set $\widehat{D} = \bigcup_{d^* \in D} \widehat{d^*}$.

Corollary 7.1.4. *Let D be a $\overline{\mathrm{DD}}(G, S, m, r)$. Then $\widehat{D}$ is a $\overline{\mathrm{DD}}(F(S), S, m, 2r)$.*

Proof. The proof is similar to that of Theorem 7.1.1. □

Chapter 8

DDCs in $\mathbb{Z}^n$

In this chapter we consider distinct difference configurations contained in the group $\mathbb{Z}^n$ with generating set $\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)\}$. We begin by presenting our example which shows that there exists a $\overline{\mathrm{DD}}(\mathbb{Z}^3,m,r)$ which is not contained in a ball of radius $r/2$. Indeed, it is not contained in a ball with radius less than $\frac{3r}{4}$. In particular, this shows that a result found in [3] which states that a $\overline{\mathrm{DD}}(\mathbb{Z}^2,m,r)$ is contained in a (possibly bi-centred or quad-centred) ball of radius $r/2$ does not generalise to $\mathbb{Z}^n$. Furthermore, Theorem 4.1.1, which shows that a $\overline{\mathrm{DD}}(F_n,m,r)$ is contained in a ball of radius $r/2$, does not necessarily extend to other groups. We then show how to generalise this example to larger values of n. We then provide upper and lower bounds on the number of elements m contained in a $\overline{\mathrm{DD}}(\mathbb{Z}^n,m,r)$ where m is maximal, in addition to a construction for $\mathbb{Z}$ which we extend to $\mathbb{Z}^2$ and subsequently to $\mathbb{Z}^n$ for all values of n. We observe that our construction produces a configuration containing an optimal number of elements m, up to multiplication by a constant. This ensures maximum connectivity between the

nodes in a wireless sensor network as each node can communicate with $m(m-1)$ other nodes. Our upper and lower bounds and construction apply to $\mathbb{Z}^n$ for all (sufficiently large) values of n, rather than only $\mathbb{Z}^2$ as in [3]. Finally, we consider the applications of our results and construction to the dihedral group. Recall that Theorem 7.0.2 gave a lower bound on the number of elements contained in a distinct difference configuration of maximal size which depended on the probability that an element had order 2. We show that despite the high proportion of elements of order 2 contained in the dihedral group, it is possible to use our construction in $\mathbb{Z}$ to obtain a 'large' distinct difference configuration of optimal size up to multiplication by a constant. Such groups may therefore still be relevant for applications in key predistribution in wireless sensor networks.

8.1 DDCs Not Contained in Balls of Radius $r/2$

We now provide our example of a $\overline{\mathrm{DD}}(\mathbb{Z}^3, m, r)$ which is not contained in a ball of radius $r/2$ about an element of $\mathbb{Z}^3$.

Example 8.1.1. Let $D = \{(0,0,0), (\frac{r}{2}, \frac{r}{2}, 0), (\frac{r}{2}, 0, \frac{r}{2}), (0, \frac{r}{2}, \frac{r}{2})\} \subseteq \mathbb{Z}^3$ where r is a positive even integer, and label these elements as a, b, c, d respectively. Each element in D is at distance r from every other element in D, so the maximum distance is r. We now show that D forms a $\overline{\mathrm{DD}}(\mathbb{Z}^3, 4, r)$. Consider the direction vectors between each pair of elements. These are as in Figure 8.1.1:

As these direction vectors are all pairwise distinct, D forms a $\overline{\mathrm{DD}}(\mathbb{Z}^3, 4, r)$.

Consider the point $P = (\frac{r}{4}, \frac{r}{4}, \frac{r}{4})$. Then $d(a,p) = d(b,p) = d(c,p) = d(d,p) = \frac{3r}{4}$. Thus,

Elements	Direction Vector
a, b	$\pm(-\frac{r}{2}, -\frac{r}{2}, 0)$
a, c	$\pm(-\frac{r}{2}, 0, -\frac{r}{2})$
a, d	$\pm(0, -\frac{r}{2}, -\frac{r}{2})$
b, c	$\pm(0, \frac{r}{2}, -\frac{r}{2})$
b, d	$\pm(\frac{r}{2}, 0, -\frac{r}{2})$
c, d	$\pm(\frac{r}{2}, -\frac{r}{2}, 0)$

Figure 8.1: Pairs of elements and their corresponding direction vectors

D is contained in a ball of radius $\frac{3r}{4}$ about P.

Theorem 8.1.2. *The configuration D in* Example 8.1.1 *is not contained in a ball with radius less than $\frac{3r}{4}$ with centre an element of $\mathbb{Z}^3$.*

Proof. Observe that if D is contained in a ball of radius less than $\frac{3r}{4}$, then it is contained in a ball of radius $\frac{3r}{4} - 1$. So suppose towards a contradiction that D is contained in a ball of radius $\frac{3r}{4} - 1$ about some point $p = (p_1, p_2, p_3)$. We first show that $0 \leq p_1, p_2, p_3 \leq r/2$. If $p_1 > r/2$, then $|p_2| + |p_3| < \frac{r}{4} - 1$ as $d(p, a) \leq \frac{3r}{4} - 1$. But if $|p_2| + |p_3| < \frac{r}{4} - 1$, then $d(p, d) > \frac{3r}{4} - 1$ as $p_1 > r/2$. This is a contradiction as D is contained in a ball of radius $\frac{3r}{4} - 1$ about p. Thus, $p_1 \leq \frac{r}{2}$. A similar argument for p_2 and p_3 shows that $p_1, p_2, p_3 \leq \frac{r}{2}$. As $\frac{r}{2}$ is a positive integer and each of a, b, c, d have all co-ordinates greater than or equal to 0, we can assume without loss of generality that $p_1, p_2, p_3 \geq 0$. Thus, $0 \leq p_1, p_2, p_3 \leq \frac{r}{2}$. Now, we have $d(a, p), d(b, p), d(c, p), d(d, p) \leq \frac{3r}{4} - 1$, which gives the following inequalities:

$$p_1 + p_2 + p_3 \leq \frac{3r}{4} - 1,$$

$$(\frac{r}{2} - p_1) + (\frac{r}{2} - p_2) + p_3 \leq \frac{3r}{4} - 1,$$

$$(\tfrac{r}{2} - p_1) + p_2 + (\tfrac{r}{2} - p_3) \leq \tfrac{3r}{4} - 1,$$

$$p_1 + (\tfrac{r}{2} - p_2) + (\tfrac{r}{2} - p_3) \leq \tfrac{3r}{4} - 1.$$

Summing these inequalities, we obtain:

$$2(\tfrac{r}{2} - p_1) + 2(\tfrac{r}{2} - p_2) + 2(\tfrac{r}{2} - p_3) + 2p_1 + 2p_2 + 2p_3 \leq 3r - 4.$$

Dividing by 2, we obtain:

$$\tfrac{r}{2} - p_1 + \tfrac{r}{2} - p_2 + \tfrac{r}{2} - p_3 + p_1 + p_2 + p_3 \leq \tfrac{3r}{2} - 2.$$

Subtracting $\frac{3r}{2}$ from both sides of the inequality gives $0 \leq -2$, a contradiction. Thus, D is not contained in a ball of radius $\frac{3r}{4} - 1$. □

We now consider the radius of bi-centred and quad-centred balls the configuration is contained in. We first define bi-centred and quad-centred balls.

Definition 8.1.3. A *bi-centred ball of radius* r is the set of elements at distance at most r from at least one point contained in a pair of points $\{p, p'\}$ where $d(p, p') = 1$.

Definition 8.1.4. A *quad-centred ball of radius* r is the set of elements at distance at most r from at least one point contained in a 4-tuple of points $\{p_1, p_2, p_3, p_4\}$ where no pair of points in the 4-tuple is at distance more than 2 apart.

We now show that the result found in [3] that a $\overline{\mathrm{DD}}(\mathbb{Z}^2, m, r)$ is contained in a (possibly bi-centred or quad-centred) ball of radius $\frac{r}{2}$ does not necessarily hold for all values of n

and r for a bi-centred ball if we have $\frac{3r}{4} - 1 \geq \frac{r}{2} + 1$, which is true for all $r \geq 2$, and for a quad-centred ball if $\frac{3r}{4} - 1 \geq \frac{r}{2} + 2$, which is true for all $r \geq 12$.

Theorem 8.1.5. *The configuration D in* Example 8.1.1 *is not contained in either a bi-centred ball with radius $\frac{3r}{4} - 2$ or a quad-centred ball with radius $\frac{3r}{4} - 3$.*

Proof. By Theorem 8.1.2, D is not contained in a ball with radius $\frac{3r}{4} - 1$. A bi-centred ball of radius $\frac{3r}{4} - 2$ is contained in a ball of radius $\frac{3r}{4} - 1$, and a quad-centred ball of radius $\frac{3r}{4} - 3$ is contained in a ball of radius $\frac{3r}{4} - 1$. Thus, as D is not contained in a ball of radius $\frac{3r}{4} - 1$, it is not contained in either a bi-centred ball of radius $\frac{3r}{4} - 2$ or a quad-centred ball of radius $\frac{3r}{4} - 3$. □

We now show how Example 8.1.1 can be extended to larger values of n to produce a family of $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r)$ configurations such that no member of the family is contained in a ball of radius less than $\frac{3r}{4}$ about an element of $\mathbb{Z}^n$.

Example 8.1.6. Let n be divisible by 3, so that $n = 3k$ for some $k \in \mathbb{N}$. We now construct a distinct difference configuration in $\mathbb{Z}^n$. Set a to be the origin, and let b, c, d be as follows. Let the first $2k$ co-ordinates of b be equal to 1, and the final k co-ordinates be equal to 0. Let the first k co-ordinates of c be 1, the middle k co-ordinates be 0, and the final k co-ordinates be 1. Let the first k co-ordinates of d be equal to 0, and the final $2k$ co-ordinates be equal to 1. Set $D = \{a, b, c, d\}$.

We now show that D forms a $\overline{\mathrm{DD}}(\mathbb{Z}^n, 4, r)$ where $r = 2k$. Each element is at distance $2k$ from every other element, and so the maximum distance r is $2k$. We now consider the direction vectors between each pair of points, where we use the notation $(k, k, 0)$ to denote

a 1 in the first and second k co-ordinates and a 0 in the final k co-ordinates. Similarly, we use the notation $(-k, -k, 0)$ to denote a -1 in the first and second k co-ordinates and a 0 in the final k co-ordinates.

Elements	**Direction Vector**
a, b	$\pm(-k, -k, 0)$
a, c	$\pm(-k, 0, -k)$
a, d	$\pm(0, -k, -k)$
b, c	$\pm(0, k, -k)$
b, d	$\pm(k, 0, -k)$
c, d	$\pm(k, -k, 0)$

As these direction vectors are all pairwise distinct, D forms a $\overline{\mathrm{DD}}(\mathbb{Z}^n, 4, r)$.

Let P be a point such that the co-ordinates of P alternate between 0 and 1 every $\frac{k}{2}$ co-ordinates. We have $d(a, p) = d(b, p) = d(c, p) = d(d, p) = \frac{3k}{2}$. Thus D is contained in a ball of radius $\frac{3k}{2} = \frac{3r}{4}$ with centre P.

Theorem 8.1.7. *The* $\overline{\mathrm{DD}}(\mathbb{Z}^n, 4, r)$ *in* Example 8.1.6 *is not contained in a ball with radius less than* $\frac{3r}{4}$ *with centre an element of* $\mathbb{Z}^n$.

Proof. The proof is similar to the $\mathbb{Z}^3$ case in Theorem 8.1.2. Observe that if D is contained in a ball of radius less than $\frac{3k}{2}$, then it is contained in a ball of radius $\frac{3k}{2} - 1$. So suppose towards a contradiction that D is contained in a ball of radius $\frac{3k}{2} - 1$ about some point $p = (p_1, p_2, \ldots, p_{3k})$. As each of a, b, c, d has co-ordinates equal to either 0 or 1 and all co-ordinates are integers, we can assume without loss of generality that $p_i \in \{0, 1\}$ for all $i \in \{1, 2, \ldots, 3k\}$. We now prove the result. We have $d(a, p), d(b, p), d(c, p), d(d, p) \leq \frac{3k}{2} - 1$, which gives the following inequalities:

$$p_1 + p_2 + \ldots + p_{3k} \leq \tfrac{3k}{2} - 1,$$

$$(1-p_1) + (1-p_2) + \ldots + (1-p_k) + (1-p_{k+1}) + \ldots + (1-p_{2k}) + p_{2k+1} + \ldots + p_{3k} \leq \tfrac{3k}{2} - 1,$$

$$(1-p_1) + \ldots + (1-p_k) + p_{k+1} + \ldots + p_{2k} + (1-p_{2k+1}) + \ldots + (1-p_{3k}) \leq \tfrac{3k}{2} - 1,$$

$$p_1 + \ldots + p_k + (1-p_{k+1}) + \ldots + (1-p_{2k}) + (1-p_{2k+1}) + \ldots + (1-p_{3k}) \leq \tfrac{3k}{2} - 1.$$

Summing these inequalities, we obtain $2k + 2k + 2k \leq 6k - 4$ and thus $0 \leq -4$, a contradiction. Thus, D is not contained in a ball of radius $\frac{3k}{2} - 1 = \frac{3r}{4} - 1$ about an element of $\mathbb{Z}^n$. □

We now present a theorem which is analogous to Theorem 8.1.5, extended to the $\mathbb{Z}^n$ case rather than restricted to $\mathbb{Z}^3$.

Theorem 8.1.8. *The configuration D in* Example 8.1.6 *is not contained in either a bi-centred ball with radius $\frac{3r}{4} - 2$ or a quad-centred ball with radius $\frac{3r}{4} - 3$.*

Proof. The proof is similar to the $\mathbb{Z}^3$ case in Theorem 8.1.5. By Theorem 8.1.7, D is not contained in a ball with radius $\frac{3r}{4} - 1$. A bi-centred ball of radius $\frac{3r}{4} - 2$ is contained in a ball of radius $\frac{3r}{4} - 1$, and a quad-centred ball of radius $\frac{3r}{4} - 3$ is contained in a ball of radius $\frac{3r}{4} - 1$. Thus, as D is not contained in a ball of radius $\frac{3r}{4} - 1$, it is not contained in either a bi-centred ball of radius $\frac{3r}{4} - 2$ or a quad-centred ball of radius $\frac{3r}{4} - 3$. □

8.2 Constructions and Bounds in $\mathbb{Z}^n$

We now present our upper bound on the number of elements contained in a distinct difference configuration contained in $\mathbb{Z}^n$. We begin with a preliminary lemma.

Lemma 8.2.1. [20] *Let $\mathcal{B}_r^{\mathbb{Z}^n}(e)$ denote the ball of radius r in $\mathbb{Z}^n$ with centre e. We have*

$$|\mathcal{B}_r^{\mathbb{Z}^n}(e)| = \sum_{i=0}^{min\{n,r\}} 2^i \binom{n}{i}\binom{r}{i}.$$

Theorem 8.2.2. *If D is a $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r)$ where n is fixed, then $m(m-1) \leq \frac{2^n r^n}{n!} + O(r^{n-1})$ when r is sufficiently large. Indeed, we have $m \leq \frac{2^{n/2} r^{n/2}}{\sqrt{n!}} + O(r^{(n-1)/2})$.*

Proof. By Lemma 8.2.1 and Theorem 7.0.1, we have $m(m-1) \leq \sum_{i=0}^{min\{n,r\}} 2^i \binom{n}{i}\binom{r}{i}$. Note that when r is sufficiently large (in particular, larger than n), we have the following:

$$\begin{aligned}\binom{r}{n} &= \frac{r(r-1)\cdots(r-(n-1))(r-n)\cdots 2\cdot 1}{n!(r-n)!} \\ &= \frac{r(r-1)\cdots(r-(n-1))}{n!} \leq \frac{r^n}{n!}.\end{aligned}$$

As the remaining terms in the summation are of size $O(r^{n-1})$, this gives $|\mathcal{B}_r^{\mathbb{Z}^n}(e)| \leq \frac{2^n r^n}{n!} + O(r^{n-1})$. Thus, $m(m-1) \leq \frac{2^n r^n}{n!} + O(r^{n-1})$.

The above inequality implies that $(m-1)^2 \leq \frac{2^n r^n}{n!} + O(r^{n-1})$, and so $m - 1 \leq \sqrt{\frac{2^n r^n}{n!} + O(r^{n-1})}$. This gives $m - 1 \leq \frac{2^{n/2} r^{n/2}}{\sqrt{n!}} + O(r^{(n-1)/2})$. Thus, $m \leq \frac{2^{n/2} r^{n/2}}{\sqrt{n!}} + O(r^{(n-1)/2}) + 1$ and so $m \leq \frac{2^{n/2} r^{n/2}}{\sqrt{n!}} + O(r^{(n-1)/2})$. □

Remark 8.2.3. Observe that as with Theorem 7.0.1, the bound in Theorem 8.2.2 implies that the number of elements contained in a distinct difference configuration in $\mathbb{Z}^n$ with

maximum distance r is at most approximately the square root of the size of the ball of radius r with centre e.

We now present the lower bound on the number of elements m in a distinct difference configuration where m is maximised obtained by using Theorem 7.0.2.

Theorem 8.2.4. *Let $n \in \mathbb{N}$ be fixed. As r tends to infinity, there exists a $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r)$ such that $m \geq \lfloor \frac{2^{n/4}(\frac{r}{2})^{n/4}}{(n!)^{1/4}} \rfloor$.*

Proof. By Theorem 7.0.2 there exists a distinct difference configuration of size m contained in $\mathcal{B}^{\mathbb{Z}^n}_{r/2}(e)$ if m satisfies $\frac{m^4}{|\mathcal{B}^{\mathbb{Z}^n}_{r/2}(e)|} + m^2 p_{r/2} < 1$, where $p_{r/2}$ is the probability that an element in $\mathcal{B}^{\mathbb{Z}^n}_{r/2}(e)$ has order 2. As $\mathbb{Z}^n$ contains no elements of order 2, we have $p_{r/2} = 0$. Thus, we require only that $m^4 < |\mathcal{B}^{\mathbb{Z}^n}_{r/2}(e)|$. As r tends to infinity we have $\binom{r/2}{n} = \frac{(r/2)^n}{n!} + O((\frac{r}{2})^{n-1})$. By Lemma 8.2.1, we thus have $|\mathcal{B}^{\mathbb{Z}^n}_{r/2}(e)| = \frac{2^n(\frac{r}{2})^n}{n!} + O((\frac{r}{2})^{n-1})$. Thus, we require $m^4 < \frac{2^n(\frac{r}{2})^n}{n!} + O((\frac{r}{2})^{n-1})$. Setting $m = \lfloor \frac{2^{n/4}(\frac{r}{2})^{n/4}}{(n!)^{1/4}} \rfloor$ satisfies this inequality, and so by Theorem 7.0.2 there exists a $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r)$ such that $m \geq \lfloor \frac{2^{n/4}(\frac{r}{2})^{n/4}}{(n!)^{1/4}} \rfloor$ as r tends to infinity.

□

Corollary 8.2.5. *Let $n \in \mathbb{N}$ be fixed. As r tends to infinity, a $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r)$ where m is of maximal size is such that $\lfloor \frac{2^{n/4}(\frac{r}{2})^{n/4}}{(n!)^{1/4}} \rfloor \leq m \leq \frac{2^{n/2} r^{n/2}}{\sqrt{n!}} + O(r^{(n-1)/2})$.*

Proof. By Theorem 8.2.4, there exists a $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r)$ such that $m \geq \lfloor \frac{2^{n/4}(\frac{r}{2})^{n/4}}{(n!)^{1/4}} \rfloor$. By Theorem 8.2.2, we have $m \leq \frac{2^{n/2} r^{n/2}}{\sqrt{n!}} + O(r^{(n-1)/2})$. □

We now present our construction of a distinct difference configuration for $\mathbb{Z}$. We make use of a construction by Singer (see [36]).

Construction 8.2.6. Consider the cyclic group $\mathbb{Z}_\alpha = \{e, a, a^2, \ldots, a^{\alpha-1}\}$, and the integer $\lfloor \frac{\alpha}{2} \rfloor$. Let P be the largest prime such that $P^2 + P + 1 \leq \min\{\lfloor \frac{\alpha}{2} \rfloor, r\}$. The Singer Construction in [36] produces a Golomb Ruler R of length P^2+P+1 with $P+1$ markings.

Now, translate the elements of R so that the smallest integer in the translated ruler R^* is 0 and the largest is $P^2 + P + 1 \leq \lfloor \frac{\alpha}{2} \rfloor$. Let $\varphi \colon R^* \to \mathbb{Z}_\alpha$ be a map where $\varphi(k) = a^k$. Set $D = \{\varphi(i) \colon i \in R^*\}$. We set the generating set to be $\{a, a^{-1}\}$.

Theorem 8.2.7. *For sufficiently large α and $r \geq \lfloor \frac{\alpha}{2} \rfloor$,* Construction 8.2.6 *produces a $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ where $m \geq \lfloor \sqrt{\frac{\alpha}{2}} \rfloor - (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^{0.525}$. For sufficiently large α and $r < \lfloor \frac{\alpha}{2} \rfloor$,* Construction 8.2.6 *produces a $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ where $m \geq \lfloor \sqrt{\frac{r}{2}} \rfloor - (\lfloor \sqrt{\frac{r}{2}} \rfloor - 1)^{0.525}$.*

Proof. We first prove that D forms a $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ where the distance between a pair of points is at most $\min\{\lfloor \sqrt{\frac{\alpha}{2}} \rfloor, r\}$. Suppose towards a contradiction that D does not form a distinct difference configuration. Then there exist $a^i, a^j, a^k, a^l \in D$ such that $a^{-i}a^j = a^{-k}a^l$. This implies that $j - i \equiv l - k \bmod \alpha$ and so $l + i \equiv k + j \bmod \alpha$. Observe that by construction, we have $i, j, k, l \leq \frac{\alpha}{2}$. If $l + i \equiv k + j \equiv 0$ and at least one of $i, j, k, l \not\equiv 0$, then $i = j = k = l = \frac{\alpha}{2}$, so (i, j) and (k, l) are the same pair of elements. Now consider the case where $0 \leq l + i < \alpha$ and $0 \leq k + j < \alpha$. This implies that $j - i = l - k$. As R^* is a distinct difference configuration, this is a contradiction. Thus, D forms a distinct difference configuration. Furthermore, as the generating set of $\mathbb{Z}$ is closed under inverses, the distance between a pair of points in D is at most the length of R^*. Hence, it is at most $P^2 + P + 1 \leq \min\{\lfloor \frac{\alpha}{2} \rfloor, r\}$.

We now consider the number of elements contained in the configuration produced by

Construction 8.2.6. If $r \geq \lfloor \frac{\alpha}{2} \rfloor$, then P is the largest prime such that $P^2 + P + 1 \leq \lfloor \frac{\alpha}{2} \rfloor$. Observe that $(\lfloor \sqrt{\frac{\alpha}{2}} \rfloor)^2 + \lfloor \sqrt{\frac{\alpha}{2}} \rfloor + 1 > \frac{\alpha}{2}$ – thus, $P < \lfloor \sqrt{\frac{\alpha}{2}} \rfloor$. Furthermore, $(\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^2 + (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1) + 1 = (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor)^2 - \lfloor \sqrt{\frac{\alpha}{2}} \rfloor + 1 \leq \frac{\alpha}{2}$ for all $\alpha \geq 2$. So P is at most $(\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)$. Now, by Lemma 5.2.3, there exists a prime number in the interval $[\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1 - (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^{0.525}, \lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1]$ for sufficiently large α. We therefore have $P \geq \lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1 - (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^{0.525}$. As Construction 8.2.6 produes a configuration with $P + 1$ markings, our configuration is of size at least $\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^{0.525}$. If $r < \lfloor \frac{\alpha}{2} \rfloor$, then P is the largest prime such that $P^2 + P + 1 \leq r$. By a similar argument, Construction 8.2.6 produces a configuration containing at least $\lfloor \sqrt{\frac{r}{2}} \rfloor - (\lfloor \sqrt{\frac{r}{2}} \rfloor - 1)^{0.525}$ elements. □

We now show how we can use Construction 8.2.6 to produce a distinct difference configuration D^* in $\mathbb{Z}^2$.

Construction 8.2.8. Let $\alpha = p \cdot q$ where p, q are primes and $p \neq q$. Let D be the $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ produced by Construction 8.2.6 and let $\phi\colon D \to \mathbb{Z}^2$ be a mapping where $\phi(x) = (x \bmod p, x \bmod q)$. Set $D^* = \{\phi(i)\colon i \in D\}$.

Theorem 8.2.9. Construction 8.2.8 *produces a* $\overline{\mathrm{DD}}(\mathbb{Z}^2, m, r^*)$ *where* $m = |D|$ *and* $r^* \leq p + q$.

Proof. We first prove that D^* forms a distinct difference configuration. Note that p and q are co-prime. By the Chinese Remainder Theorem, for $x, y \in \mathbb{Z}_{pq}$ there exist unique $(a, b), (c, d) \in \mathbb{Z}_p \times \mathbb{Z}_q$ such that $x \equiv a \bmod p$, $x \equiv b \bmod q$ and $y \equiv c \bmod p$, $y \equiv d \bmod q$. Furthermore, $x - y$ has a unique representation as $(a - c, b - d) \in \mathbb{Z}_p \times \mathbb{Z}_q$. If D^* does not form a distinct difference configuration, then there exist two different pairs of elements

$(a_1, a_2), (b_1, b_2)$ and $(c_1, c_2), (d_1, d_2)$ in D^* where $(a_1, a_2) \neq (b_1, b_2)$ and $(c_1, c_2) \neq (d_1, d_2)$ such that $(a_1 - b_1, a_2 - b_2) = (c_1 - d_1, c_2 - d_2)$. Then $(a_1 - b_1, a_2 - b_2)$ is the unique representation of $\phi^{-1}((a_1, a_2)) - \phi^{-1}((b_1, b_2))$ and $\phi^{-1}((c_1, c_2)) - \phi^{-1}((d_1, d_2))$. But as D is a distinct difference configuration, this implies that $\phi^{-1}((a_1, a_2)) = \phi^{-1}((c_1, c_2))$ and $\phi^{-1}((b_1, b_2)) = \phi^{-1}((d_1, d_2))$. Thus, $(a_1, a_2) = (c_1, c_2)$ and $(b_1, b_2) = (d_1, d_2)$ and so $(a_1, a_2), (b_1, b_2)$ and $(c_1, c_2), (d_1, d_2)$ are the same pair. Hence, D^* must form a distinct difference configuration.

We now show that $m = |D|$. As ϕ is a bijection (by the Chinese Remainder Theorem), there is a one-to-one correspondence between the elements in D and those in D^*. Thus, $|D| = |D^*|$.

We now show that the distance between a pair of elements in D^* is at most $p + q$. Each pair of elements in D^* is of the form $(u \bmod p, u \bmod q), (v \bmod p, v \bmod q)$ for some $u, v \in D$. Therefore the distance between a pair of elements in D^* is $|(u \bmod p - v \bmod p)| + |(u \bmod q - v \bmod q)| \leq p + q$. Thus, every pair of elements is at distance at most $p + q$ apart and so $r^* \leq p + q$. □

Remark 8.2.10. We make three observations regarding Construction 8.2.8. Firstly, as every element in D^* is of the form (a, b) where $0 \leq a \leq p$ and $0 \leq b \leq q$, it follows that D^* is contained in a $p \times q$ rectangle.

Secondly, suppose without loss of generality that $p > q$. Then D^* is contained in a ball of radius p about $(\frac{p}{2}, \frac{p}{2})$, which has size $2p^2 + 2p + 1$. By Theorem 7.0.1, a distinct difference configuration contained in this ball has at most $\sqrt{2}p + O(\sqrt{p})$ elements. Now, if α is

sufficiently large and $r \geq \lfloor \frac{\alpha}{2} \rfloor$, then $|D^*| \geq \lfloor \sqrt{\frac{\alpha}{2}} \rfloor - (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^{0.525}$. If p and q are approximately equal, then $p \approx \sqrt{\alpha}$, and so D^* contains approximately $\lfloor \frac{p}{\sqrt{2}} \rfloor - (\lfloor \frac{p}{\sqrt{2}} \rfloor - 1)^{0.525}$ elements (as a minimum). Thus, the number of elements in D^* is optimal up to multiplication by a constant.

Thirdly, we use the $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ produced by Construction 8.2.6 in Construction 8.2.8, as this produces a distinct difference configuration with m close to the upper bound. However, any $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ could be used.

We now provide a generalised version of Construction 8.2.8 which applies to all values of n. We first define some notation, which we adapt from Construction 8.2.8. Let $\alpha = p_1 \cdot p_2 \cdots p_n$ where p_i is prime and $p_i \neq p_j$ unless $i = j$ for all $i, j \in \{1, 2, \ldots, n\}$. Then $p_1, p_2, \ldots, p_n$ are co-prime.

Construction 8.2.11. Let D be the $\overline{\mathrm{DD}}(\mathbb{Z}_\alpha, m, r)$ produced by Construction 8.2.6 and let $\phi\colon D \to \mathbb{Z}^n$ be a mapping where $\phi(x) = (x \bmod p_1, x \bmod p_2, \ldots, x \bmod p_n)$. Set $D^* = \{\phi(i)\colon i \in D\}$.

Theorem 8.2.12. Construction 8.2.11 *produces a* $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, r^*)$ *where* $m = |D|$ *and* $r^* \leq p_1 + p_2 + \ldots + p_n$.

Proof. We first prove that D^* forms a distinct difference configuration. By the Chinese Remainder Theorem, for $x, y \in \mathbb{Z}_\alpha$ there exist unique $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_n}$ such that $x \equiv x_1 \bmod p_1, x \equiv x_2 \bmod p_2, \ldots, x \equiv x_n \bmod p_n$ and $y \equiv y_1 \bmod p_1, y \equiv y_2 \bmod p_2, \ldots, y \equiv y_n \bmod p_n$. Furthermore, $x - y$ has a unique representation as $(x_1 - y_1, x_2 - y_2, \ldots, x_n - y_n) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_n}$. Now,

if D^* does not form a distinct difference configuration then there exist two different pairs of elements $((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n))$ and $((c_1, c_2, \ldots, c_n), (d_1, d_2 \ldots, d_n))$ in D^* where $(a_1, a_2, \ldots, a_n) \neq (b_1, b_2, \ldots, b_n)$ and $(c_1, c_2, \ldots, c_n) \neq (d_1, d_2, \ldots, d_n)$ such that $(a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n) = (c_1 - d_1, c_2 - d_2, \ldots, c_n - d_n)$. Then $(a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n)$ is the unique representation of $\phi^{-1}((a_1, a_2, \ldots, a_n)) - \phi^{-1}((b_1, b_2, \ldots, b_n))$ and $\phi^{-1}((c_1, c_2, \ldots, c_n)) - \phi^{-1}((d_1, d_2, \ldots, d_n))$. But as D is a distinct difference configuration, this implies that $\phi^{-1}((a_1, a_2, \ldots, a_n)) = \phi^{-1}((c_1, c_2, \ldots, c_n))$ and $\phi^{-1}((b_1, b_2, \ldots, b_n)) = \phi^{-1}((d_1, d_2, \ldots, d_n))$. Thus, $(a_1, a_2, \ldots, a_n) = (c_1, c_2, \ldots, c_n)$ and $(b_1, b_2, \ldots, b_n) = (d_1, d_2, \ldots, d_n)$ and so $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)$ and $(c_1, c_2, \ldots, c_n), (d_1, d_2, \ldots, d_n)$ are the same pair. Hence, D^* forms a distinct difference configuration.

We now show that $m = |D|$. As ϕ is a bijection (by the Chinese Remainder Theorem), there is a one-to-one correspondence between the elements in D and those in D^*. Thus, $|D| = |D^*|$.

We now show that the distance between a pair of elements in D^* is at most $p_1 + p_2 + \ldots + p_n$. Each pair of elements in D^* is of the form $((u \bmod p_1, u \bmod p_2, \ldots, u \bmod p_n), (v \bmod p_1, v \bmod p_2, \ldots, v \bmod p_n))$ for some $u, v \in D$. Therefore the distance between a pair of elements in D^* is $|(u \bmod p_1 - v \bmod p_1)| + |(u \bmod p_2 - v \bmod p_2)| + \ldots + |(u \bmod p_n - v \bmod p_n)| \leq p_1 + p_2 + \ldots + p_n$. Thus, every pair of elements is at distance at most $p_1 + p_2 + \ldots + p_n$ apart and so $r^* \leq p_1 + p_2 + \ldots + p_n$. □

Remark 8.2.13. We make two observations regarding Construction 8.2.11. Firstly, as every element in D^* is of the form $(a_1, a_2, \ldots, a_n)$ where $0 \leq a_i \leq p_i$ for all $i \in \{1, 2, \ldots, n\}$,

it follows that D^* is contained in a $p_1 \times p_2 \times \ldots \times p_n$ box.

Secondly, suppose without loss of generality that $p_1 > p_i$ for all $i \in \{2, 3, \ldots, n\}$. Then D^* is contained in a ball of radius $n \cdot \frac{p_1}{2}$ about $(\frac{p_1}{2}, \frac{p_1}{2}, \ldots, \frac{p_1}{2})$, and the maximum distance in D^* is at most $n \cdot p_1$. By Theorem 8.2.2, if $n \cdot p_1$ is sufficiently large then a $\overline{\mathrm{DD}}(\mathbb{Z}^n, m, n \cdot p_1)$ is such that $m \leq \frac{2^{n/2}(n \cdot p_1)^{n/2}}{\sqrt{n!}} + O((n \cdot p_1)^{(n-1)/2})$. Now, if α is sufficiently large and $r \geq \lfloor \frac{\alpha}{2} \rfloor$, then $|D^*| \geq \lfloor \sqrt{\frac{\alpha}{2}} \rfloor - (\lfloor \sqrt{\frac{\alpha}{2}} \rfloor - 1)^{0.525}$. If the p_i are approximately equal then $p_1 \approx \alpha^{1/n}$, and so $p_1^{n/2} \approx \sqrt{\alpha}$. Thus, D^* contains approximately $\lfloor \sqrt{\frac{p_1^n}{2}} \rfloor - (\lfloor \sqrt{\frac{p_1^n}{2}} \rfloor - 1)^{0.525}$ elements (as a minimum). Thus, the number of elements m in D^* is optimal up to multiplication by a constant.

8.3 Applications to Dihedral Group

We provide upper and lower bounds on the number of elements contained in a distinct difference configuration in the dihedral group. Observe that the results in this section come from the fact that the dihedral group contains a large subgroup with very few involutions (sometimes zero, depending on the order of the group), and we can work within this subgroup to produce large distinct difference configurations. Similar results would therefore apply to any group with this structure. We begin by defining the dihedral group and the generating set we use throughout.

Let $D_{2k} = \langle a, b, a^{k-1} | a^k = e, b^2 = e, bab = a^{-1} \rangle$. Note that the 'standard' generating set omits a^{k-1} as a generating element, however as we require the generating set to be closed under inverses we include it. Observe that approximately half the elements of the dihedral

group have order 2. Our probabilistic lower bound in Theorem 7.0.2 gives a weaker lower bound on the maximum number of elements contained in a distinct difference configuration if the group has a large number of elements of order 2. By showing that a large distinct difference configuration can still be obtained in a group with a high proportion of elements of order 2, we show that such a group may still be useful in the applications of distinct difference configurations (in addition to being mathematically interesting in its own right). We begin with the lower bound obtained by applying Theorem 7.0.2 to the dihedral group.

Theorem 8.3.1. *Let $r/2 \leq k$. There exists a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ such that $m = \lceil (\frac{r}{2})^{1/4} \rceil - 1$.*

Proof. By Theorem 7.0.2, a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ exists if the value of m satisfies $\frac{m^4}{|\mathcal{B}_{r/2}(e)|} + m^2 p_{r/2} < 1$, where $p_{r/2}$ denotes the probability that an element in $\mathcal{B}_{r/2}(e)$ has order 2. Consider the cyclic subgroup of order k in D_{2k} – that is, the set of elements $\{e, a, a^2, \ldots, a^{k-1}\}$. As k is odd, this set contains no elements of order 2. This set therefore has $p_{r/2} = 0$ and for all r and k we have $|\mathcal{B}_{r/2}(e)| \geq r/2$. Thus, by Theorem 7.0.2, a distinct difference configuration contained in the cyclic subgroup containing m elements exists if $m^4 < r/2$ for sufficiently large r. Setting $m = \lceil (\frac{r}{2})^{1/4} \rceil - 1$ satisfies this inequality, and so a distinct difference configuration of size $m = \lceil (\frac{r}{2})^{1/4} \rceil - 1$ contained in the cyclic subgroup exists. Thus, a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ where $m = \lceil (\frac{r}{2})^{1/4} \rceil - 1$ exists. □

We now show how to apply Construction 8.2.6 to the dihedral group to obtain an improved lower bound for both odd and even k.

Theorem 8.3.2. *For sufficiently large k and $r \geq \lfloor \frac{n}{2} \rfloor$, there exists a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ where $m \geq \lfloor \sqrt{\frac{k}{2}} \rfloor - (\lfloor \sqrt{\frac{k}{2}} \rfloor - 1)^{0.525}$. For sufficiently large k and $r < \lfloor \frac{k}{2} \rfloor$, there exists a*

$\overline{\mathrm{DD}}(D_{2k}, m, r)$ *where* $m \geq \lfloor\sqrt{\frac{r}{2}}\rfloor - (\lfloor\sqrt{\frac{r}{2}}\rfloor - 1)^{0.525}$.

Proof. We apply Construction 8.2.6 to the cyclic subgroup of order k. Theorem 8.2.7 then gives the result. □

We now provide an upper bound on the number of elements contained in a distinct difference configuration contained in the dihedral group.

Theorem 8.3.3. *If D is a $\overline{\mathrm{DD}}(D_{2k}, m, r)$, then $m(m-1) \leq 2r+1$. Indeed, we have $m \leq \sqrt{2r+1}+1$.*

Proof. We have $|\mathcal{B}_r(e)| = 2r$ if $r = k$. Otherwise, $|\mathcal{B}_r(e)| = 2r+1$. So $|\mathcal{B}_r(e)| \leq 2r+1$ for all r. By Theorem 7.0.1, we have $m(m-1) \leq 2r+1$ for all r. Thus, $(m-1)^2 \leq 2r+1$ and so $m-1 \leq \sqrt{2r+1}$. Hence, $m \leq \sqrt{2r+1}+1$. □

Corollary 8.3.4. *Let D be a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ such that m is of maximum possible size and k is sufficiently large. If $r < \lfloor\frac{k}{2}\rfloor$ then $\lfloor\sqrt{\frac{r}{2}}\rfloor - (\lfloor\sqrt{\frac{r}{2}}\rfloor - 1)^{0.525} \leq m \leq \sqrt{2r+1}+1$. If $r \geq \lfloor\frac{k}{2}\rfloor$ then $\lfloor\sqrt{\frac{k}{2}}\rfloor - (\lfloor\sqrt{\frac{k}{2}}\rfloor - 1)^{0.525} \leq m \leq \sqrt{2r+1}+1$.*

Proof. By Theorem 8.3.2, if $r < \lfloor\frac{k}{2}\rfloor$ then there exists a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ such that $m \geq \lfloor\sqrt{\frac{r}{2}}\rfloor - (\lfloor\sqrt{\frac{r}{2}}\rfloor - 1)^{0.525}$. Furthermore, if $r \geq \lfloor\frac{k}{2}\rfloor$ then there exists a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ such that $m \geq \lfloor\sqrt{\frac{k}{2}}\rfloor - (\lfloor\sqrt{\frac{k}{2}}\rfloor - 1)^{0.525}$. By Theorem 8.3.3 $m \leq \sqrt{2r+1}+1$ for all r. □

Remark 8.3.5. Observe that as $r \leq k$ in the dihedral group, the bounds stated in Corollary 8.3.4 imply the following. If $r < \lfloor\frac{k}{2}\rfloor$ then we can construct a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ of size $\Omega(\sqrt{r})$ and the upper bound on the number of elements contained in such a configuration is $O(\sqrt{r})$. If $r \geq \lfloor\frac{k}{2}\rfloor$ then we can construct a $\overline{\mathrm{DD}}(D_{2k}, m, r)$ of size $\Omega(\sqrt{k})$ and the upper bound on the number of elements contained in such a configuration is $O(\sqrt{k})$. We can

therefore construct a distinct difference configuration with an optimal number of elements up to multiplication by a constant. Thus, it is possible to find 'large' distinct difference configurations in groups which contain a high proportion of elements of order 2.

Chapter 9

Difference from Unique Pair Configurations

We introduce the concept of a 'difference from unique pair configuration' (DUPC), a natural generalisation of our definition of a $\overline{\mathrm{DD}}(G, S, m, r)$ which allows for two differences to be equal provided they are formed by the same pair of elements. We motivate the study of these configurations by showing that if the group G contains elements of order 2, the lower bound given by the probabilistic argument in Theorem 7.0.2 is not restricted in the same way as it is when applied to distinct difference configurations. We show that a set contained in a group G where G contains no elements of order 2 forms a DUPC if and only if it forms a $\overline{\mathrm{DD}}(G, S, m, r)$. Finally, we provide an example of a set which forms a DUPC but not a $\overline{\mathrm{DD}}(G, S, m, r)$, and does not necessarily retain the property that a pair of nodes share at most one key in common when we apply our key predistribution scheme. Thus, whilst DUPCs are a natural generalisation of the concept of a $\overline{\mathrm{DD}}(G, S, m, r)$ and

merit further study, they are not necessarily appropriate for the applications of our work to key predistribution.

Definition 9.0.1. Let G be a group, S a generating set of G, and $D \subseteq G$ where $D = \{d_1, d_2, \ldots, d_m\}$ and every pair of elements in D is at distance at most r apart. Then D is a *difference from unique pair configuration*, denoted $\widetilde{\mathrm{DD}}(G, S, m, r)$, if for any non-identity element $g \in G$ there exists at most one unordered pair of elements $\{d_i, d_j\} \in D$ where $d_i \neq d_j$ such that either $d_i^{-1} d_j = g$ or $d_j^{-1} d_i = g$.

Informally, if given any element in G there exists at most one pair of distinct elements in D with a difference equal to g, then D is a difference from unique pair configuration.

We now provide a lower bound on the size of a difference from unique pair configuration in which the number of elements is maximised. Note that this is similar to Theorem 7.0.2, however our use of difference from unique pair configurations means that elements of order 2 do not cause bad events as they do with distinct difference configurations.

Theorem 9.0.2. *Let G be a group and S a generating set of G where S is closed under inverses. For sufficiently large L there exists a difference from unique pair configuration $D \subseteq \mathcal{B}_L$ of size m if the inequality $\frac{m^4}{|\mathcal{B}_L|} < 1$ is satisfied.*

Proof. The proof is similar to that in Theorem 7.0.2. However, note that $x_l^{-1} x_k = x_k^{-1} x_l$ for some $x_k, x_l \in D$ is not a bad event as a difference from unique pair configuration allows differences to be equal if those differences are formed by the same pair of elements. We therefore require only that $\frac{m^4}{|\mathcal{B}_L|} < 1$ is satisfied. □

Corollary 9.0.3. *Let G be a group and S a generating set of G where S is closed under inverses. If $|\mathcal{B}_L| \geq a^L$ for some $a > 1$, then a difference from unique pair configuration D of maximal size contained in $\mathcal{B}_L$ is such that $|D| \geq \lfloor b^L \rfloor$ for some $b > 1$. Indeed, we may take $b = a^{1/4-\varepsilon}$ for some $0 < \varepsilon < \frac{1}{4}$.*

Proof. Let $|D| = m$. By Theorem 9.0.2, there exists a difference of unique pair configuration of size m contained in $\mathcal{B}_L$ if m satisfies $\frac{m^4}{|\mathcal{B}_L|}$ and so $m^4 < |\mathcal{B}_L|$. We have $|\mathcal{B}_L| \geq a^L$. So we require $m < (a^{1/4})^L$. Set $b = a^{1/4-\varepsilon}$ where $0 < \varepsilon < \frac{1}{4}$. As $a > 1$, we have $b > 1$. Furthermore, $(a^{1/4})^L > b^L$. Set $m = \lfloor b^L \rfloor$. □

We now provide a theorem which states that if a group contains no elements of order 2, then a difference from unique pair configuration contained in that group also forms a distinct difference configuration (and vice-versa).

Theorem 9.0.4. *Let G be a group which contains no elements of order 2, S a generating set of G where S is closed under inverses, and $D \subseteq G$. Then D forms a $\widetilde{\mathrm{DD}}(G, S, m, r)$ if and only if D forms a $\overline{\mathrm{DD}}(G, S, m, r)$.*

Proof. We first prove that if D forms a $\widetilde{\mathrm{DD}}(G, S, m, r)$ then D also forms a $\overline{\mathrm{DD}}(G, S, m, r)$. Suppose towards a contradiction that G contains no elements of order 2, and that D forms a $\widetilde{\mathrm{DD}}(G, S, m, r)$ but not a $\overline{\mathrm{DD}}(G, S, m, r)$. Then there exist two pairs of elements $(d_i, d_j) \in D$ and $(d_k, d_l) \in D$ such that $i \neq j$ and $k \neq l$ and $d_i^{-1} d_j = d_k^{-1} d_l$ and $d_i = d_l$ and $d_j = d_k$. We now explain why we have the condition $d_i = d_l$ and $d_j = d_k$. As D forms a $\widetilde{\mathrm{DD}}(G, S, m, r)$, two pairs of distinct elements with the same difference must be the same pair. Therefore, d_i, d_j and d_k, d_l are the same pair. If $d_i = d_k$ and $d_j = d_l$ for all such pairs then D forms a $\overline{\mathrm{DD}}(G, S, m, r)$ by definition, a contradiction. So we must

have $d_i = d_l$ and $d_j = d_k$. Thus, we have $d_i^{-1}d_j = d_j^{-1}d_i$. Left multiplying by d_i and subsequently by d_j^{-1}, we obtain $e = d_j^{-1}d_i d_j^{-1}d_i$. Then $e = (d_j^{-1}d_i)^2$ and so G contains an element of order 2, a contradiction. Thus, D forms a $\overline{\mathrm{DD}}(G, S, m, r)$.

For the converse implication, observe that by definition if D forms a $\overline{\mathrm{DD}}(G, S, m, r)$ then D forms a $\widetilde{\mathrm{DD}}(G, S, m, r)$. □

We now provide an example which shows that given a group G, a difference from unique pair configuration $D \subseteq G$ and an element $g \in G$, it does not necessarily follow that gD is such that $|D \cap gD| \leq 1$. By Theorem 2.4.2, if D were a distinct difference configuration then it would follow that $|D \cap gD| \leq 1$. This property follows from the fact that difference from unique pair configurations allow for involutory differences, whereas distinct difference configurations do not. This property ensures that a pair of nodes share at most one key in common, and so the key storage capacity of the nodes is not wasted. Thus, using a difference from unique pair configuration does not ensure that a pair of nodes will share at most one key in common, and so such a configuration may not be appropriate for our applications.

Example 9.0.5. Let $G = \mathbb{Z}_2^3$, so $G = \{0,1\}^3, S = \{(1,0,0),(0,1,0),(0,0,1)\}$, and $1+1 = 0$. Let $D = \{(1,1,0),(1,0,1),(0,1,1)\}$ and label these elements as a, b, c respectively. The possible pairs of distinct elements are $(a,b),(a,c),(b,c)$. We now list the differences formed by these pairs:

$$D(a,b) = (0,1,1) = D(b,a),$$

$$D(a,c) = (1,0,1) = D(c,a),$$

$$D(b, c) = (1, 1, 0) = D(c, b).$$

We have $D(a, b) = D(b, a)$, and so D does not form a distinct difference configuration. As the differences formed by different pairs of elements are pairwise distinct, for every difference $x \in G$ there exists at most one pair of elements $d_1, d_2 \in D$ such that either $d_1^{-1}d_2 = x$ or $d_2^{-1}d_1 = x$. Thus, D forms a difference from unique pair configuration. Let $g = (0, 1, 1)$. Then $gD = \{(1, 0, 1), (1, 1, 0), (0, 0, 0)\}$, and so $|D \cap gD| = 2$.

Bibliography

[1] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes, ii. *Proceedings of the London Mathematical Society*, 83(3):pp. 532–562, (2003).

[2] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson. Efficient key predistribution for grid-based wireless sensor networks. In *Proceedings of the* 3^{rd} *International Conference on Information Technology and Science*, pages 54–69. Springer, (2008).

[3] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson. Two-dimensional patterns with distinct differences – constructions, bounds, and maximal anticodes. *IEEE Transactions on Information Theory*, 56(3):pp. 1216–1229, (2010).

[4] S. R. Blackburn, A. Panoui, M. B. Paterson, and D. Stinson. Honeycomb arrays. *The Electronic Journal of Combinatorics*, page R172, (2010).

[5] R.C. Bose. An affine analogue of singer's theorem. *J. Ind. Math. Soc.*, 6:1–15, (1942).

[6] P. J. Cameron. *Combinatorics: Topics, Techniques, Algorithms*. Cambridge University Press, (1994).

[7] S. A. Camtepe, B. Yener, and M. Yung. Expander graph based key distribution

mechanisms in wireless sensor networks. In *2006 IEEE international conference on communications*, volume 5, pages 2262–2267. IEEE, (2006).

[8] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *2003 Symposium on Security and Privacy, 2003.*, pages 197–213. IEEE, (2003).

[9] J. Colannino. Circular and modular Golomb rulers, (2003). URL `http://cgm.cs.mcgill.ca/~athens/cs507/Projects/2003/JustinColannino/`.

[10] Charles Colbourne and Jeffrey Dinitz. *Handbook of combinatorial designs*. CRC press Boca Raton, FL, (2007).

[11] A. Ćustić, V. Krčadinac, and Y. Zhou. Tiling groups with difference sets. *The Electronic Journal of Combinatorics*, 22(2), (2015).

[12] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):228–258, (2005).

[13] X. Du, M. Galloway, F. Hu, Rai V. K., Bo Sun, and Y. Xiao. A survey of key management schemes in wireless sensor networks. *Computer Communications*, 30 (11-12):pp. 2314–2341, (2007).

[14] P. Erdős and P. Turán. On a problem of Sidon in additive number theory, and on some related problems. *Journal of the London Mathematical Society*, 16(4):212–215, (1941).

[15] P. Erdős, R. Graham, Z. Ruzsa, and H. Taylor. Bounds for arrays of dots with distinct slopes or lengths. *Combinatorica*, 12(1):pp.39–44, (1992).

[16] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41–47, (2002).

[17] A. Golemac, J. Mandić, and T. Vučičić. One (96, 20, 4)-symmetric design and related nonabelian difference sets. *Designs, Codes and Cryptography*, 37(1):pp. 5–13, (2005).

[18] S. Golomb. How to number a graph. *Graph Theory and Computing*, pages pp. 23–37, (1972).

[19] S. Golomb and H. Taylor. Constructions and properties of Costas arrays. In *Proceedings of the Institute of Electrical and Electronics Engineers*, volume 72, pages 1143–1163. IEEE, (1984).

[20] S. Golomb and L. R. Welch. Perfect codes in the Lee metric and the packing of polyominoes. *SIAM Journal on Applied Mathematics*, 18(2):302–317, (1970).

[21] S. M. Guru, D. Hugo, P. McCarthy, J. McCulloch, W. Peng, and A. Terhorst. Wireless sensor network deployment deployment for water use efficiency in irrigation. In *Proceedings of the Workshop on Real-World Wireless Sensor Networks*, pages 46–50, (2008).

[22] P. Hall. On representatives of subsets. In *Classic Papers in Combinatorics*, pages 58–62. Springer, (2009).

[23] R. Han, C. Hartung, S. Holbrook, and C. Seielstad. Firewxnet: A multi-tiered portable wireless system for monitoring weather conditions in wildland fire environments. In *Proceedings of the* 4^{th} *International Conference on Mobile Systems, Applications and Services*, pages 28–41. ACM, (2006).

[24] J. E. Iiams. A note on certain 2-groups with Hadamard difference sets. *Designs, Codes and Cryptography*, 23(1):pp. 75–80, (2001).

[25] N. Kajastie. Slope engineering: Giving a signal, (2021). URL `https://www.geplus.co.uk/features/slope-engineering-giving-a-signal-08-06-2021/`.

[26] J. Lee and D. R. Stinson. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. *ACM Transactions on Information and System Security (TISSEC)*, 11(2):1–35, (2008).

[27] S. A. Lyon, M. Martonosi, C. M. Sadler, and P. Zhang. Hardware design experiences in zebranet. In *Proceedings of the* 2^{nd} *International Conference on Embedded Networked Systems*, pages 227–238, (2004).

[28] Y. Ma, M. Richards, M. Ghanem, Y. Guo, and J. Hassard. Air pollution monitoring and mining based on sensor grid in London. *Sensors*, 8(6):pp. 3601–3623, (2008).

[29] K. M. Martin. The combinatorics of cryptographic key establishment. *Surveys in Combinatorics*, 346 of London Mathematical Society Lecture Notes Series:pp. 223–273, (2007).

[30] K. M. Martin and M. B. Paterson. An application-oriented framework for wireless

sensor network key establishment. *Electronic Notes in Theoretical Computer Science*, 192:pp. 31–41, (2008).

[31] J. Meier. *Groups, Graphs and Trees: An Introduction to the Geometry of Infinite Groups*. Cambridge University Press, (2008).

[32] A. Panoui. *Wide-Sense Fingerprinting Codes and Honeycomb Arrays*. PhD thesis, Royal Holloway, University of London, (2012).

[33] I. Reiman. Über ein problem von K. Zarankiewicz. *Acta Mathematica Academiae Scientiarum Hungarica*, 9(3-4):pp. 269–273, (1958).

[34] J. S. D. Robinson. *A Course in the Theory of Groups*. Springer, 2nd edition, (1995).

[35] B. Schmidt and M. Tan. Construction of relative difference sets and Hadamard group. *Designs, Codes and Cryptography*, 73(1):pp. 105–119, (2014).

[36] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, (1938).

[37] Robert et al. Szewczyk. An analysis of a large scale habitat monitoring application. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pages 214–226, (2004).

[38] D. Wagner and R. Wattenhofer, editors. *Algorithms for Sensor and Ad Hoc Networks*. Springer, Berlin, (2007).

[39] Q. Xiang. Recent progress in algebraic design theory. *Finite Fields and Their Applications*, 11(3):pp. 622–653, (2005).