Algebraic and Geometric Problems for Non-Volatile Memory

Sarit Buzaglo

Algebraic and Geometric Problems for Non-Volatile Memory

Research Thesis

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

Sarit Buzaglo

Submitted to the Senate of
the Technion — Israel Institute of Technology
Sivan 5775 Haifa June 2014

The research thesis was done under the supervision of Professor Tuvi Etzion and Professor Eitan Yaakobi in the Computer Science Department.

I would like to thank my advisor, mentor, and role model, Professor Tuvi Etzion, for his caring guidance throughout my PhD studies. Tuvi taught me how to explore a research problem from different perspectives, to exploit the full potential of the research, to be patient and to never give up.

I would also like to thank my co-advisor, Professor Eitan Yaakobi, for guiding me throughout the last two years of my PhD studies. Eitan introduced me to new research problems and methods and has always been willing to go above and beyond to help me with any academic matter.

Finally, I would like to thank my family who has always believed in me and to dedicate this PhD thesis to my pride and joy, my son Yali, and to my father, who I hope to make proud.

The generous financial support of the Technion and the Jacobs family is gratefully acknowledged.

Publication List

- S. Buzaglo and T. Etzion, "Tilings with n-dimensional chairs and their applications to asymmetric codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 3, pp. 1573–1582, March 2013.

- S. Buzaglo and T. Etzion, "Tilings by $(0.5, n)$-crosses and perfect codes," *SIAM Journal on Discrete Mathematics,* vol. 27, no. 2, pp. 1067-1081, June 2013.

- S. Buzaglo and T. Etzion, "Perfect permutation codes with the Kendall's τ-metric," *Proc. of IEEE Int. Symp. on Inform. Theory,* pp. 2391–2395, Honolulu, Hawaii, 2014.

- S. Buzaglo and E. Yaakobi, "Constrained codes for rank modulation," *Proc. of IEEE Int. Symp. on Inform. Theory,* pp. 2396–2400, Honolulu, Hawaii, 2014.

- S. Buzaglo, E. Yaakobi, T. Etzion, and J. Bruck, "Error-correcting codes for multipermutations," *Proc. of IEEE Int. Symp. on Inform. Theory,* pp. 724–728, Istanbul, Turkey, July 2013.

- S. Buzaglo, E. Yaakobi, T. Etzion, and J. Bruck, "Systematic codes for rank modulation," *Proc. of IEEE Int. Symp. on Inform. Theory,* pp. 2386–2390, Honolulu, Hawaii, 2014.

Contents

List of Figures

List of Tables

Abstract

Flash memory is one of the most important types of non-volatile memory (NVM) in use today. The high interest and many applications of such memories increase the importance of this research and lead to a wide range of stimulating problems. Flash memory cells are electrically programable to one of q discrete states and therefore, can store $\log_2 q$ bits. Reducing a cell state into a lower state requires the erasure of the whole block to which the cell belongs. This operation is very costly and should be avoided if possible. To decrease the probability of over-shooting errors, charge is injected into a cell over several iterations, which results in a slow programming. This PhD research focus on two coding frameworks for flash memory: the *asymmetric limited magnitude error model* and the *rank modulation scheme*.

The asymmetric limited magnitude error model addresses the inherit asymmetric behavior of common error types in flash memory, under the reasonable assumption that errors are not likely to exceed a certain limit. My research in this context is restricted to the study of perfect error-correcting codes. Using two concepts which are equivalent to perfect linear codes, namely, lattice tiling and group splitting, constructions of perfect error-correcting codes for the asymmetric limited magnitude error model are presented. It is also proved that perfect linear error-correcting codes for this model do no exist for infinitely many parameters.

In many error models, error-correcting codes can be viewed as packings of the n-dimensional Euclidian space with a certain shape. If the code is perfect then the corresponding packing becomes a tiling, which is a partition of the space into translations of the shape. The asymmetric limited magnitude error model is one example of such model. Another important example is the binary symmetric channel for which error-correcting codes can be viewed as packing of the n -dimensional Euclidian space with a shape called the n-dimensional cross. The exact values of n for which a tiling with the n-dimensional cross with arms of length half are presented along with constructions of such tilings that are based on perfect coded for the binary and ternary symmetric channels.

Rank modulation is a coding scheme that was designed to improve the efficiency of programming a flash memory cell. Under this setup, data is encoded into permutations which are derived by the relative charge levels of the cells, rather than by their absolute levels. In this thesis the rank modulation scheme is studied for three fundamental concepts in coding theory; perfect codes, systematic codes, and constrained codes. The main results in this context include the nonexistence of some perfect single-error-correcting codes, construction of systematic codes, and capacity computations of codes under certain constraints.

Abbreviations and Notations

$\mathbb{Z}$	—	The set of integers
$\mathbb{R}$	—	The set of real numbers
$\mathbf{e}_r$	—	The rth unit vector.
$\mathbf{0}$	—	The all-zero vector (the origin).
$\mathbf{1}$	—	The all-one vector.
$\mathcal{A}^n$	—	The Cartesian product of the set $\mathcal{A}$, $\mathcal{A}^n \overset{\text{def}}{=} \{(a_1, a_2, \ldots, a_n) \ : \ a_i \in \mathcal{A}, \text{ for all } 1 \leq i \leq n\}$
$\mathbf{u} + \mathcal{S}$	—	The translation of $\mathcal{S} \subseteq \mathbb{R}^n$ by a vector $\mathbf{u} \in \mathbb{R}^n$, $\mathbf{u} + \mathcal{S} \overset{\text{def}}{=} \{\mathbf{u} + \mathbf{x} \ : \ \mathbf{x} \in \mathcal{S}\}$.
$\alpha\mathcal{S}$	—	The multiplication of $\mathcal{S} \subseteq \mathbb{R}^n$ by a scalar $\alpha \in \mathbb{R}^n$, $\alpha\mathcal{S} \overset{\text{def}}{=} \{\alpha \cdot \mathbf{x} \ : \ \mathbf{x} \in \mathcal{S}\}$.
$\mathcal{S}_1 + \mathcal{S}_2$	—	The addition of $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathbb{R}^n$, $\mathcal{S}_1 + \mathcal{S}_2 \overset{\text{def}}{=} \{\mathbf{x} + \mathbf{y} \ : \ \mathbf{x} \in \mathcal{S}_1, \ \mathbf{y} \in \mathcal{S}_2\}$.
$[n]$	—	The set $\{1, 2, \ldots, n\}$.
$[a, b]$	—	The set $\{a, a+1, \ldots, b\}$, $a, b \in \mathbb{Z}$, $a \leq b$.
$\mathcal{M}$	—	A multiset.
S_n	—	The set of all permutations on $[n]$.
$S([a, b])$	—	The set of all permutations on $[a, b]$.
$S(\mathcal{M})$	—	The set of all multipermutations on the multiset $\mathcal{M}$.
G_n	—	The graphic representation of S_n with the Kendall's τ-metric.
$G(\mathcal{M})$	—	The graphic representation of $S(\mathcal{M})$ with the Kendall's τ-metric.
G_n^c	—	The graphic representation of S_n with the cyclic Kendall's τ-metric.
ε	—	The identity permutation.
$\pi \circ \sigma$	—	The multiplication of $\sigma \in S_n$ and $\pi \in S_n$. $\pi \circ \sigma(i) \overset{\text{def}}{=} \sigma(\pi(i))$, for all $i \in [n]$.
$\sigma(\mathcal{S})$	—	For $\sigma \in S_n$, $\mathcal{S} \subseteq \mathbb{R}^n$,

$\sigma(\mathcal{S})\overset{\text{def}}{=}\{(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})\ :\ (x_1,x_2,\ldots,x_n)\in\mathcal{S}\}$.

$\mathcal{P}$ — A packing.

$\mathcal{T}$ — A tiling.

$\mathbb{P}$ — A set of points such that $\{\mathbf{x}+\mathcal{S}\ :\ \mathbf{x}\in\mathbb{P}\}$ is a packing with $\mathcal{S}$. Also called a packing.

$\mathbb{T}$ — A set of points such that $\{\mathbf{x}+\mathcal{S}\ :\ \mathbf{x}\in\mathbb{T}\}$ is a tiling with $\mathcal{S}$. Also called a tiling.

Λ — A lattice.

$V(\Lambda)$ — The volume of the lattice Λ.

$\mathbf{G}(\Lambda)$ — The generator matrix of the lattice Λ.

$C(\mathbf{x})$ — The n-dimensionl unit cube centered at $\mathbf{x}\in\mathbb{R}^n$,
$C(\mathbf{x})\overset{\text{def}}{=}\{(y_1,y_2,\ldots,y_n)\in\mathbb{R}^n\ :\ |x_i-y_i|\leq 0.5,\ 1\leq i\leq n\}$.

$\mathcal{C}$ — A code.

$E(\mathcal{C})$ — The expanded code of $\mathcal{C}$.

$d_H(\mathbf{x},\mathbf{y})$ — The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$.

$d_M(\mathbf{x},\mathbf{y})$ — The Manhattan distance between $\mathbf{x}$ and $\mathbf{y}$.

$d_L(\mathbf{x},\mathbf{y})$ — The Lee distance between $\mathbf{x}$ and $\mathbf{y}$.

$d_C(\mathbf{x},\mathbf{y})$ — The cross distance between $\mathbf{x}$ and $\mathbf{y}$.

$d_K(\sigma,\pi)$ — The Kendall's τ-distance between the permutations σ and π.

$d_\kappa(\sigma,\pi)$ — The cyclic Kendall's τ-distance between the permutations σ and π.

$d_I(\sigma,\pi)$ — The inversion distance between the permutations σ and π.

$w_H(\mathbf{x})$ — The Hamming weight of $\mathbf{x}$.

$||\mathbf{x}||$ — The Manhattan weight of $\mathbf{x}$.

$w_C(\mathbf{x})$ — The cross weight of $\mathbf{x}$.

$w_K(\sigma)$ — The Kendall's τ- weight of the permutations σ.

$w_\kappa(\sigma)$ — The cyclic Kendall's τ-weight of the permutations σ.

$d_H(\mathcal{C})$ — The minimum Hamming distance between of the code $\mathcal{C}$.

$d_C(\mathcal{C})$ — The minimum cross distance of the code $\mathcal{C}$.

Υ_n — The $(0.5,n)$-cross scaled by two.

$\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ — The n-dimensional chair for $\boldsymbol{\ell},\boldsymbol{k}\in\mathbb{R}^n$.

$\mathbb{S}_K(n,t,\sigma)$ — The Kendall's τ-sphere of radius t centered at $\sigma\in S_n$.

$\mathbb{S}_K(n,t)$ — The Kendall's τ-sphere of radius t centered at the identity permutation $\varepsilon\in S_n$.

$\mathbb{S}_I(n,t,\sigma)$ — The inversion sphere of radius t centered at $\sigma\in S_n$.

$s_I(n,t)$ — The size of $\mathbb{S}_I(n,t,\sigma)$.

$A_{n,k}$ — The set of all permutations in S_n that satisfied the

		two-neighbor k-constraint.
$B_{n,k}$	—	The set of all permutations in S_n that satisfied the asymmetric two-neighbor k-constraint.
$\mathbb{S}_I(A_{k,n},t,\sigma)$	—	The set $A_{n,k} \cup \mathbb{S}_I(n,t,\sigma)$.
H_n	—	The set $[n]^n$.
$\mathbb{S}_M(S,t,\sigma)$	—	The set $\{\mathbf{y} \in S \ : \ d_M(\mathbf{y},\mathbf{x}) \leq t\}$, for $S \subset H_n$.
$C(\epsilon)$	—	The capacity of two-neighbor k-constrained codes, where $k = \Theta(n^{\epsilon})$.
$\tilde{C}(\epsilon)$	—	The capacity of asymmetric two-neighbor k-constrained codes, where $k = \Theta(n^{\epsilon})$.
$C(\epsilon,\delta)$	—	The capacity of two-neighbor k-constrained t-error-correcting codes, where $k = \Theta(n^{\epsilon})$ and $t = \Theta(n^{\delta})$.
$\tilde{C}(\epsilon,\delta)$	—	The capacity of asymmetric two-neighbor k-constrained t-error-correcting codes, where $k = \Theta(n^{\epsilon})$ and $t = \Theta(n^{\delta})$.

Introduction

Flash memory is a nonvolatile memory that is both electrically programmable and electrically erasable. Its reliability, high storage density, and relatively low cost have made it a dominant nonvolatile memory technology. In the standard flash technology, every flash cell has q discrete levels and therefore can store $\log_2 q$ bits. The most conspicuous property of flash storage is its inherent asymmetry between cell programming and cell erasing. While injecting charge to a single cell is a fast and simple operation, reducing the charge level of a single cell requires the erasure and reprogramming of a large block of cells. Thus, a single-cell erase operation requires the cumbersome process of copying an entire block to a temporary location, erasing it, and then programming all the cells in the block. As a consequence, flash cells programming is relatively costly in time and energy, since in order to avoid over-shooting errors, cells should essentially injected with their exact designated charge level. The asymmetry between programming and erasing of flash memory cells, causes significant error sources to change cell levels in one dominant direction. Moreover, all reported common flash error mechanisms induce errors whose magnitudes are small and independent of the alphabet size, that may be significantly larger than the typical error magnitude. In this PhD research two coding frameworks for flash memory are studied: the *asymmetric limited magnitude error model* and the *rank modulation scheme*.

The asymmetric limited magnitude error model addresses the asymmetric nature of common errors in multi level cell flash memory. Errors in this model are in one direction and are not likely to exceed a certain limit. This means that a cell in level i can be raised by an error to level j, such that $i < j \leq q-1$ and $j - i \leq \ell \leq q-1$, where ℓ is the error limited-magnitude. Asymmetric error-correcting codes with limited-magnitude were proposed in [2] and were first considered for nonvolatile memories in [9, 10]. Recently, several other papers have considered these codes, e.g. [22, 23, 48, 104].

The rank modulation scheme has been proposed to improve programming efficiency in flash memory [43]. Codes in this model are subsets of S_n, the set of all permutations on n elements, where each permutation corresponds to a ranking of n cells' levels. Permutation codes were mainly studied in this context using two metrics, the infinity metric and the Kendall's τ-metric. Codes in S_n under the infinity metric were considered in [49, 77, 92, 94]. The Kendall's τ-distance between two permutations $\sigma, \pi \in S_n$ is the minimum number of adjacent transpositions needed to change σ into π, where an adjacent transposition is the exchange of two adjacent elements in a permutation. Under the Kendall's τ-metric, codes in S_n with minimum distance d should correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors that are caused by charge leakage and read disturbance. A comprehensive work on error-correcting codes in S_n using the Kendall's τ-metric [46], is given in [44]. In that paper a construction of single-error-correcting codes using codes in the Lee metric, is also presented. This method was generalized in [5] for the construction of t-error-correcting codes that are of optimal size, up to a constant factor, where t is fixed. In [108, 109] systematic-error-correcting codes for permutations were proposed and in [73] the capacity of permutation codes under a certain constraint was studied.

This PhD dissertation comprises of two parts. The first part deals with the concept of tiling of the n-dimensional Euclidian space with a certain shape. Such tilings are studied for two shapes, the $(0.5, n)$-*cross* and the *n-dimensional chair*. Tilings with the n-dimensional chair form error-correcting codes for the asymmetric limited magnitude error model. The second parts is devoted to the study of error-correcting codes for permutations using the Kendall's τ-metric.

Error-correcting codes and packing and tiling of the n-dimensional Euclidian space with a certain shape are closely connected concepts. Therefore, packing and tiling with a certain shape are two concept that attract a substantial interest from coding theory researchers. A tiling of the n-dimensional Euclidian space with a shape $\mathcal{S}$ is a partition of the space into translations of $\mathcal{S}$. Basic definitions for tiling and packing are given in Chapter 1, along with a discussion on the connection between these concepts and error-correcting codes. Two of the most studied shapes in this context are the semicross and the cross. A (k, n)-*semicross* is an n-dimensional shape whose center is an n-dimensional unit cube from which n *arms* consisting of k n-dimensional unit cubes are spanned in the n positive directions. A (k, n)-*cross* is an n-dimensional shape whose center is an n-dimensional unit cube from which $2n$ *arms* consisting of k n-dimensional unit cubes are spanned in the n directions (one for the positive and one for the negative). Examples of a $(2, 3)$-cross and a $(2, 3)$-semicross are given in Figure 1. Packing and tiling with semicrosses and crosses is a well studied topic (see [86, 88] and references therein). The high interest in packing and tiling with semicrosses and crosses lies in the fact that such packing and tiling correspond to error-correcting codes with the Hamming metric, which are codes that correct symmetric errors [58].

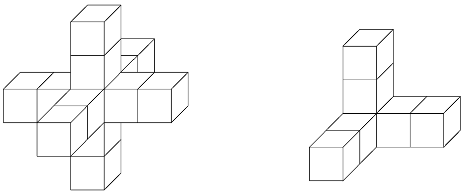

Figure 1: A $(2,3)$-cross and a $(2,3)$-semicross.

Tiling with the $(0.5,n)$-cross are studied in Chapter 2. The $(0.5,n)$-cross consists of one complete (non-fractional) unit cube and $2n$ halves unit cubes. Usually, it is more convenient to handle tiling with complete unit cubes. Hence, after scaling the $(0.5,n)$-cross by two a new shape is obtained. This shape comprises of an n-dimensional unit cube of length 2, which consists of 2^n n-dimensional unit cubes, and to each of which $n-1$-dimensional faces attached are n-dimensional unit cubes. Example of the $(0.5,3)$-cross and its scaling by two is given in Figure 2.1. In addition to the high interest on crosses mentioned above, another motivation for the study of tiling with $(0.5,n)$-cross was pointed out by Italo J. Dejter [18]. Such a tiling is equivalent to a perfect dominating set in $\mathbb{Z}^n$, where each of its connectivity components are n-dimensional unit cubes of length 2. This problem was considered by several authors, e.g. [4, 100] and references therein. The main result of Chapter 2, solves one of the main open problems on this topic. This result states that an integer tiling of the n-dimensional Euclidian space with the $(0.5,n)$-cross, scaled by 2, exists if and only if $n=2^t-1$ or $n=3^t-1$, where t is a positive integer.

In Chapter 3, tilings with the n-dimensional chair are studied. An n-dimensional chair is an n-dimensional box from which a smaller n-dimensional box is removed from one of its corners (example of a three dimensional chair is given in Figure 3.1). The study of tiling with the n-dimensional chair is motivated by the asymmetric limited magnitude error model, since such tilings correspond to codes that correct up to $n-1$ asymmetric limited magnitude errors. These tilings have another application for constructing WOM codes with multiple writing. Only lattice tilings are considered in the context of the n-dimensional chair. An equivalent way to present a lattice tiling is given. This method is called a generalized splitting and it generalizes the concepts of splitting defined in [82]; and the concept of $B_h[\ell]$

sequences defined and used for construction of codes correcting asymmetric errors with limited-magnitude in [48]. Two constructions of tilings based on generalized splitting are presented. A lattice tiling is derived based on a construction of a splitting sequence. Mihalis Kolountzakis and James H. Schmerl [53] pointed on [87], where this lattice tiling was first proposed, and further discussed in [52, 75].

In the second part of this dissertation, codes for permutations using the Kendall's metric are discussed. Recently, to improve the number of rewrites, the rank modulation scheme was extended such that multiple cells can share the same ranking [24, 25]. Thus, the cells no longer determine permutations but rather multipermutations, which are also known as permutations with repetitions. Error-correcting codes for multipermutations subject to the Kendall's τ-metric were presented in [74] and also studied in [7]. Multipermutations are used to construct codes in Chapters 6 and 7. Basic definitions and properties of permutations, multipermutations, and Kendall's τ-metric are presented in Chapter 4.

In Chapter 5 the concepts of perfect codes and diameter perfect codes for permutations are studied. Perfect codes for permutations, using the Kendall's τ-metric are shortly discussed in [108]. In this paper systematic single-error codes in S_n of size $(n-2)!$ are constructed. These codes are of optimal size, assuming that a perfect single-error-correcting code does not exist. However, the nonexistence of perfect single-error-correcting codes is proved only for $n = 4$. The first section of this chapter is devoted to perfect single-error-correcting codes in S_n, using the Kendall's τ-metric. Perfect codes is one of the most fascinating topics in coding theory. A perfect t-error-correcting code with the Kendall's τ-metric is a code $\mathcal{C} \subseteq S_n$ such that every permutation in S_n is at Kendall's τ-distance at most t from exactly one codeword of $\mathcal{C}$. In Section 5.1 it is proved that perfect single-error-correcting codes in S_n, where $n > 4$ is a prime or $4 \leq n \leq 10$, do not exist. It is also proved that if such a code exists for n which is not a prime then the code should have some uniform structure. In Section 5.2 diameter perfect codes in S_n, using the Kendall's τ-metric, are studied. As a result, known upper bounds on the size of a code in S_n with even minimum Kendall's τ-distance are improved. A natural variation of the Kendall's τ-distance is the cyclic Kendall's τ-distance. In Section 5.3 perfect single-error-correcting code in S_5 and single-error-correcting code, using the cyclic Kendall's τ-distance, are presented. These codes are also single-error-correcting codes, using the Kendall's τ-distance, and they are larger than the known ones in S_5 and S_7. This cyclic Kendall's τ-metric was studied in [42], where an algorithm to compute the distance between two permutations in S_n with running time $O(n^2)$ was given. A simpler and more explicit algorithm to compute the cyclic Kendall's τ-distance between two permutations in S_n with running time $O(n^2)$ is presented in Section 5.3 . The cyclic Kendall's τ-distance also has applications in Biology, as was suggested in [31], since it capture the genetic difference between some bacteria and viruses, that usually have a circular genome. A lower bound on the maximum cyclic Kendall's τ-distance between two permutations in S_n was also given in [31], while in [106] it was shown that this lower bound is tight.

Chapter 6 deals with systematic error-correcting codes for permutations. As mentioned above, this concept for permutations was proposed in [108, 109]. A systematic code $\mathcal{C}$ for permutations in S_n is a code consists of $k!$ codewords. Each permutation of S_k (on a given set of specific k symbols) is a sub-permutation (subsequence) of exactly one codeword of $\mathcal{C}$. In this PhD research some of the results in [108, 109] are improved. A construction of systematic error-correcting codes for permutations is presented in Section 6.2. This construction is based on two ingredients. The first is a partition of S_k into t-error-correcting codes. The second is a code $\mathcal{C}_r$ for multipermutations with minimum Kendall's τ-distance $2t$, whose size is the number of parts in the partition. Each code from the partition of S_k is substituted into a different codeword of $\mathcal{C}_r$. It is proved that for large enough k, this construction uses less redundancy symbols than the number of redundancy symbols in the codes of the known constructions. In particular, for a given t and for sufficiently large k we can obtain $r = t+1$. This construction is generalized in Section 6.3 to systematic codes for multipermutations.

Constrained codes for permutations are discussed in Chapter 7. This work was inspired from a recent research by Sala and Dolecek [73, 72] who studied a certain constraint that is motivated by the inter-cell interference (ICI) in flash memory. The ICI is a phenomena in which the level of a cell, called a *victim cell* might increase, if its neighbor cells are programmed to significantly higher levels [54]. The ICI is caused by the parasitic capacitance between neighboring cells and in particular, multilevel cell programming is severely influenced by this effect. In the model studied in [73], the authors explored the *single-neighbor* constraint in which the differences between charge levels of adjacent cells are upper bounded. This constraint prevents the scenario in which a high-level cell affects its low-level neighbor cell. In this work, two constraints that captures the ICI phenomenon are considered, the *two-neighbor* constraint and the *asymmetric two-neighbor* constraint. The former constraint was proposed in [72]. A permutation satisfies this constraint if the difference between the level of a cell and the level of one of its neighbors is bounded by some prescribed value k. In the asymmetric version, the differences between charge levels are constrained only for sequences of the form high-low-high. This constraint is motivated by the fact that the ICI in flash memories mainly affects sequences of the form high-low-high and not the other ones. The capacities of these two constraints are computed in Sections 7.1 and 7.2. The constraints studied in this work as well as in [73] are effective in reducing the errors caused by the ICI. However, random errors may still happen. In Section 7.3 error-correcting codes with the Kendall's τ-distance that, yet consist of only permutations that satisfy the constraints are studied.

Part I

Tiling of the n-Dimensional Euclidian Space and its Applications

Chapter 1

Preliminaries: Tiling, Packing, and Error-Correcting Codes

Definitions and properties of tiling and packing are given in this chapter, and the connection between tiling and packing and error-correcting codes is explained. The basic concepts presented in this chapter are widely used throughout this part of the dissertation.

For a set $\mathcal{S} \in \mathbb{R}^n$ and a vector $\mathbf{u} \in \mathbb{R}^n$ the *translation* of $\mathcal{S}$ by $\mathbf{u}$ is $\mathbf{u}+\mathcal{S} \overset{\text{def}}{=} \{\mathbf{u}+\mathbf{x} \ : \ \mathbf{x} \in \mathcal{S}\}$. The *multiplication* of $\mathcal{S}$ by a scalar $\alpha \in \mathbb{R}$ is defined by $\alpha\mathcal{S} \overset{\text{def}}{=} \{\alpha \cdot \mathbf{x} \ : \ \mathbf{x} \in \mathcal{S}\}$. For two sets $\mathcal{S}_1 \subseteq \mathbb{R}^n$ and $\mathcal{S}_2 \subseteq \mathbb{R}^n$ the *set addition* $\mathcal{S}_1+\mathcal{S}_2$ is defined by $\mathcal{S}_1+\mathcal{S}_2 \overset{\text{def}}{=} \{\mathbf{x}+\mathbf{y} \ : \ \mathbf{x} \in \mathcal{S}_1, \ \mathbf{y} \in \mathcal{S}_2\}$.

Let $\mathcal{S}$ be an n-dimensional shape in the n-dimensional Euclidian space ($\mathbb{R}^n$). We say that two translations of $\mathcal{S}$, $\mathcal{S}_1$ and $\mathcal{S}_2$, are *disjoint* if their intersection is contained in an $(n-1)$-dimensional space.

Definition 1.1 *A* packing $\mathcal{P}$ *of the n-dimensional Euclidian space with the shape $\mathcal{S}$ is a set of disjoint translations of $\mathcal{S}$.*

Definition 1.2 *A* tiling $\mathcal{T}$ *of the n-dimensional Euclidian space with the shape $\mathcal{S}$ is a packing of the n-dimensional Euclidian space, $\mathbb{R}^n$, with the shape $\mathcal{S}$ such that each point $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ is contained in at least one translation of $\mathcal{S}$.*

For a given shape $\mathcal{S}$ we choose a fixed point which will be called the *balanced point* of the shape. In any other translation of $\mathcal{S}$ the balanced point will be chosen in the same relative position. The set of balanced points in the translations of $\mathcal{S}$ contained in the packing $\mathcal{P}$ defines the packing. Hence, a packing $\mathcal{P}$ will be defined by a set of points $\mathbb{P} \subset \mathbb{R}^n$ and a shape $\mathcal{S}$. A point $\mathbf{x}$ belongs to $\mathbb{P}$ if and only if the translation $\mathbf{x}+\mathcal{S}$ belongs to $\mathcal{P}$. Henceforth, $\mathbb{P}$ will be called a packing if the shape $\mathcal{S}$ is known. In particular, for a tiling $\mathcal{T}$ with a shape $\mathcal{S}$, the set $\mathbb{T} \overset{\text{def}}{=} \{\mathbf{x} \in \mathbb{R}^n ~:~ \mathbf{x}+\mathcal{S} \in \mathcal{T}\}$ will also be called a tiling with the shape $\mathcal{S}$.

Lemma 1.3 *If $\mathbb{P}$ is a packing (a tiling) with a shape $\mathcal{S}$ and $\mathbf{u} \in \mathbb{R}^n$ then $\mathbf{u}+\mathbb{P}$ is also a packing (a tiling) with $\mathcal{S}$.*

For a set $\mathcal{S} \subseteq \mathbb{R}^n$ and a permutation $\sigma = [\sigma(1), \sigma(2), \ldots, \sigma(n)]$ of $\{1, 2, \ldots, n\}$, let $\sigma(\mathcal{S}) \overset{\text{def}}{=} \{(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) ~:~ (x_1, x_2, \ldots, x_n) \in \mathcal{S}\}$.

Lemma 1.4 *If $\mathbb{P}$ is a packing (a tiling) with an n-dimensional shape $\mathcal{S}$ and σ is a permutation of $[n]$ then $\sigma(\mathbb{P})$ is a packing (a tiling) with the n-dimensional shape $\sigma(\mathcal{S})$.*

Definition 1.5 *A packing (a tiling) $\mathbb{P}$ with a shape $\mathcal{S}$ is called an* integer packing *(an integer tiling), if $\mathbb{P} \subseteq \mathbb{Z}^n$. An integer packing (tiling) is also called a* $\mathbb{Z}$-packing *(a* $\mathbb{Z}$-tiling*).*

Definition 1.6 *For $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, an n-dimensional unit cube centered at $\mathbf{x}$, $C(\mathbf{x})$, is defined as the set $C(\mathbf{x}) \overset{\text{def}}{=} \{(y_1, y_2, \ldots, y_n) \in \mathbb{R}^n ~:~ |x_i - y_i| \leq 0.5,~ 1 \leq i \leq n\}$.*

Definition 1.7 *An n-dimensional shape $\mathcal{S}$ is a* discrete shape *if $\mathcal{S}$ is a union of n-dimensional unit cubes, whose centers are in $\mathbb{Z}^n$.*

A discrete n-dimensional shape $\mathcal{S}$ can be identified by a set of points in $\mathbb{Z}^n$. Conversely, a set of points in $\mathbb{Z}^n$ defines a discrete shape. By abuse of notation, the same notation will be used for the discrete shape and the set of points in $\mathbb{Z}^n$ that defines the shape, where the meaning should be clear from the context. If $\mathbb{T}$ is an integer tiling with a discrete shape $\mathcal{S}$, then each point of $\mathbb{Z}^n$ is contained in exactly one translation of $\mathcal{S}$ by an element of $\mathbb{T}$. By abuse of language, $\mathbb{T}$ is called a tiling of $\mathbb{Z}^n$ with the set $\mathcal{S} \subseteq \mathbb{Z}^n$. Similarly, if $\mathbb{P}$ is an integer packing with $\mathcal{S}$, then $\mathbb{P}$ is called a packing of $\mathbb{Z}^n$ with the set $\mathcal{S} \subseteq \mathbb{Z}^n$.

The vector $(x_1, x_2, \ldots, x_n)$ is called the *r-th unit vector* and will be denoted by $\mathbf{e}_r$ if $x_r = 1$ and for all $i \neq r$, $x_i = 0$. The origin $(0, 0, \ldots, 0) \in \mathbb{R}^n$ is denoted by $\mathbf{0}$. The all-one vector $(1, 1, \ldots, 1) \in \mathbb{R}^n$ is denoted by $\mathbf{1}$.

Definition 1.8 *A set $\mathcal{A}$ is called* periodic *with period p if $\mathbf{x} \in \mathcal{A}$ implies that $\mathbf{x} + \alpha \cdot p \cdot e_i \in \mathcal{A}$, for all $\alpha \in \mathbb{Z}$ and $1 \leq i \leq n$. A packing (a tiling) $\mathbb{P}$ with the shape $\mathcal{S}$ is a periodic packing (a periodic tiling) if it is a periodic set.*

Lemma 1.9 *A tiling $\mathbb{T}$ is periodic with period p if and only if $\mathbf{x} \in \mathbb{T}$ implies that $\mathbf{x} + p \cdot \mathbf{e}_i \in \mathbb{T}$ for all i, $1 \leq i \leq n$.*

Definition 1.10 *A* lattice Λ *is a discrete, additive subgroup of the real n-space $\mathbb{R}^n$,*

$$\Lambda \overset{\text{def}}{=} \{u_1\mathbf{v}_1 + u_2\mathbf{v}_2 + \cdots + u_n\mathbf{v}_n \ : \ u_1, u_2, \cdots, u_n \in \mathbb{Z}\},$$

where $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a set of linearly independent vectors in $\mathbb{R}^n$, i.e. the lattice has rank n. The set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is called a basis *for Λ, and the $n \times n$ matrix*

$$\mathbf{G}(\Lambda) \overset{\text{def}}{=} \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{bmatrix}$$

having these vectors as its rows is said to be a generator matrix *for Λ.*

The *volume* of a lattice Λ, denoted by $V(\Lambda)$, is inversely proportional to the number of lattice points per a unit volume. More precisely, $V(\Lambda)$ may be defined as the volume of the *fundamental parallelogram* $\Pi(\Lambda)$, which is given by

$$\Pi(\Lambda) \overset{\text{def}}{=} \{\xi_1\mathbf{v}_1 + \xi_2\mathbf{v}_2 + \cdots + \xi_n\mathbf{v}_n \ : \ 0 \leq \xi_i < 1, \ 1 \leq i \leq n\} \ .$$

There is a simple expression for the volume of Λ, namely, $V(\Lambda) = |\det \mathbf{G}|$.

A lattice Λ is a *lattice tiling* with $\mathcal{S}$ if $\mathbb{T} \overset{\text{def}}{=} \Lambda$ forms a tiling with $\mathcal{S}$. A lattice tiling Λ is an *integer lattice tiling* with if all entries of $\mathbf{G}$ are integers. The following lemma is well known.

Lemma 1.11 *A necessary condition that a lattice Λ defines a lattice packing (tiling) with a shape $\mathcal{S}$ is that $V(\Lambda) \geq |\mathcal{S}|$ ($V(\Lambda) = |\mathcal{S}|$). A sufficient condition that a lattice packing Λ with a shape $\mathcal{S}$ defines a lattice tiling with the shape $\mathcal{S}$ is that $V(\Lambda) = |\mathcal{S}|$.*

A *code* $\mathcal{C}$ of length n over $\mathbb{Z}_q$ (over $\mathbb{Z}$) is a subset of $\mathbb{Z}_q^n$ (of $\mathbb{Z}^n$). The elements of $\mathcal{C}$ are called *codewords*. Let Λ_n be the lattice generated by the basis $\{q \cdot \mathbf{e}_i \ : \ 1 \leq i \leq n\}$. A code $\mathcal{C} \subseteq \mathbb{Z}_q^n$ can be viewed also as a subset of $\mathbb{Z}^n$.

Definition 1.12 *The code $E(\mathcal{C}) = \mathcal{C} + \Lambda_n$ is the* expanded code *of $\mathcal{C}$. If $E(\mathcal{C})$ is a packing (a tiling) of $\mathbb{Z}^n$ with the shape $\mathcal{S}$ then we also call $\mathcal{C}$ a packing (a tiling) of $\mathbb{Z}_q^n$ with the shape $\mathcal{S}$.*

Conversely, a tiling $\mathbb{T} \subseteq \mathbb{Z}^n$ with a period p can be viewed as an expanded code, $E(\mathcal{C})$, of a code $\mathcal{C}$ of length n over $\mathbb{Z}_p$, where $\mathcal{C} = \mathbb{T} \cap \{0, 1, \ldots, p-1\}^n$. If $\mathcal{C}$ is a packing of $\mathbb{Z}_q^n$ with the shape $\mathcal{S}$ then $\mathcal{C}$ is called an *error-correcting code* with $\mathcal{S}$, and $\mathcal{S}$ is called an *error sphere*. The elements of $\mathcal{S}$ are called *error-vectors*. If $\mathcal{C}$ is an error-correcting code with and error sphere $\mathcal{S}$ then for every $\mathbf{y} \in \mathbb{Z}_q^n$ there exists at most one codeword $\mathbf{x} \in \mathcal{C}$ such that $\mathbf{y} \in \mathbf{x}+\mathcal{S}$. Therefore, if $\mathbf{y} = \mathbf{x} + \mathbf{e}$, where $\mathbf{x} \in \mathcal{C}$ and $\mathbf{e} \in \mathcal{S}$, then $\mathbf{x}$ can be uniquely determined from $\mathbf{y}$. If $\mathcal{C}$ is a tiling of $\mathbb{Z}_q^n$ with the shape $\mathcal{S}$ then $\mathcal{C}$ is called a *perfect* error-correcting code for $\mathcal{S}$. In that case, for every $\mathbf{y} \in \mathbb{Z}_q^n$ there exists exactly one codeword $\mathbf{x} \in \mathcal{C}$ such that $\mathbf{y} - \mathbf{x} \in \mathcal{S}$.

One important example are error-correcting codes with the *Hamming* metric. These codes are also known as error-correcting codes for the *symmetric channel.*

Definition 1.13 *For every two given words $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$ the* Hamming distance *$d_H(\mathbf{x}, \mathbf{y})$ is the number of positions in which $\mathbf{x}$ and $\mathbf{y}$ differ, i.e.*

$$d_H(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} |\{i \ : \ x_i \neq y_i, \ 1 \leq i \leq n\}| \ .$$

The Hamming weight *of $\mathbf{x} \in \mathbb{Z}_q^n$, $w_H(\mathbf{x})$, is the Hamming distance of $\mathbf{x}$ and $\mathbf{0}$.*

A code $\mathcal{C}$ is a t-error-correcting code with the Hamming metric if for every $\mathbf{y} \in \mathbb{Z}_q^n$ there exists at most one codeword $\mathbf{x} \in \mathcal{C}$ such that $d_H(\mathbf{x}, \mathbf{y}) \leq t$. Let $\mathcal{S} = \{\mathbf{y} \in \mathbb{Z}^n \ : \ w_H(\mathbf{y}) \leq t\}$. The shape $\mathcal{S}$ is called the *Hamming sphere* of radius t and $\mathcal{C}$ is a t-error-correcting code with the Hamming metric if and only if $\mathcal{C}$ is a packing of $\mathbb{Z}_q^n$ with the shape $\mathcal{S}$. A perfect t-error-correcting code with the Hamming metric over $\mathbb{Z}_q^n$ is equivalent to a tiling of $\mathbb{Z}_q^n$ with the shape $\mathcal{S}$. In particular, a perfect single-error-correcting code with the Hamming metric is equivalent to a tiling of $\mathbb{Z}_q^n$ with the $((q-1)/2, n)$-cross. For a code $\mathcal{C}$, its *minimum Hamming distance* is the largest integer d for which $d_H(\mathbf{x}, \mathbf{y}) \geq d$, for every two distinct codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. A code $\mathcal{C} \subseteq \mathbb{Z}_q^n$ with minimum Hamming distance d is a t-error-correcting code if and only if $d \geq 2t+1$. If $d \geq 2t+1$ then $\mathcal{C}$ is a perfect t-error-correcting code if for every $\mathbf{y} \in \mathbb{Z}_q^n$ there exists a codeword $\mathbf{x} \in \mathcal{C}$ such that $d_H(\mathbf{y}, \mathbf{x}) \leq t$.

Chapter 2

Tiling with the $(0.5, n)$-Cross

Packing and covering are two fundamental concepts in combinatorics. Tiling is a concept which combines both packing and covering and hence it attracts a substantial interest. Tiling of the Euclidian space with specific shapes is one of the main interest in this respect. The (k, n)-cross and (k, n)-semicross are two shapes that were intensively studied in this context. A (k, n)-*semicross* is an n-dimensional shape whose center is an n-dimensional unit cube from which n *arms* consisting of k n-dimensional unit cubes are spanned in the n positive directions. A (k, n)-*cross* is an n-dimensional shape whose center is an n-dimensional unit cube from which $2n$ *arms* consisting of k n-dimensional unit cubes are spanned in the, ,n directions, one for the positive direction and one for the negative direction (see Figure 1 for example of a $(2, 3)$-cross and a $(2, 3)$-semicross). As mentioned in [88], the origins of the study of the cross and semicross are in several independent sources [36, 45, 82, 95], some of which are pure mathematics and some are connected to coding theory. Semicross and cross are two types of "error spheres" as explained in [35]. Golomb and Welch [36] proved that the $(1, n)$-cross tiles the n-dimensional Euclidian space for all $n \geq 1$. Such a tiling is a perfect code in the Manhattan metric and if the tiling is periodic then it is also a perfect code in the Lee metric. Their work inspired future work (see [27] and references therein) on perfect codes in the Lee (and Manhattan) metric.

As said before, packing and tiling with semicrosses and crosses are well studied topics [14, 30, 36, 38, 39, 57, 82, 83, 85, 89, 90, 91]. The results in these research works include bounds on the size of the arms, constructions for such packings and tilings, parameters for which such tilings cannot exist, lattice and non-lattice tilings, etc. Recently, the topic has gained a new interest since the (k, n)-semicross is the error sphere of the *asymmet-*

ric error model associated with flash memories [10, 48], the most advanced type of storage currently used. Schwartz [76] investigated lattice tilings with generalized crosses and semicrosses in the connection of *unbalanced limited magnitude error model* for multi level flash memories.

Not much is known about tiling of crosses with arms which are not of integer length. Moreover, most tilings considered in the literature are integer lattice tilings. In this chapter the existence of tiling of the n-dimensional Euclidian space with a $(0.5, n)$-cross is studied.

A unit cube centered at $(c_1, c_2, \ldots, c_n) \in \mathbb{R}^n$ is a union of two disjoint half unit cubes in one of the n directions. For the r-th direction one *half unit cube* is defined by the set of points $\{(x_1, x_2, \ldots, x_n) \ : \ 0 \leq x_r - c_r \leq 0.5, \ |x_i - c_i| \leq 0.5, \ 1 \leq i \leq n, \ i \neq r\}$ and a second *half unit cube* is defined by the set of points $\{(x_1, x_2, \ldots, x_n) \ : \ -0.5 \leq x_r - c_r \leq 0, \ |x_i - c_i| \leq 0.5, \ 1 \leq i \leq n, \ i \neq r\}$. A $(0.5, n)$-cross is a unit cube to which two half unit cubes are attached in the r-th direction for each $1 \leq r \leq n$, one in its negative direction and one in its positive direction. It is more convenient to handle shapes with complete unit cubes (discrete shapes) and therefore the $(0.5, n)$-cross is scaled by two to obtain a new shape which will be denoted by Υ_n. Examples of a $(0.5, 3)$-cross and Υ_3 are given in Figure 2.1. The complete unit cube in the $(0.5, n)$-cross is transferred into an n-dimensional cube with sides of length two in Υ_n. This cube in Υ_n will be called the *core* of Υ_n; the core consists of 2^n unit cubes. In the sequel, only integer tilings with Υ_n will be considered. In such an integer tiling Υ_n can be represented by $2^n(n+1)$ points of $\mathbb{Z}^n$ which are the centers of its $2^n(n+1)$ unit cubes. The discussion on the shape Υ_n is restricted only for integer tiling (also known as $\mathbb{Z}$-tiling) which is a tiling in which the centers of the unit cubes are placed on points of $\mathbb{Z}^n$. Such a tiling is proven to exists if and only if $n = 2^t - 1$ or $n = 3^t - 1$, where $t > 0$. The related tiling with a $(0.5, n)$-cross (obtained after scaling by 0.5) will be called a $\frac{1}{2}\mathbb{Z}$-tiling. Analysis of the structure obtained from such a tiling is presented. The tiling which is considered for the $(0.5, n)$-cross is usually not an integer tiling. Moreover, general tilings are considered and not just lattice tilings as done in most literature.

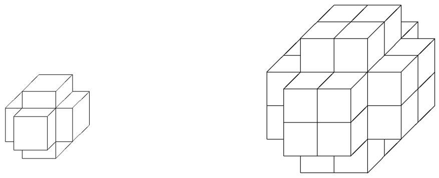

Figure 2.1: A $(0.5, 3)$-cross and an Υ_3.

Dejter [18] has pointed out that a tiling with Υ_n is a perfect dominating set in $\mathbb{Z}^n$. This problem was considered by several authors, e.g. [4, 100] and references therein. The problem that is considered in this chapter is one of the main open problems on this topic.

To handle tilings with the $(0.5, n)$-cross, three distance measures are needed, the well known Hamming distance (see Definition 1.13), the Manhattan distance, and the new defined cross distance.

Definition 2.1 *For every two given points* $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ *the* Manhattan distance $d_M(\mathbf{x}, \mathbf{y})$ *is defined as follows.*

$$d_M(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} \sum_{i=1}^{n} |x_i - y_i| \ .$$

Definition 2.2 *For every two given points* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ *the* cross distance $d_C(\mathbf{x}, \mathbf{y})$ *is defined as follows.*

$$d_C(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} \sum_{i=1}^{n} \max\{0, |y_i - x_i| - 1\}.$$

The *Manhattan weight* and *cross weight* of $\mathbf{x} \in \mathbb{Z}_q^n$ are defined by $w_M(\mathbf{x}) \overset{\text{def}}{=} d_M(\mathbf{x}, \mathbf{0})$ and $w_C(\mathbf{x}) \overset{\text{def}}{=} d_C(\mathbf{x}, \mathbf{0})$, respectively.

While the Hamming distance is an association scheme, the Manhattan distance is only a metric distance and not an association scheme (see [58] for the definition of an association scheme). The cross distance is not a metric, but it will be most important in the discussion on tilings with a $(0.5, n)$-cross.

Let $\mathbb{T}$ be a tiling with Υ_n. It is assumed throughout this chapter that if $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{T}$ then the set $\{(c_1, c_2, \ldots, c_n) \ : \ c_i \in \{x_i - 1, x_i\}, \ 1 \leq i \leq n\}$ is the related core of the translation $\mathbf{x} + \Upsilon_n$. The core of Υ_n is $\{-1, 0\}^n$ and $\Upsilon_n \overset{\text{def}}{=} \{\mathbf{u} \in \mathbb{Z}^n \ : \ d_M(\mathbf{x}, \mathbf{u}) = 1, \ \mathbf{x} \in \{-1, 0\}^n\}$. If $\mathbb{T}$ is a tiling with Υ_n then $0.5\mathbb{T}$ is a tiling with a $(0.5, n)$-cross. Clearly, if for each $(x_1, x_2, \ldots, x_n) \in \mathbb{T}$, x_i is even for all $1 \leq i \leq n$, then also $0.5\mathbb{T}$ is an integer tiling. However, if there exists a point $(x_1, x_2, \ldots, x_n) \in \mathbb{T}$ such that for at least one j we have that x_j is odd then $0.5\mathbb{T}$ is not an integer tiling. To this end, a $\frac{1}{2}\mathbb{Z}$-tiling is defined. A tiling $\mathbb{T}$ is a $\frac{1}{2}\mathbb{Z}$-*tiling* if $\mathbb{T} \subseteq 0.5\mathbb{Z}^n$.

Lemma 2.3 *The tiling* $\mathbb{T}$ *is an integer tiling with* Υ_n *if and only if* $0.5\mathbb{T}$ *is a* $\frac{1}{2}\mathbb{Z}$*-tiling with a* $(0.5, n)$*-cross.*

Given a set $\mathbb{T} \subset \mathbb{Z}^n$, it should be determined whether $\mathbb{T}$ is a tiling with Υ_n. To show that $\mathbb{T}$ is a tiling it is sufficient to prove the following.

($\boldsymbol{\mathcal{P}}$.1) For each point $Y \in \mathbb{Z}^n$ there exists a translation $\mathcal{S}_1$ of Υ_n in the tiling such that $\mathcal{S}_1$ contains Y.

($\boldsymbol{\mathcal{P}}$.2) A point $Y \in \mathbb{Z}^n$ is not contained in more than one translation of Υ_n in the tiling, i.e. for each two translations $\mathcal{S}_1$ and $\mathcal{S}_2$ of Υ_n in the tiling we have $\mathcal{S}_1 \cap \mathcal{S}_2 = \varnothing$.

A set $\mathbb{T} \subset \mathbb{Z}^n$ is a *covering* with Υ_n if it satisfies property **($\boldsymbol{\mathcal{P}}$.1)** and it is a packing with Υ_n if it satisfies property **($\boldsymbol{\mathcal{P}}$.2)**. A tiling is clearly both a covering and a packing.

The following two lemmas are immediate results from the definition of Υ_n.

Lemma 2.4 *If $\mathcal{S}$ is a translation of Υ_n and $\mathbf{x} \in \mathcal{S}$ is not a core point of $\mathcal{S}$ then there exists a core point $\mathbf{y} \in \mathcal{S}$ such that $d_M(\mathbf{x}, \mathbf{y}) = 1$.*

Lemma 2.5 *If $\mathcal{S}_1$ and $\mathcal{S}_2$ are two translations of Υ_n for which $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \varnothing$ then there exists a point $\mathbf{x} \in \mathcal{S}_1 \cap \mathcal{S}_2$ which is not in the core of $\mathcal{S}_1$.*

Corollary 2.6 *If $\mathcal{S}_1$ and $\mathcal{S}_2$ are two translations of Υ_n for which $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \varnothing$ then there exist two core points $\mathbf{x}_1 \in \mathcal{S}_1$ and $\mathbf{x}_2 \in \mathcal{S}_2$ such that $d_M(\mathbf{x}_1, \mathbf{x}_2) \leq 2$.*

Lemma 2.7 *If $\mathcal{S}_1$ and $\mathcal{S}_2$ are two translations of Υ_n for which there exist two core points $\mathbf{x}_1 \in \mathcal{S}_1$ and $\mathbf{x}_2 \in \mathcal{S}_2$ such that $d_M(\mathbf{x}_1, \mathbf{x}_2) \leq 2$, then $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \varnothing$.*

Proof. If $d_M(\mathbf{x}_1, \mathbf{x}_2) \leq 2$ then there exists a point $\mathbf{y} \in \mathbb{Z}^n$ such that $d_M(\mathbf{x}_1, \mathbf{y}) \leq 1$ and $d_M(\mathbf{x}_2, \mathbf{y}) \leq 1$. By definition $\mathbf{y} \in \mathcal{S}_1 \cap \mathcal{S}_2$.

□

Corollary 2.8 *Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two translations of Υ_n. Then $\mathcal{S}_1 \cap \mathcal{S}_2 = \varnothing$ if and only if for every two core points $\mathbf{x}_1 \in \mathcal{S}_1$ and $\mathbf{x}_2 \in \mathcal{S}_2$ we have $d_M(\mathbf{x}_1, \mathbf{x}_2) \geq 3$.*

Theorem 2.9 *Let $\mathcal{S}_1 = \mathbf{x} + \Upsilon_n$ and $\mathcal{S}_2 = \mathbf{y} + \Upsilon_n$, where $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$, be two translations of Υ_n. Then $\mathcal{S}_1 \cap \mathcal{S}_2 = \varnothing$ if and only if $d_C(\mathbf{x}, \mathbf{y}) \geq 3$.*

Proof. Let $\tilde{\mathbf{x}} = (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n)$ and $\tilde{\mathbf{y}} = (\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_n)$ be the centers of mass of $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively. Clearly, $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{y}}$ are in $(0.5, 0.5, \ldots, 0.5) + \mathbb{Z}^n$. The core points of $\mathcal{S}_1$ are $\{(c_1, c_2, \ldots, c_n) \ : \ c_i \in \{\tilde{x}_i - 0.5, \tilde{x}_i + 0.5\}\}$ and the core points of $\mathcal{S}_2$ are $\{(c_1, c_2, \ldots, c_n) \ : \ c_i \in \{\tilde{y}_i - 0.5, \tilde{y}_i + 0.5\}\}$. Let $\mathbf{x}' = (x'_1, x'_2, \ldots, x'_n)$ and $\mathbf{y}' = (y'_1, y'_2, \ldots, y'_n)$ be the two core points of

$\mathcal{S}_1$ and $\mathcal{S}_2$, respectively, defined as follows. If $\tilde{x}_i = \tilde{y}_i$ then $x'_i \overset{\text{def}}{=} \tilde{x}_i + 0.5$ and $y'_i \overset{\text{def}}{=} \tilde{y}_i + 0.5$. If $\tilde{x}_i < \tilde{y}_i$ then $x'_i \overset{\text{def}}{=} \tilde{x}_i + 0.5$ and $y'_i \overset{\text{def}}{=} \tilde{y}_i - 0.5$. If $\tilde{x}_i > \tilde{y}_i$ then $x'_i \overset{\text{def}}{=} \tilde{x}_i - 0.5$ and $y'_i \overset{\text{def}}{=} \tilde{y}_i + 0.5$. Clearly, $d_C(\mathbf{x}, \mathbf{y}) = d_C(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) = d_M(\mathbf{x}', \mathbf{y}')$ and for any two core points $\hat{\mathbf{x}} \in \mathcal{S}_1$ and $\hat{\mathbf{y}} \in \mathcal{S}_2$ we have that $d_M(\hat{\mathbf{x}}, \hat{\mathbf{y}}) \geq d_M(\mathbf{x}', \mathbf{y}')$. Now, by Corollary 2.8 we have that $\mathcal{S}_1 \cap \mathcal{S}_2 = \varnothing$ if and only if $d_C(\mathbf{x}, \mathbf{y}) \geq 3$.

□

Corollary 2.10 *The set $\mathbb{T}$ induces a packing of the n-dimensional Euclidian space with Υ_n if and only if for every two elements $\mathbf{x}, \mathbf{y} \in \mathbb{T}$, we have $d_C(\mathbf{x}, \mathbf{y}) \geq 3$.*

To prove that a set is a tiling with Υ_n it is sufficient to show that it satisfies properties **($\mathcal{P}$.1)** and **($\mathcal{P}$.2)**. For this purpose it is proven that each point of $\mathbb{Z}^n$ is contained (covered) in exactly one translation $\mathcal{S}$ of Υ_n in the tiling. A point $\mathbf{u} \in \mathbb{Z}^n$ is *covered* by a codeword $\mathbf{x}$ in a tiling $\mathbb{T}$ if $\mathbf{u}$ is contained in the translation $\mathbf{x} + \Upsilon_n$. In this case it is said that $\mathbf{x}$ *covers* $\mathbf{u}$.

Given a tiling $\mathbb{T}$ with Υ_n it has to satisfy properties **($\mathcal{P}$.1)** and **($\mathcal{P}$.2)**. By considering how each point $\mathbf{u} \in \mathbb{Z}^n$ is covered by a codeword $\mathbf{x} \in \mathbb{T}$ (property **($\mathcal{P}$.1)**), the structure of $\mathbb{T}$ will be discovered. To this end, property **($\mathcal{P}$.2)** is used, i.e. for each two codewords $\mathbf{x}, \mathbf{y} \in \mathbb{T}$ we have that $d_C(\mathbf{x}, \mathbf{y}) \geq 3$ (by Corollary 2.10).

2.1 The Nonexistence of Tilings with the $(0.5, n)$-Cross

In this section it is proved that an integer tiling $\mathbb{T}$ with Υ_n exists only if $n = 2^t - 1$ or $n = 3^t - 1$, for some $t > 0$. First, this claim is proved for odd n if $\mathbb{T}$ is an integer tiling and for all n if $\mathbb{T}$ is a lattice tiling (see Definition 1.10). Then, the proof is completed for even n. This goal is obtained by proving that given a tiling $\mathbb{T}$ with Υ_n, certain elements of $\mathbb{Z}^n$ must be contained in $\mathbb{T}$. It is proved by considering how elements with a small cross weight are covered. For the rest of this section let $\mathbb{T}$ be a tiling with Υ_n. By Lemma 1.3, for every $\mathbf{u} \in \mathbb{Z}^n$, $\mathbf{u} + \mathbb{T}$ is also a tiling with Υ_n, thus, without loss of generality we assume throughout this section that $\mathbf{0} \in \mathbb{T}$. By Corollary 2.10, if $\mathbf{x}, \mathbf{y} \in \mathbb{T} \setminus \{\mathbf{0}\}$, where $\mathbf{x} \neq \mathbf{y}$, then $w_C(\mathbf{x}) \geq 3$, $w_C(\mathbf{y}) \geq 3$, and $d_C(\mathbf{x}, \mathbf{y}) \geq 3$.

The first lemma is an immediate result from the definition of Υ_n.

Lemma 2.11 *Let* $\mathbf{x} \in \mathbb{T}$ *and* $\mathbf{u} = (u_1, u_2, \dots, u_n) \in \mathbb{Z}^n$. *The point* $\mathbf{u}$ *is covered by* $\mathbf{x}$ *if and only if* $x_i \in \{u_i - 1, u_i, u_i + 1, u_i + 2\}$, *for* $1 \leq i \leq n$, *and for at most one* i *we have* $x_i \in \{u_i - 1, u_i + 2\}$.

Let $\mathcal{D}_1$ be the set of points from $\{0, 1, 2, 3\}^n$ in which 2 and 3 appear exactly once.

Lemma 2.12 *If* $\mathbf{x} \in \mathcal{D}_1 \cap \mathbb{T}$ *then* $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s$ *for some* $r \neq s$.

Proof. Assume without loss of generality that $\mathbf{x} = (3, 2, 1, x_4, \dots, x_n)$, where $x_i \in \{0, 1\}$, for $4 \leq i \leq n$. The point $\mathbf{u} = (1, 1, -1, 0, \dots, 0)$ is covered by a codeword $\mathbf{y} \in \mathbb{T}$. By Lemma 2.11 we have that $\mathbf{y} \notin \{\mathbf{x}, \mathbf{0}\}$ and we can distinguish between three cases:
Case 1: If $y_i \in \{u_i, u_i + 1\}$ for all i, $1 \leq i \leq n$, then $w_C(\mathbf{y}) \leq 2$, a contradiction.
Case 2: There exists a j such that $y_j = u_j - 1$ and $y_i \in \{u_i, u_i + 1\}$ for all $i \neq j$. Since $w_C(Y) \geq 3$ it follows that $j = 3$ and hence $\mathbf{y} = (2, 2, -2, y_4, \dots, y_n)$, where $y_i \in \{0, 1\}$, for $4 \leq i \leq n$. This implies that $d_C(\mathbf{x}, \mathbf{y}) = 2$, a contradiction.
Case 3: There exists a j such that $y_j = u_j + 2$ and $y_i \in \{u_i, u_i + 1\}$ for all $i \neq j$. Since $w_C(\mathbf{y}) \geq 3$ it follows that $j \neq 3$. Without loss of generality it implies that $\mathbf{y}$ can take one of the following forms:

- $\mathbf{y} = (3, 2, y_3, y_4, \dots, y_n)$ or $\mathbf{y} = (2, 3, y_3, y_4, \dots, y_n)$, where $y_3 \in \{-1, 0\}$ and $y_i \in \{0, 1\}$, for $4 \leq i \leq n$.

- $\mathbf{y} = (2, 2, y_3, 2, y_5, \dots, y_n)$, where $y_3 \in \{-1, 0\}$ and $y_i \in \{0, 1\}$, for $5 \leq i \leq n$.

Both forms implies that $d_C(\mathbf{x}, \mathbf{y}) \leq 2$, a contradiction.

Therefore, there is no codeword $\mathbf{y} \in \mathbb{T}$ which covers $\mathbf{u}$, a contradiction. Thus, if $\mathbf{x} \in \mathcal{D}_1 \cap \mathbb{T}$ then $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s$ for some $r \neq s$.

□

Let $\mathcal{D}_2$ be the set of points from $\{0, 1, 4\}^n$ in which 4 appears exactly once.

Lemma 2.13 *If* $\mathbf{x} \in \mathcal{D}_2 \cap \mathbb{T}$ *then* $\mathbf{x} = 4\mathbf{e}_r$ *for some* $1 \leq r \leq n$.

Proof. Assume without loss of generality that $\mathbf{x} = (4, 1, x_3, \dots, x_n)$, where $x_i \in \{0, 1\}$, for $3 \leq i \leq n$. The point $\mathbf{u} = (1, 1, 0, \dots, 0)$ is covered by a codeword $\mathbf{y} \in \mathbb{T}$. By Lemma 2.11 we have that $\mathbf{y} \notin \{\mathbf{x}, \mathbf{0}\}$ and we can distinguish between two cases:

Case 1: If $y_i \in \{u_i, u_i + 1\}$ for all i, $1 \leq i \leq n$, with a possible exception for at most one j, for which $y_j = a_j - 1$, then $w_C(Y) \leq 2$, a contradiction.
Case 2: There exists a j such that $y_j = u_j + 2$ and $y_i \in \{u_i, u_i + 1\}$ for all $i \neq j$. Without loss of generality it implies that $\mathbf{y}$ can take one of the following forms:

- $\mathbf{y} = (3, 2, y_3, \ldots, y_n)$, $\mathbf{y} = (2, 3, y_3, \ldots, y_n)$, where $y_i \in \{0, 1\}$ for $3 \leq i \leq n$.
- $\mathbf{y} = (2, 2, 2, y_4, \ldots, y_n)$, where $y_i \in \{0, 1\}$ for $4 \leq i \leq n$.

Hence, $d_C(\mathbf{x}, \mathbf{y}) \leq 2$, a contradiction.

Therefore, there is no codeword $\mathbf{y} \in \mathbb{T}$ which covers $\mathbf{u}$, a contradiction. Thus, if $\mathbf{x} \in \mathcal{D}_2 \cap \mathbb{T}$ then $\mathbf{x} = 4\mathbf{e}_r$ for some $1 \leq r \leq n$.

□

Corollary 2.14 *For each r, $1 \leq r \leq n$, the point $2\mathbf{e}_r$ is covered by a codeword $\mathbf{x} \in \mathbb{T}$, where either $\mathbf{x} = 4\mathbf{e}_r$ or $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s$ for some $s \neq r$.*

Proof. By Lemma 2.11, $\mathbf{x}$ is not the all-zero codeword. Moreover, since $w_C(\mathbf{x}) \geq 3$ it can be easily verified that either $\mathbf{x} \in \mathcal{D}_1$ or $\mathbf{x} \in \mathcal{D}_2$. It follows from Lemmas 2.12 and 2.13 that either $\mathbf{x} = 4\mathbf{e}_r$ or $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s$ for some $s \neq r$.

□

Let $\mathcal{D}_3$ be the set of points from $\{0, 1, 2\}^n$ in which 2 appears exactly three times.

Lemma 2.15 *If $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ then for every $k \notin \{r, s\}$ there exists a unique $j \notin \{r, s, k\}$ and a codeword $\mathbf{y} \in \mathcal{D}_3 \cap \mathbb{T}$ such that $y_r = 1, y_s = y_k = y_j = 2$.*

Proof. Let $k \notin \{r, s\}$ and consider the point $\mathbf{u} = \mathbf{e}_r + \mathbf{e}_s + \mathbf{e}_k$. Assume without loss of generality that $r = 1$, $s = 2$, and $k = 3$, i.e. $\mathbf{x} = (3, 2, 0, \ldots, 0)$ and $\mathbf{u} = (1, 1, 1, 0 \ldots, 0)$. The point $\mathbf{u}$ is covered by a codeword $\mathbf{y} \in \mathbb{T}$. By Lemma 2.11 we have that $\mathbf{y} \notin \{\mathbf{x}, \mathbf{0}\}$ and we can distinguish between three cases:
Case 1: If $y_i \in \{u_i, u_i + 1\}$ for $1 \leq i \leq n$, then since $w_C(\mathbf{y}) \geq 3$ it follows that $\mathbf{y} = (2, 2, 2, y_4, \ldots, y_n)$, where $y_i \in \{0, 1\}$, for $4 \leq i \leq n$. Hence, $d_C(\mathbf{x}, \mathbf{y}) = 1$, a contradiction.
Case 2: There exists a j such that $y_j = u_j - 1$ and $y_i \in \{u_i, u_i + 1\}$ for all $i \neq j$. If $j \leq 3$ then $w_C(\mathbf{y}) \leq 2$, a contradiction. If $j > 3$ then since $w_C(\mathbf{y}) \geq 3$ it follows that $\mathbf{y} = (2, 2, 2, y_4, \ldots, y_n)$, where $y_i \in \{-1, 0, 1\}$ for $4 \leq i \leq n$, and hence $d_C(\mathbf{x}, \mathbf{y}) = 1$, a contradiction.

Case 3: There exists a j such that $y_j = u_j + 2$ and $y_i \in \{u_i, u_i + 1\}$ for all $i \neq j$. If $j \leq 3$ then since $w_C(\mathbf{y}) \geq 3$ and $d_C(\mathbf{x}, \mathbf{y}) \geq 3$ it follows that $\mathbf{y} = (1, 2, 3, y_4, \dots, y_n)$, where $y_i \in \{0, 1\}$, for $4 \leq i \leq n$, a contradiction to Lemma 2.12.

Therefore, there exists a $j > 3$ such that $y_j = u_j + 2$ and $y_i \in \{u_i, u_i + 1\}$ for all $i \neq j$. Assume without loss of generality that $j = 4$. Since $w_C(\mathbf{y}) \geq 3$ and $d_C(\mathbf{x}, \mathbf{y}) \geq 3$ it follows that $\mathbf{y} = (1, 2, 2, 2, y_5, \dots, y_n)$, where $y_i \in \{0, 1\}$, for $5 \leq i \leq n$. The uniqueness of j follows from the fact that if there exists another j and a related codeword $\mathbf{y}'$ then $d_C(\mathbf{y}, \mathbf{y}') \leq 2$.

□

Corollary 2.16 *If $3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$, for some $r, s \in [n]$, $r \neq s$, then n is even.*

Proof. By Lemma 2.15 all coordinates except for r and s should be paired, in disjoint pairs (such a pair $\{k, j\}$ induces a codeword of the form $\mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathcal{D}_3 \cap \mathbb{T}$, where $y_r = 1, y_s = y_k = y_j = 2$). Thus, n is even.

□

From Corollaries 2.14 and 2.16 it is infered that

Corollary 2.17 *If n is odd then for all $\mathbf{x} \in \mathbb{T}$ and $1 \leq r \leq n$ we have $\mathbf{x} + 4\mathbf{e}_r \in \mathbb{T}$, i.e. $\mathbb{T}$ is a periodic tiling with period 4.*

Theorem 2.18 *If $\mathbb{T}$ is an integer tiling with Υ_n, where n is an odd integer, then $n = 2^t - 1$ for some $t > 0$.*

Proof. By Corollary 2.17 we have that $\mathbb{T}$ is a periodic tiling with period 4. Therefore, $\mathbb{C} = \mathbb{T} \cap \{0, 1, 2, 3\}^n$ is a tilling of $\mathbb{Z}_4^n$ with Υ_n. Therefore, $|\mathbb{C}| \cdot |\Upsilon_n| = 4^n$ and $|\Upsilon_n|$ divides 4^n. The size of Υ_n is $2^n(n + 1)$ and hence $n = 2^t - 1$ for some $t > 0$.

□

Lemma 2.19 *If there exist two distinct codewords $\mathbf{x} = 3\mathbf{e}_i + 2\mathbf{e}_j$ and $\mathbf{x}' = 3\mathbf{e}_r + 2\mathbf{e}_s$ in $\mathbb{T}$ then $\{i, j\} \cap \{r, s\} = \varnothing$.*

Proof. Assume without loss of generality that $i = 1$ and $j = 2$. Since $d_C(\mathbf{x}, \mathbf{x}') \geq 3$ it follows that $r \neq 1$ and $\mathbf{x}' \neq 3\mathbf{e}_2 + 2e_1$. If $r = 2$ or $s = 2$ then assume without loss of generality that $\mathbf{x}' = (0, 3, 2, 0, \dots, 0)$ or $\mathbf{x}' = (0, 2, 3, 0, \dots, 0)$. By Lemma 2.15 we have a codeword $\mathbf{y} = (1, 2, 2, y_4, \dots, y_n) \in \mathcal{D}_3 \cap \mathbb{T}$. It implies that $d_C(\mathbf{x}', \mathbf{y}) = 1$, a contradiction. The case where $s = 1$ and $r > 2$ is symmetric to the case where $r = 2$ and $s > 2$.

□

From Corollary 2.14 and Lemma 2.19 we have that

Corollary 2.20 *If* $3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ *then* $4\mathbf{e}_s \in \mathbb{T}$.

Theorem 2.21 *If* $\mathbb{T}$ *is an integer lattice tiling with* Υ_n *then either* $n = 2^t-1$ *or* $n = 3^t - 1$ *for some* $t > 0$.

Proof. Assume that there are exactly k codewords of the form $3\mathbf{e}_i + 2\mathbf{e}_j$ in $\mathbb{T}$. From Corollaries 2.14 and 2.20 and by Lemma 2.19 the lattice $\mathbb{T}$ contains a sublattice defined by these k codewords and $n-k$ codewords of the form $4\mathbf{e}_s$. The generator matrix of this sublattice is a block-diagonal matrix with k 2×2 blocks of the form $\begin{bmatrix} 3 & 2 \\ 0 & 4 \end{bmatrix}$ and $n-2k$ 1×1 blocks of the form $[\ 4\ ]$. The volume of this sublattice is divided by the volume of the lattice $\mathbb{T}$. The volume of the sublattice is $3^k 4^{n-k}$ and therefore, the volume of the lattice $\mathbb{T}$ is of the form $3^\ell 2^m$, for some $\ell \geq 0$ and $m \geq 0$. On the otherhand the volume of the lattice $\mathbb{T}$ is the volume of the shape Υ_n, i.e. $2^n(n+1)$. By Theorem 2.18 we have that if n is odd then $n = 2^t - 1$ for some $t > 0$. If n is even then $n+1$ is odd and since $3^\ell 2^m = 2^n(n+1)$ we must have that $n = 3^\ell - 1$ for some $\ell > 0$.

□

It remains to prove that if there exists an integer tiling of $\mathbb{Z}^n$ with Υ_n, where n is even, then $n = 3^t - 1$, for some $t > 0$. To this end, the concept of packing triple system is required, which will be used to prove that if n is even then $\mathbb{T}$ contains exactly $\frac{n}{2}$ codewords of the form $3\mathbf{e}_r + 2\mathbf{e}_s$, where the union of their nonzero coordinates is the set of all n coordinates. The structure of the codewords in $\mathbb{T}$ combined with arguments based on reflections and translations of the tiling, will imply a period 12 for the tiling when n is even. As a consequence it is infered that if n is even then $n = 3^t - 1$, for some $t > 0$.

A *packing triple system* of order n is a pair $(Q, \mathcal{B})$, where Q is an n-set and $\mathcal{B}$ is a collection of 3-subsets of Q, called *blocks* such that each 2-subset of Q is contained in at most one block of $\mathcal{B}$. Spencer [81] proved that if $n \not\equiv 5 \pmod 6$ then

$$|\mathcal{B}| \leq \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor \ . \tag{2.1}$$

Lemma 2.22 *For each* $1 \leq i < j \leq n$, *the point* $\mathbf{e}_i + \mathbf{e}_j$ *is covered by a codeword* $\mathbf{x} \in \mathbb{T}$, *where* $\mathbf{x} = 3\mathbf{e}_i + 2\mathbf{e}_j$ *or* $\mathbf{x} = 3\mathbf{e}_j + 2\mathbf{e}_i$ *or* $\mathbf{x} \in \mathcal{D}_3$, *where* $x_i = x_j = 2$.

Proof. Follows from Lemmas 2.11 and 2.12 and the fact that for each nonzero codeword $\mathbf{x} \in \mathbb{T}$ we have $w_C(\mathbf{x}) \geq 3$.

□

Let

$$\mathcal{F}_1 \overset{\text{def}}{=} \{\{i,j\} \ : \ 3\mathbf{e}_i + 2\mathbf{e}_j \in \mathbb{T}\}$$

and

$$\mathcal{F}_2 \overset{\text{def}}{=} \{\{i,j,k\} \ : \ 2\mathbf{e}_i + 2\mathbf{e}_j + 2\mathbf{e}_k + \sum_{m \notin \{i,j,k\}} \alpha_m \mathbf{e}_m \in \mathbb{T}, \ \alpha_m \in \{0,1\}\} \ .$$

Since $\mathbb{T}$ is a tiling it follows that each point $\mathbf{e}_i + \mathbf{e}_j$, $i \neq j$, is covered by exactly one codeword of $\mathbb{T}$. As a consequence of Lemma 2.22, we have that each pair $\{r,s\}$ is a subset of exactly one element from $\mathcal{F}_1 \cup \mathcal{F}_2$. Therefore, $\mathcal{F}_2$ is a packing triple system of order n.

Theorem 2.23 *If $\mathbb{T}$ is an integer tiling with Υ_n then $n \not\equiv 4$ (mod 6).*

Proof. Assume $\mathbb{T}$ is an integer tiling with Υ_n, $n \equiv 4$ (mod 6). By (2.1) we have that

$$|\mathcal{F}_2| \leq \frac{n^2 - 2n - 2}{6} \ .$$

Since each pair $\{i,j\} \subset \{1,2,\ldots,n\}$ is contained in either $\mathcal{F}_1$ or $\mathcal{F}_2$ it follows that

$$|\mathcal{F}_1| + 3|\mathcal{F}_2| = \binom{n}{2} \ .$$

Hence, $|\mathcal{F}_1| \geq \frac{n}{2} + 1$. Lemma 2.19 implies that $|\mathcal{F}_1| \leq \frac{n}{2}$, a contradiction.

□

By using the same arguments as in the proof of Theorem 2.23 we have that if $n \equiv 0$ or 2 (mod 6) then $|\mathcal{F}_1| \geq \frac{n}{2}$. Hence, by Lemma 2.19 the following lemma is inferred

Lemma 2.24 *If n is even and $\mathbb{T}$ is an integer tiling with Υ_n, then there are exactly $\frac{n}{2}$ codewords of the form $3\mathbf{e}_r + 2\mathbf{e}_s$.*

Combing Lemmas 2.19 and 2.24 results in the following corollary.

Corollary 2.25 *If n is even and $\mathbb{T}$ is an integer tiling with Υ_n, then there are exactly $\frac{n}{2}$ codewords of the form $3\mathbf{e}_r + 2\mathbf{e}_s$ and the set $\{i \ : \ 3\mathbf{e}_i + 2\mathbf{e}_j \in \mathbb{T}$ or $3\mathbf{e}_j + 2\mathbf{e}_i \in \mathbb{T}\}$ contains all the integers between 1 and n.*

Let $\mathbb{T}'$ be the tiling of $\mathbb{Z}^n$ with Υ_n defined by $\mathbb{T}' \overset{\text{def}}{=} \{\mathbf{x} \ : \ -\mathbf{x} \in \mathbb{T}\}$. Since $\mathbb{T}'$ is a tiling of $\mathbb{Z}^n$ with Υ_n, it follows that the lemmas and the corollaries that hold for the tiling $\mathbb{T}$ hold also for $\mathbb{T}'$. They imply new lemmas and corollaries for $\mathbb{T}$. For example we have

Corollary 2.26 *For each r, $1 \leq r \leq n$, the point $-2\mathbf{e}_r$ is covered by a codeword $\mathbf{x} \in \mathbb{T}$, where either $\mathbf{x} = -4\mathbf{e}_r$ or $\mathbf{x} = -3\mathbf{e}_r - 2\mathbf{e}_s$ for some $s \neq r$.*

In a similar way we can define 2^n tilings of $\mathbb{Z}^n$ with Υ_n. For $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, where $a_i \in \{-1, 1\}$, let $\mathbb{T}_\mathbf{a}$ be the tiling of $\mathbb{Z}^n$ with Υ_n defined by

$$\mathbb{T}_\mathbf{a} \overset{\text{def}}{=} \{(x_1, x_2, \ldots, x_n) \ : (a_1x_1, a_2x_2, \ldots, a_nx_n) \in \mathbb{T}\}.$$

As for $\mathbb{T}' = \mathbb{T}_{(-1,-1,\ldots,-1)}$, each lemma and each corollary holds for $\mathbb{T}_\mathbf{a}$ and thus implies new claims on $\mathbb{T}$. Without loss of generality we assume (based on Lemma 1.4, Corollaries 2.20 and 2.25) that $3\mathbf{e}_{2i-1}+2\mathbf{e}_{2i} \in \mathbb{T}$ and $4\mathbf{e}_{2i} \in \mathbb{T}$, for all $1 \le i \le \frac{n}{2}$.

Lemma 2.27 *If* $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ *then* $-4\mathbf{e}_s \in \mathbb{T}$.

Proof. Without loss of generality we will prove the claim for $r = 1$ and $s = 2$; let $\mathbf{a} = (1, -1, 1, \ldots, 1)$. Since $3\mathbf{e}_{2i-1} + 2\mathbf{e}_{2i} \in \mathbb{T}$, for all $2 \le i \le \frac{n}{2}$, it follows that $3\mathbf{e}_{2i-1} + 2\mathbf{e}_{2i} \in \mathbb{T}_\mathbf{a}$, for all $2 \le i \le \frac{n}{2}$, and by Corollary 2.25 we have that either $3\mathbf{e}_1 + 2\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$ or $2\mathbf{e}_1 + 3\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$. If $2\mathbf{e}_1 + 3\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$ then Corollary 2.20 implies that $\mathbf{y} = 4\mathbf{e}_1 \in \mathbb{T}_\mathbf{a}$. Therefore, $\mathbf{y} = 4\mathbf{e}_1 \in \mathbb{T}$, and since $d_C(\mathbf{x}, \mathbf{y}) = 1$ we have a contradiction. Hence, $3\mathbf{e}_1 + 2\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$, and therefore, by Corollary 2.20 we have that $4\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$, i.e. $-4\mathbf{e}_2 \in \mathbb{T}$.

□

Corollary 2.28 $4\mathbf{e}_s \in \mathbb{T}$ *if and only if* $-4\mathbf{e}_s \in \mathbb{T}$.

Lemma 2.29 *If* $\mathbf{x} = 3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ *then* $-3\mathbf{e}_r - 2\mathbf{e}_s \in \mathbb{T}$.

Proof. Without loss of generality we will prove the claim for $r = 1$ and $s = 2$; let $\mathbf{a} = (-1, -1, 1, \ldots, 1)$. Since $3\mathbf{e}_{2i-1} + 2\mathbf{e}_{2i} \in \mathbb{T}$, for all $2 \le i \le \frac{n}{2}$, it follows that $3\mathbf{e}_{2i-1} + 2\mathbf{e}_{2i} \in \mathbb{T}_\mathbf{a}$, for all $2 \le i \le \frac{n}{2}$, and by Corollary 2.25 we have that either $3\mathbf{e}_1 + 2\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$ or $2\mathbf{e}_1 + 3\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$. If $2\mathbf{e}_1 + 3\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$ then Lemma 2.27 implies that $-4\mathbf{e}_1 \in \mathbb{T}_\mathbf{a}$. Therefore, $\mathbf{y} = 4\mathbf{e}_1 \in \mathbb{T}$, and since $d_C(\mathbf{x}, \mathbf{y}) = 1$ we have a contradiction. Hence, $3\mathbf{e}_1 + 2\mathbf{e}_2 \in \mathbb{T}_\mathbf{a}$, and therefore we have that $-3\mathbf{e}_1 - 2\mathbf{e}_2 \in \mathbb{T}$.

□

Corollary 2.30 $3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ *if and only if* $-3\mathbf{e}_r - 2\mathbf{e}_s \in \mathbb{T}$.

Lemma 2.31 *If* $3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ *then* $12\mathbf{e}_r, 12\mathbf{e}_s \in \mathbb{T}$.

Proof. By Corollary 2.20 we have that $4\mathbf{e}_s \in \mathbb{T}$. The translation $\mathbb{T}_1 = -4\mathbf{e}_s + \mathbb{T}$ is a tiling with Υ_n for which $\mathbf{0}, -4\mathbf{e}_s \in \mathbb{T}_1$. It follows by Corollary 2.28 that $4\mathbf{e}_s \in \mathbb{T}_1$ and hence $8\mathbf{e}_s \in \mathbb{T}$. Similarly, $12\mathbf{e}_s \in \mathbb{T}$.

Similarly, by Corollary 2.30 we have that $\mathbf{0}, 3\mathbf{e}_r + 2\mathbf{e}_s \in \mathbb{T}$ implies that $6\mathbf{e}_r + 4\mathbf{e}_s, 9\mathbf{e}_r + 6\mathbf{e}_s, 12\mathbf{e}_r + 8\mathbf{e}_s \in \mathbb{T}$. The translation $\mathbb{T}_1 = -12\mathbf{e}_r - 8\mathbf{e}_s + \mathbb{T}$

is a tiling with Υ_n for which $\mathbf{0}, -3\mathbf{e}_r - 2\mathbf{e}_s \in \mathbb{T}_1$. By Corollary 2.30 and Lemma 2.27 we have that $-4\mathbf{e}_s \in \mathbb{T}_1$, and hence $12\mathbf{e}_r + 4\mathbf{e}_s \in \mathbb{T}$. Similarly, by Corollary 2.28 we have $12\mathbf{e}_r + 4\mathbf{e}_s, 12\mathbf{e}_r + 8\mathbf{e}_s \in \mathbb{T}$ which implies that $12\mathbf{e}_r \in \mathbb{T}$.

□

Corollary 2.32 *If n is even and $\mathbb{T}$ is an integer tiling with Υ_n, then $\mathbb{T}$ is a periodic tiling with period 12.*

Theorem 2.33 *If $\mathbb{T}$ is an integer tiling with Υ_n, where n is an even integer, then $n = 3^t - 1$ for some $t > 0$.*

Proof. By Corollary 2.32 we have that $\mathbb{T}$ is a periodic tiling with period 12. Therefore, the size of Υ_n divides 12^n. The size of Υ_n is $2^n(n+1)$ and hence $n+1$ divides $2^n 3^n$. Since n is even it follows that $n+1$ is odd and thus $n = 3^t - 1$ for some $t > 0$.

□

Theorems 2.18 and 2.33 are combined to obtain

Corollary 2.34 *If $\mathbb{T}$ is an integer tiling with Υ_n, then either $n = 2^t - 1$ or $n = 3^t - 1$, for some $t > 0$.*

Corollary 2.35 *If $\mathbb{T}$ is a $\frac{1}{2}\mathbb{Z}$-tiling with a $(0.5, n)$-cross, then either $n = 2^t - 1$ or $n = 3^t - 1$, for some $t > 0$.*

2.2 Tilings based on Perfect Codes in the Hamming Scheme

In section 2.1 it is proved that a $\frac{1}{2}\mathbb{Z}$-tiling with $(0.5, n)$-cross exists only if $n = 2^t - 1$ or $n = 3^t - 1$, for some $t > 0$. In this section it is proved that this necessary condition is also sufficient. Surprisingly, two constructions which produce the related tilings are based on perfect codes in the Hamming scheme (for definition of Hamming distance see Definition 1.13) . If $n = 2^t - 1$ then the perfect code is binary of length n and the construction of the tiling is very simple. If $n = 3^t - 1$ then the perfect code is ternary of length $\frac{n}{2}$.

Recall that for a code $\mathcal{C}$, its minimum Hamming distance, $d_H(\mathcal{C})$, is the largest integer d for which $d_H(\mathbf{x}, \mathbf{y}) \geq d$, for every two distinct codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. The *minimum cross distance* of a code $\mathcal{C}$, $d_C(\mathcal{C})$, is defined similarly. A code $\mathcal{C} \subset \mathbb{Z}_q^n$ with minimum Hamming distance $2t+1$ is a perfect t-error-correcting code if for each word $\mathbf{a} \in \mathbb{Z}_q^n$ there exists a codeword $\mathbf{x} \in \mathcal{C}$

such that $d_H(\mathbf{a}, \mathbf{x}) \leq t$. Such a code is capable to correct up to t transmission errors [58]. The Hamming sphere of radius t centered at $\mathbf{u} \in \mathbb{Z}_q^n$ is the set $\{\mathbf{v} \in \mathbb{Z}_q^n \ : \ d_H(\mathbf{u}, \mathbf{v}) \leq t\}$. The code $\mathcal{C}$ is a perfect single-error-correcting code if and only if $\mathcal{C}$ is a tiling of $\mathbb{Z}_q^n$ with a Hamming sphere of radius one. Only single-error-correcting are used in this section. Henceforth, a perfect single-error-correcting code will shortly be called a perfect code. Binary ($q = 2$) perfect codes exists if and only if $n = 2^t - 1$, where $t > 0$. Ternary ($q = 3$) perfect codes exists if and only if $n = \frac{3^t-1}{2}$, where $t > 0$. These are the only perfect codes which are of interest in this section. Finally, we note that a perfect code is identified by its size, its minimum distance, and the fact that each element of $\mathbb{Z}_q^n$ is covered by at least one codeword. One can easily verify that given any two of these parameters one can determine whether the code is perfect or not perfect. This fact will be used throughout this section.

Remark 2.1 *A perfect code $\mathcal{C}$ of length n over $\mathbb{Z}_q$ is known to exist if q is a power of a prime and $n = \frac{q^t-1}{q-1}$, where $t > 0$. The related sphere of radius one can be viewed as a $(q-1, n)$-semicross or as a $(\frac{q-1}{2}, n)$-cross. Thus, these perfect codes form tilings with the related semicrosses and crosses. Only if q is a prime some of the known tilings are lattice tilings (they are related to linear perfect codes). If q is not a prime then the tiling of $\mathbb{Z}^n$ is done first by using any one-to-one mapping between GF(q) (on which the codes are defined) and $\mathbb{Z}_q$. Tilings of this type have applications in flash memories [76]. If $q = 2$ then $\mathcal{C}$ is a tiling of $\mathbb{Z}_2^n$ with $(0.5, n)$-cross and $E(\mathcal{C})$ forms a tiling of $\mathbb{Z}^n$ with $(0.5, n)$-cross.*

2.2.1 Binary Perfect Codes

Since the size of of a sphere with radius one in $\mathbb{Z}_2^n$ is $n + 1$, it follows that a binary perfect code of length $n = 2^t - 1$ has 2^{n-t} codewords.

Theorem 2.36 *There exists an one-to-one correspondence between the set of binary perfect codes of length $n = 2^t - 1$ and the set of integer tilings with Υ_n in which each codeword has only even entries.*

Proof. Note first, that by Corollary 2.17 a tiling $\mathbb{T}$ of $\mathbb{Z}^n$ with Υ_n is periodic with period 4 and hence it can be reduced to a tiling of $\mathbb{Z}_4^n$ with Υ_n.

The size of an $(1, n)$-semicross is equal the size of a $(0.5, n)$-cross. It implies that the number of codewords in a binary perfect single-error-correcting code $\mathcal{C}$ of length $n = 2^t - 1$ is equal the number of codewords in a tiling $\mathbb{T}$

of $\mathbb{Z}_4^n$ with Υ_n. If $\mathbf{x}, \mathbf{y} \in \{0,2\}^n$ then $0.5\mathbf{x}$ and $0.5\mathbf{y}$ are binary words and it is easy to verify that $d_C(\mathbf{x}, \mathbf{y}) = d_H(0.5\mathbf{x}, 0.5\mathbf{y})$.

Therefore, if $\mathcal{C}$ is a binary perfect code of length $n = 2^t - 1$ then $2E(\mathcal{C})$ is a tiling of $\mathbb{Z}^n$ with Υ_n in which each codeword has only even entries. Similarly, if $\mathbb{T}$ is a tiling of $\mathbb{Z}^n$ with Υ_n, in which each codeword has only even entries, then $0.5\mathbb{T} \cap \{0,1\}^n$ is a binary perfect code.

□

Corollary 2.37 *There exists an one-to-one correspondence between the set of binary perfect codes of length $n = 2^t - 1$ and the set of integer tilings with $(0.5, n)$-cross.*

Do there exists any integer tilings with Υ_n, where $n = 2^t - 1$, except for those implied by Theorem 2.36? The answer is that there exist many such tilings. Let $\mathcal{C}$ be a binary code of length n. Its *punctured* code $\mathcal{C}'$ of length $n-1$ is defined by $\mathcal{C}' \overset{\text{def}}{=} \{\mathbf{c} \ : \ (\mathbf{c}, x) \in \mathcal{C}, \ x \in \{0,1\}\}$.

Construction 2.38 *Let $\mathcal{C}$ be a binary perfect code of length n and $\mathcal{C}'$ its punctured code. Let $\mathcal{C}'_e$ and $\mathcal{C}'_o$ be the set of codewords from $\mathcal{C}'$ with even weight and odd weight, respectively. We define a code $\mathcal{C}^* \overset{\text{def}}{=} \mathcal{C}_1^* \cup \mathcal{C}_2^*$ over $\mathbb{Z}_4^n$, where*

$$\mathcal{C}_1^* \overset{\text{def}}{=} \{(2\mathbf{c}, 2x) \ : \ \mathbf{c} \in \mathcal{C}'_e, \ (\mathbf{c}, x) \in \mathcal{C}\} \text{ and } \mathcal{C}_2^* \overset{\text{def}}{=} \{(2\mathbf{c}, 2x{+}1) \ : \ \mathbf{c} \in \mathcal{C}'_o, \ (\mathbf{c}, x) \in \mathcal{C}\} \ .$$

Theorem 2.39 *The expanded code of $\mathcal{C}^*$,*

$$E(\mathcal{C}^*) = \{\mathbf{x} \in \mathbb{Z}^n \ : \ (x_1(\ mod \ 4), x_2(\ mod \ 4), \ldots, x_n(\ mod \ 4)) \in \mathcal{C}^*\},$$

defines a tiling of $\mathbb{Z}^n$ with Υ_n, in which not all entries are even.

Proof. Since $d_H(\mathcal{C}) = 3$ it follows that $d_H(\mathcal{C}') = d_H(\mathcal{C}'_e) = d_H(\mathcal{C}'_o) = 2$ and $d_C(\mathcal{C}_1^*) = d_C(\mathcal{C}_2^*) = 3$. If $\tilde{\mathbf{c}}_1 \in \mathcal{C}'_e$ and $\tilde{\mathbf{c}}_2 \in \mathcal{C}'_o$ then $d_H(\tilde{\mathbf{c}}_1, \tilde{\mathbf{c}}_2)$ is an odd integer. Hence, since $d_H(\mathcal{C}') = 2$, it follows that $d_H(\tilde{\mathbf{c}}_1, \tilde{\mathbf{c}}_2) \geq 3$. Therefore, if $\tilde{\mathbf{c}}_1^* \in \mathcal{C}_1$ and $\tilde{\mathbf{c}}_2^* \in \mathcal{C}_2$ then $d_C(\tilde{\mathbf{c}}_1^*, \tilde{\mathbf{c}}_2^*) \geq 3$ and thus $d_C(\mathcal{C}^*) \geq 3$. The minimum distance of the code $\mathcal{C}^*$ and its number of codewords implies that $\mathcal{C}^*$ is a tiling of $\mathbb{Z}_4^n$ with Υ_n. It is easy to verify that $\mathcal{C}'_o$ has at least one codeword (in fact it can be proved that it contains exactly half of the codewords) and hence the last entry in at least one of the codewords of $\mathcal{C}^*$ is 1 or 3.

□

Example 2.40 *The following code forms a tiling of $\mathbb{Z}_4^7$ with Υ_7:*

0000000	0000222	2222000	2222222
2200201	2200023	0022201	0022023
2020021	2020203	0202021	0202203
2002002	2002220	0220002	0220220

Remark 2.2 *Let ξ be a mapping from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ defined by $\xi(0) = \xi(1) = 0$, $\xi(2) = \xi(3) = 1$. If $\mathbb{T}$ forms a tiling of $\mathbb{Z}_4^n$ with Υ_n then the code $\mathcal{C} = \{\xi(\mathbf{x}) \ : \ \mathbf{x} \in \mathbb{T}\}$, where $\xi(x_1, x_2, \ldots, x_n) = (\xi(x_1), \xi(x_2), \ldots, \xi(x_n))$ is a binary perfect code of length n.*

Remark 2.3 *By Corollary 2.17 an integer tiling with Υ_n, where n is odd, has period 4. Hence, the related $\frac{1}{2}\mathbb{Z}$-tiling $\mathbb{T}$ with $(0.5, n)$-cross has period 2. It implies that this tiling is also a tiling with the $(1, n)$-semicross (even if $\mathbb{T}$ is not a $\mathbb{Z}$-tiling).*

2.2.2 Ternary Perfect Codes

Let $\nu = \frac{n}{2}$. Since the size of a sphere with radius one in $\mathbb{Z}_3^\nu$ is $2\nu+1$, it follows that a ternary perfect code of length ν has $3^{\nu-t}$ codewords. Let Λ_n be the lattice generated by the basis $\{3\mathbf{e}_{2i-1} + 2\mathbf{e}_{2i} \ : \ 1 \leq i \leq \nu\} \cup \{4\mathbf{e}_{2i} \ : \ 1 \leq i \leq \nu\}$. Let G_n be the quotient group $\mathbb{Z}^n / \Lambda_n$. The following lemma can be readily verified.

Lemma 2.41 *The group G_2 has size 12 and the 12 representatives of elements from G_2 (the cosets of Λ_2 in $\mathbb{Z}^2$) can be taken as $\{0,1,2\} \times \{0,1,2,3\} = [0,2] \times [0,3]$.*

Let $([0,2] \times [0,3])^m \overset{\text{def}}{=} \underbrace{([0,2] \times [0,3]) \times ([0,2] \times [0,3]) \times \ \cdots \ \times ([0,2] \times [0,3])}_{m \text{ times}}$.

Corollary 2.42 *The group G_n has size 12^ν and the 12^ν representatives of elements from G_n (the cosets of Λ_n in $\mathbb{Z}^n$) can be taken as the elements of $([0,2] \times [0,3])^\nu$.*

Consider the mapping $\Phi : \mathbb{Z}_3^\nu \to G_n$ defined by

$$\Phi(x_1, x_2, ..., x_\nu) = (\phi(x_1), \phi(x_2), ..., \phi(x_\nu)) \ ,$$

where $\phi : \mathbb{Z}_3 \to G_2$ is a mapping defined by

$$\phi(x) = \begin{cases} (0,0) & \text{if } x = 0 \\ (1,2) & \text{if } x = 1 \\ (2,0) & \text{if } x = 2 \end{cases}.$$

It is easy to verify that both ϕ and Φ are injective group homomorphisms.

Let $\mathcal{C}$ be a ternary perfect code of length ν with $3^{\nu-t}$ codewords, and let $\Phi(\mathcal{C}) \overset{\text{def}}{=} \{\Phi(\tilde{\mathbf{c}}) : \tilde{\mathbf{c}} \in \mathcal{C}\}$. Since the elements of $\Phi(\mathcal{C})$ are representatives of elements of G_n (see Corollary 2.42) it follows that the elements of $\Phi(\mathcal{C})$ can be considered as elements in $\mathbb{Z}^n$. Let $\mathbb{T}_n \overset{\text{def}}{=} \Phi(\mathcal{C}) + \Lambda_n$.

Theorem 2.43 *The set $\mathbb{T}_n$ is a tiling of $\mathbb{Z}^n$ with Υ_n.*

Proof. Clearly, Λ_n is a lattice with period 12 and hence $\mathbb{T}_n$ is a periodic code of $\mathbb{Z}^n$ with period 12. Therefore, without loss of generality we can restrict our discussion to $\mathbb{Z}_{12}^n$. i.e. codewords of $\mathbb{T}_n \cap [0, 11]^n$. Since $|\Upsilon_n| = 2^{2\nu}3^t$ it follows that the size of the tiling $\mathbb{T}_n$ in $[0, 11]^n$, $|\mathbb{T}_n \cap [0, 11]^n|$, should be $2^{2\nu}3^{2\nu-t}$. To prove that $\mathbb{T}_n$ is a tiling of $\mathbb{Z}^n$ with Υ_n we will show that the size of $\mathbb{T}_n \cap [0, 11]^n$ is $2^{2\nu}3^{2\nu-t}$ and we will prove that each point of $\mathbb{Z}^n$ is covered by an element of $\mathbb{T}_n$.

Claim: For any two codewords $\tilde{\mathbf{c}}_1, \tilde{\mathbf{c}}_2 \in \mathcal{C}$, and two lattice points $\mathbf{y}_1, \mathbf{y}_2 \in \Lambda_n$, we have $\Phi(\tilde{\mathbf{c}}_1) + \mathbf{y}_1 \neq \Phi(\tilde{\mathbf{c}}_2) + \mathbf{y}_2$, unless $\tilde{\mathbf{c}}_1 = \tilde{\mathbf{c}}_2$ and $\mathbf{y}_1 = \mathbf{y}_2$.

Proof: Assume that $\Phi(\tilde{\mathbf{c}}_1) + \mathbf{y}_1 = \Phi(\tilde{\mathbf{c}}_2) + \mathbf{y}_2$, i.e. $\Phi(\tilde{\mathbf{c}}_1) - \Phi(\tilde{\mathbf{c}}_2) = \mathbf{y}_2 - \mathbf{y}_1$, $\tilde{\mathbf{c}}_1, \tilde{\mathbf{c}}_2 \in \mathcal{C}$ and $\mathbf{y}_1, \mathbf{y}_2 \in \Lambda_n$. Hence, $\mathbf{y}_2 - \mathbf{y}_1 = (\alpha_1, \dots, \alpha_n)$ is a lattice point and unless $\mathbf{y}_1 = \mathbf{y}_2$ we have that for at least one i, $|\alpha_i| > 2$. Denote $\Phi(\tilde{\mathbf{c}}_1) - \Phi(\tilde{\mathbf{c}}_2) = (\beta_1, \dots, \beta_n)$. By the definition of Φ, for each i, $1 \leq i \leq n$, we have $|\beta_i| \leq 2$. Therefore, $\mathbf{y}_1 = \mathbf{y}_2$ and $\Phi(\tilde{\mathbf{c}}_1) = \Phi(\tilde{\mathbf{c}}_2)$ and since Φ is an injective mapping it implies that $\tilde{\mathbf{c}}_1 = \tilde{\mathbf{c}}_2$ and the claim is proved.

The claim implies that $|\mathbb{T}_n \cap [0, 11]^n| = |\Phi(\mathcal{C})| \cdot |\Lambda_n \cap [0, 11]^n|$. Since Φ is an injective mapping we also have that $|\Phi(\mathcal{C})| = |\mathcal{C}|$. Since Λ_n has period 12 and $V(\Lambda_n) = 12^\nu$ it follows that $|\Lambda_n \cap [0, 11]^n| = 12^\nu$. Therefore,

$$|\mathbb{T}_n \cap [0, 11]^n| = |\Phi(\mathcal{C})| \cdot |\Lambda_n \cap [0, 11]^n| = |\mathcal{C}| \cdot |\Lambda_n \cap [0, 11]^n| = 3^{\nu-t}12^\nu = 2^{2\nu}3^{2\nu-t}$$

as required.

	class [(0,0)]	(0,0)	(0,3)	(2,2)	(2,1)	$\longleftarrow (x_1, x_2)$
(P.1)	$[(y_1, y_2)] = [(0,0)]$	(0,0)	(0,4)	(3,2)	(3,2)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$
(P.2)	$[(y_1, y_2)] = [(1,2)]$	(1,2)	(1,2)	(1,2)	(1,2)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$
(P.2)	$[(y_1, y_2)] = [(2,0)]$	(2,0)	(2,4)	(2,4)	(2,0)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$

	class [(1,2)]	(1,2)	(1,1)	(0,1)	(0,2)	$\longleftarrow (x_1, x_2)$
(P.2)	$[(y_1, y_2)] = [(0,0)]$	(3,2)	(3,2)	(0,0)	(0,4)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$
(P.1)	$[(y_1, y_2)] = [(1,2)]$	(1,2)	(1,2)	(1,2)	(1,2)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$
(P.2)	$[(y_1, y_2)] = [(2,0)]$	(2,4)	(2,0)	(-1,2)	(-1,2)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$

	class [(2,0)]	(2,0)	(1,3)	(2,3)	(1,0)	$\longleftarrow (x_1, x_2)$
(P.2)	$[(y_1, y_2)] = [(0,0)]$	(3,2)	(0,4)	(3,2)	(0,0)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$
(P.2)	$[(y_1, y_2)] = [(1,2)]$	(4,0)	(1,2)	(4,4)	(1,2)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$
(P.1)	$[(y_1, y_2)] = [(2,0)]$	(2,0)	(2,4)	(2,4)	(2,0)	$\longleftarrow (u_1, u_2) + (y_1, y_2)$

Table 2.1: Properties **(P.1)** and **(P.2)**.

To show that every point of $\mathbb{Z}^n$ is covered by an element of $\mathbb{T}_n$ we first partition the elements of $[0,2] \times [0,3]$ into three classes:

$$\begin{array}{l} [(0,0)] = \{(0,0), (0,3), (2,2), (2,1)\} \\ [(1,2)] = \{(1,2), (1,1), (0,1), (0,2)\} \\ [(2,0)] = \{(2,0), (1,3), (2,3), (1,0)\} \end{array} \quad ,$$

The following two properties are readily verified (as can be verified from Table 2.1).

(P.1) For each element (x_1, x_2) in a class $[(y_1, y_2)]$ there exists an element $(u_1, u_2) \in \Lambda_2$ such that $u_i + y_i \in \{x_i, x_i + 1\}$, for $i \in \{1, 2\}$.

(P.2) For each element $(x_1, x_2) \in [0,2] \times [0,3]$ and each class $[(y_1, y_2)]$ there exists an element $(u_1, u_2) \in \Lambda_2$ such that $u_i + y_i \in \{x_i - 1, x_i, x_i + 1, x_i + 2\}$, for $i \in \{1, 2\}$, and for at most one i we have $u_i + y_i \in \{x_i - 1, x_i + 2\}$.

Consider the mapping $\Psi : ([0,2] \times [0,3])^\nu \to [0,2]^\nu$ defined by

$$\Psi(x_1, x_2, ..., x_n) = (\psi(x_1, x_2), \psi(x_3, x_4), ..., \psi(x_{n-1}, x_n)) \ ,$$

where $\psi : [0,2] \times [0,3] \to \mathbb{Z}_3$ is a mapping defined by

$$\psi(x_1, x_2) = \begin{cases} 0 & \text{if } (x_1, x_2) \in [(0,0)] \\ 1 & \text{if } (x_1, x_2) \in [(1,2)] \\ 2 & \text{if } (x_1, x_2) \in [(2,0)] \end{cases} \ .$$

For a given point $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{Z}^n$ we will exhibit a point $\mathbf{x} \in \mathbb{T}_n$ which covers $\mathbf{z}$. By Corollary 2.42 we have that there exists an element

$\mathbf{y} \in \Lambda_n$ such that $\mathbf{z}+\mathbf{y} \in ([0,2] \times [0,3])^\nu$. Let $\mathbf{b} = \mathbf{z}+\mathbf{y} = (b_1, b_2, \ldots, b_n)$ and let $\Psi(\mathbf{b}) = (\alpha_1, \alpha_2, \ldots, \alpha_\nu) \in \mathbb{Z}_3^\nu$. Since $\mathcal{C}$ is a perfect code of length ν over $\mathbb{Z}_3$ it follows that there exists a codeword $(c_1, c_2, \ldots, c_\nu) \in \mathcal{C}$ such that $d_H((\alpha_1, \alpha_2, \ldots, \alpha_\nu), (c_1, c_2, \ldots, c_\nu)) \leq 1$. Let $\boldsymbol{\gamma} = \Phi(c_1, c_2, \ldots, c_\nu)$, where $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n)$. Note that by the definitions of Φ and Ψ it follows that (b_{2i-1}, b_{2i}) and $\phi(\alpha_i)$ are in the same class, for all $1 \leq i \leq \nu$. Now, we distinguish between two cases:

Case 1: If $(\alpha_1, \alpha_2, \ldots, \alpha_\nu) = (c_1, c_2, \ldots, c_\nu)$ then by property **(P.1)** there exists an element $(u_1, u_2, \ldots u_n) \in \Lambda_n$ such that $u_i + \gamma_i \in \{b_i, b_i+1\}$, for $1 \leq i \leq n$. Therefore, by Lemma 2.11 we have that $(u_1, u_2, \ldots, u_n) + (\gamma_1, \gamma_2, \ldots, \gamma_n)$ covers $\mathbf{b}$ and hence the required $\mathbf{x}$ is

$$\mathbf{x} = (u_1, u_2, \ldots u_n) + (\gamma_1, \gamma_2, \ldots, \gamma_n) - \mathbf{y}.$$

Case 2: If $(\alpha_1, \alpha_2, \ldots, \alpha_\nu) \neq (c_1, c_2, \ldots, c_\nu)$ then the Hamming distance between $(\alpha_1, \alpha_2, \ldots, \alpha_\nu)$ and $(c_1, c_2, \ldots, c_\nu)$ is one, and hence there exists exactly one coordinate s such that $\alpha_s \neq c_s$. By properties **(P.1)** and **(P.2)** there exists an element $(u_1, u_2, \ldots, u_n) \in \Lambda_n$ such that $u_i+\gamma_i \in \{b_i-1, b_i, b_i+1, b_i+2\}$, for $1 \leq i \leq n$, and for at most one i we have $u_i+\gamma_i \in \{b_i-1, b_i+2\}$. Therefore, by Lemma 2.11 we have that $(u_1, u_2, \ldots, u_n) + (\gamma_1, \gamma_2, \ldots, \gamma_n)$ covers $\mathbf{b}$ and hence the required $\mathbf{x}$ is

$$\mathbf{x} = (u_1, u_2, \ldots, u_n) + (\gamma_1, \gamma_2, \ldots, \gamma_n) - \mathbf{y}.$$

Since we proved that the size of $\mathbb{T}_n \cap [0,11]^n$ is $2^{2\nu}3^{2\nu-t}$ and each point of $\mathbb{Z}^n$ is covered by an element of $\mathbb{T}_n$, the theorem is proved.

□

Theorem 2.44 *If $\mathcal{C}$ is a linear code then $\mathbb{T}_n$ is a lattice tiling.*

Proof. Follows immediately from Theorem 2.43 and the facts that $\mathcal{C}$ is a linear code and Φ is a group homomorphism.

□

Chapter 3

Tiling with n-Dimensional Chairs and Their Applications to Asymmetric Codes

Storage media which are constrained to change of values in any location of information only in one direction were constructed throughout the last fifty years. From the older punch cards to later optical disks and modern storage such as flash memories, there was a need to design coding which enables the values of information to be increased but not to be decreased. These kind of storage medias are asymmetric memories. The codes used in these medias are called, *asymmetric codes.* Some of these memories behave as write-once memories (or WOMs in short) and coding for them was first considered in the seminal work of Rivest and Shamir [70]. This work initiated a sequence of papers on this topic, e.g. [16, 32, 33, 101, 107].

The emerging new storage media of flash memory raised many new interesting problems. Flash memory is a nonvolatile reliable memory with high storage density. Its relatively low cost makes it the ideal memory to replace the magnetic recording technology in storage media. A multilevel flash cell is electronically programmed into q threshold levels which can be viewed as elements of the set $\{0, 1, \ldots, q-1\}$. Raising the charge level of a cell is an easy operation, but reducing the charge level of a single cell requires to erase the whole block to which the cell belongs. This makes the reducing of a charge level to be a complicated, slow, and unwanted operation. Hence, the cells of the flash memory act as an asymmetric memory as long as blocks are not erased. This has motivated new research work on WOMs, e.g. [11, 79, 99, 103, 105].

Moreover, usually in programming of the cells, the charge level in a single cell of a flash memory can only to be raised, and hence the errors in a single cell are asymmetric. Asymmetric error-correcting codes were subject to extensive research due to their applications in coding for computer memories [68]. The errors in a cell of a flash memory are a new type of asymmetric errors which have limited-magnitude. Errors in this model are in one direction and are not likely to exceed a certain limit. This means that a cell in level i can be raised by an error to level j, such that $i < j \leq q-1$ and $j - i \leq \ell \leq q-1$, where ℓ is the error limited-magnitude. Asymmetric error-correcting codes with limited-magnitude were proposed in [2] and were first considered for nonvolatile memories in [9, 10]. Recently, several other papers have considered the problem, e.g. [22, 23, 48, 104].

In this work solutions for both the construction problem of asymmetric codes with limited-magnitude and the coding problem in WOMs are presented. The proposed solutions use the concept of tiling. Tiling is a well established concept in combinatorics and especially in combinatorial geometry. There are many algebraic methods related to tiling [88] and it is an important topic also in coding theory. Tiling in this work is done with a shape $\mathcal{S}$ and only shapes which form an error sphere for asymmetric limited-magnitude codes or their immediate generalization in $\mathbb{R}^n$ are considered (see Chapter 1 for definition of tiling).

As mentioned in Chapter 2, two of the most considered shapes for tiling are the cross and the semi-cross [86, 88]. These were also considered in connections to flash memories [76]. In this chapter another shape which will be called in the sequel an *n-dimensional chair* is considered. An n-dimensional chair is an n-dimensional box from which a smaller n-dimensional box is removed from one of its corners (example of a three dimensional chair is given in Figure 3.1). This is a generalization of the original concept which is an n-dimensional cube from which one vertex was removed [55]. Lattice tiling with this shape is discussed, regardless of the length of each side of the larger box and the length of each side of the smaller box.

An equivalent way to present a lattice tiling is given. This method is called a generalized splitting and it generalizes the concepts of splitting defined in [82]; and the concept of $B_h[\ell]$ sequences defined and used for construction of codes correcting asymmetric errors with limited-magnitude in [48]. Two applications of tilings with such a shape are presented. One application is for construction of codes which correct up to $n-1$ asymmetric limited-magnitude errors with any given magnitude for each cell; and a second application is for constructing WOM codes with multiple writing.

An n-dimensional chair $\mathcal{S}_{\boldsymbol{\ell},\mathbf{k}} \subset \mathbb{R}^n$, $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n)$, $\mathbf{k} = (k_1, k_2, ..., k_n) \in \mathbb{R}^n$, $0 < k_i < \ell_i$ for each i, $1 \leq i \leq n$, is an n-dimensional $\ell_1 \times \ell_2 \times \cdots \times \ell_n$ box from which an n-dimensional $k_1 \times k_2 \times \cdots \times k_n$ box was removed from one of its corners. Formally, it is defined by

$$\mathcal{S}_{\boldsymbol{\ell},\mathbf{k}} \overset{\text{def}}{=} \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \ : \ \begin{array}{c} 0 \leq x_i < \ell_i \ , \text{ and there exists a } j, \\ 1 \leq j \leq n, \text{ such that } x_j < \ell_j - k_j \end{array} \right\}.$$

The following lemma on the volume of $\mathcal{S}_{\boldsymbol{\ell},\mathbf{k}}$ is an immediate consequence of the definition.

Lemma 3.1 *If $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n)$, $\mathbf{k} = (k_1, k_2, ..., k_n)$ are two vectors in $\mathbb{R}^n$, where $0 < k_i < \ell_i$ for each i, $1 \leq i \leq n$, then*

$$|\mathcal{S}_{\boldsymbol{\ell},\mathbf{k}}| = \prod_{i=1}^{n} \ell_i - \prod_{i=1}^{n} k_i \ .$$

If $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n)$, $\mathbf{k} = (k_1, k_2, ..., k_n) \in \mathbb{Z}^n$ then the n-dimensional chair, $\mathcal{S}_{\boldsymbol{\ell},\mathbf{k}}$, is a discrete shape. In this case the formal definition of the n-dimensional chair, which considers only points of $\mathbb{Z}^n$, is

$$\mathcal{S}_{\boldsymbol{\ell},\mathbf{k}} \overset{\text{def}}{=} \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \ : \ \begin{array}{c} 0 \leq x_i < \ell_i \ , \text{ and there exists a } j, \\ 1 \leq j \leq n, \text{ such that } x_j < \ell_j - k_j \end{array} \right\}.$$

For $n = 2$, if $\ell_1 = \ell_2 = \ell$ and $k_1 = k_2 = \ell - 1$, then the chair coincides with the shape known as a corner (or a semi-cross) [85]. Examples of a two-dimensional semi-cross and a three-dimensional chair are given in Figure 3.1.

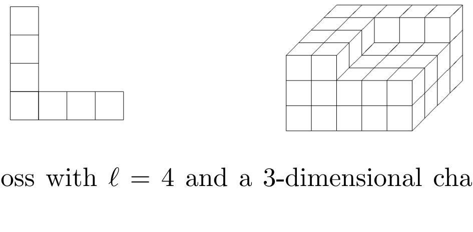

Figure 3.1: A semi-cross with $\ell = 4$ and a 3-dimensional chair with $\boldsymbol{\ell} = (5, 4, 3)$ and $\mathbf{k} = (3, 3, 1)$.

Let G be an Abelian group and let $\boldsymbol{\beta} = \beta_1, \beta_2, ..., \beta_n$ be a sequence with n elements of G. For every $\mathbf{x} = (x_1, x_2, ...x_n) \in \mathbb{Z}^n$ we define

$$\mathbf{x} \cdot \boldsymbol{\beta} = \sum_{i=1}^{n} x_i \beta_i,$$

where addition and multiplication are performed in G.

A set $\mathcal{S} \subset \mathbb{Z}^n$ *splits* an Abelian group G with a *splitting sequence* $\boldsymbol{\beta} = \beta_1, \beta_2, ..., \beta_n$, $\beta_i \in G$, for each i, $1 \leq i \leq n$, if the set $\{\mathbf{e} \cdot \boldsymbol{\beta} \ \ : \ \mathbf{e} \in \mathcal{S}\}$ contains $|\mathcal{S}|$ distinct elements from G. We will call this operation a *generalized splitting*. The splitting defined in [37] and discussed in [40, 82, 84, 86] is a special case of the generalized splitting. It was used for the shapes known as cross and semi-cross [84, 85], and quasi-cross [76]. The $B_h[\ell]$ sequences defined in [48] and discussed in [48, 50] for construction of codes which correct asymmetric errors with limited-magnitude are also a special case of the generalized splitting. These $B_h[\ell]$ sequences are modification of the well known Sidon sequences and their generalizations [63]. The generalized splitting also makes generalization for a method discussed by Varshamov [96, 97]. The generalization can be easily obtained, but to our knowledge a general and complete proven theory was not given before.

Lemma 3.2 *If Λ is a lattice packing of $\mathbb{Z}^n$ with a shape $\mathcal{S} \subset \mathbb{Z}^n$ then there exists an Abelian group G of order $V(\Lambda)$, such that $\mathcal{S}$ splits G.*

Proof. Let $G = \mathbb{Z}^n/\Lambda$ and let $\phi : \mathbb{Z}^n \to G$ be the group homomorphism which maps each element $\mathbf{x} \in \mathbb{Z}^n$ to the coset $\mathbf{x}+\Lambda$. Clearly, $|\det G| = V(\Lambda)$.

Let $\boldsymbol{\beta} = \beta_1, \beta_2, ..., \beta_n$, be a sequence defined by $\beta_i = \phi(\mathbf{e}_i)$ for each i, $1 \leq i \leq n$. Clearly, for each $\mathbf{x} \in \mathbb{Z}^n$ we have $\phi(\mathbf{x}) = \mathbf{x} \cdot \beta$.

Now assume that there exist two distinct elements $\mathbf{e}, \mathbf{f} \in \mathcal{S}$, such that

$$\phi(\mathbf{e}) = \mathbf{e} \cdot \boldsymbol{\beta} = \mathbf{f} \cdot \boldsymbol{\beta} = \phi(\mathbf{f}) \ .$$

It implies that

$$\phi(\mathbf{e} - \mathbf{f}) = (\mathbf{e} - \mathbf{f}) \cdot \boldsymbol{\beta} = \mathbf{e} \cdot \boldsymbol{\beta} - \mathbf{f} \cdot \boldsymbol{\beta} = 0 \ .$$

Since $\phi(\mathbf{x}) = 0$ if and only if $\mathbf{x} \in \Lambda$ it follows that there exists $\mathbf{x} \in \Lambda$, $\mathbf{x} \neq \mathbf{0}$, such that

$$\mathbf{e} = \mathbf{f} + \mathbf{x} \ .$$

Therefore, $\mathcal{S} \cap (\mathbf{x} + \mathcal{S}) \neq \varnothing$ which contradicts the fact that Λ is a lattice packing of $\mathbb{Z}^n$ with the shape $\mathcal{S}$.

Thus, $\mathcal{S}$ splits G with the splitting sequence $\boldsymbol{\beta}$.

□

Lemma 3.3 *Let G be an Abelian group and let $\mathcal{S}$ be a shape in $\mathbb{Z}^n$. If $\mathcal{S}$ splits G with a splitting sequence $\boldsymbol{\beta}$ then there exists a lattice packing Λ of $\mathbb{Z}^n$ with the shape $\mathcal{S}$, for which $V(\Lambda) \leq |\det G|$.*

Proof. Consider the group homomorphism $\phi : \mathbb{Z}^n \to G$ defined by

$$\phi(\mathbf{x}) = \mathbf{x} \cdot \boldsymbol{\beta}.$$

Clearly, $\Lambda = \ker(\phi)$ is a lattice and the volume of Λ, $V(\Lambda) = |\phi(\mathbb{Z}^n)| \leq |\det G|$.

To complete the proof we have to show that Λ is a packing of $\mathbb{Z}^n$ with the shape $\mathcal{S}$. Assume to the contrary that there exists $\mathbf{x} \in \Lambda$ such that $\mathcal{S} \cap (\mathbf{x} + \mathcal{S}) \neq \varnothing$. Hence, there exist two distinct elements $\mathbf{e}, \mathbf{f} \in \mathcal{S}$ such that $\mathbf{e} = \mathbf{f} + \mathbf{x}$ and therefore,

$$\phi(\mathbf{e}) = \phi(\mathbf{f} + \mathbf{x}) = \phi(\mathbf{f}) + \phi(\mathbf{x}) = \phi(\mathbf{f}).$$

Therefore, $\mathbf{e} \cdot \boldsymbol{\beta} = \mathbf{f} \cdot \boldsymbol{\beta}$, which contradicts the fact that $\mathcal{S}$ splits G with the splitting sequence $\boldsymbol{\beta}$.

Thus, Λ is a lattice packing with the shape $\mathcal{S}$.

□

Corollary 3.4 *A lattice tiling of $\mathbb{Z}^n$ with the shape $\mathcal{S} \subseteq \mathbb{Z}^n$ exists if and only if there exists an Abelian group G of order $|\mathcal{S}|$ such that $\mathcal{S}$ splits G.*

If our shape $\mathcal{S}$ is a discrete shape, i.e. $\mathcal{S}$ can be viewed as a subset of $\mathbb{Z}^n$, then an integer lattice tiling with the shape $\mathcal{S}$ is equivalent to a group splitting. In fact, both methods are complementary. If we consider the matrix $\mathcal{H} = [\beta_1 \; \beta_2 \; \cdots \; \beta_n]$ then the vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ is contained in the related lattice if and only if $\mathcal{H}\mathbf{x}^T = 0$. Therefore, $\mathcal{H}$ has some similarity to a parity-check matrix in coding theory. The representation of a lattice with its generator matrix seems to be more practical. But, sometimes it is not easy to construct one. Moreover, the splitting sequence has in many cases a nice structure and from its structure the general structure of the lattice can be found. This is the case in the next two sections. In Section 3.1 two constructions of tilings based on generalized splitting are presented. Even though the second one generalizes the first one, the mathematical structure of the first one has its own beauty and hence both constructions are given. The construction of the lattice, in $\mathbb{R}^n$, given in Section 3.2, was derived based on the structure of the lattices, in $\mathbb{Z}^n$, obtained from the construction of the splitting sequences in Section 3.1. Mihalis Kolountzakis and James H. Schmerl [53] pointed on [87], where this lattice was first proposed, and further discussed in [52, 75].

3.1 Constructions based on Generalized Splitting

In this section a construction of a tiling with n-dimensional chairs based on generalized splitting is presented. The n-dimensional chairs which are considered in this section are discrete, i.e. $\boldsymbol{\ell}, \mathbf{k} \in \mathbb{Z}^n$. First, a construction in which all the ℓ_i's are equal to ℓ, and all the k_i's are equal to $\ell - 1$ is given. This construction is generalized to a case in which all the k_i's, with a possible exception of one, have multiplicative inverses in the related Abelian group.

For the ring $G = \mathbb{Z}_q$, the ring of integers modulo q, let G^* be the multiplicative group of G formed from all the elements of G which have multiplicative inverses in G.

Lemma 3.5 *Let $n \geq 2$, $\ell \geq 2$, be two integers and let G be the ring of integers modulo $\ell^n - (\ell-1)^n$, i.e. $\mathbb{Z}_{\ell^n-(\ell-1)^n}$. Then,*

(P1) $\ell - 1$ and ℓ are elements of G^*.

(P2) $\alpha = \ell(\ell-1)^{-1}$ is an element of order n in G^*.

(P3) $1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1}$ equals to zero *in G.*

Proof.

(P1) By definition, $\ell^n - (\ell-1)^n$ is *zero* in $G = \mathbb{Z}_{\ell^n-(\ell-1)^n}$. We also have that $\ell^n - (\ell-1)^n = \sum_{i=0}^{n-1} \binom{n}{i} (\ell-1)^i = 1 + (\ell-1) \sum_{i=1}^{n-1} \binom{n}{i} (\ell-1)^{i-1}$. It follows that $(\ell-1)(-\sum_{i=1}^{n-1} \binom{n}{i} (\ell-1)^{i-1}) = 1$ in G, and hence, $\ell - 1 \in G^*$. Since $\ell^n - (\ell-1)^n$ is *zero* in G, it follows that $\ell^n = (\ell-1)^n$, and hence $\ell \in G^*$ if and only if $\ell - 1 \in G^*$.

(P2) Clearly, $\alpha^n = \ell^n((\ell-1)^{-1})^n$ and since $\ell^n = (\ell-1)^n$, it follows that $\alpha^n = (\ell-1)^n(\ell-1)^{-n} = 1$. This also implies that α has a multiplicative inverse and hence $\alpha = \ell(\ell-1)^{-1} \in G^*$.

Now, note that for each i, $1 \leq i \leq n-1$, we have $0 < \ell^i - (\ell-1)^i < \ell^n - (\ell-1)^n$. Therefore, $\ell^i \neq (\ell-1)^i$ in G and hence $\alpha^i = \ell^i((\ell-1)^{-1})^i \neq 1$. Thus, the order of α in G^* is n.

(P3) Clearly, $0 = \alpha^n - 1 = (\alpha - 1)(1 + \alpha + \alpha^2 + ... + \alpha^{n-1})$. By definition, $\alpha = \ell(\ell-1)^{-1}$ and hence $\alpha(\ell-1) = \ell$, $\alpha\ell - \alpha = \ell$, $\alpha - \alpha\ell^{-1} = 1$, $\alpha - 1 = \alpha\ell^{-1}$, $\alpha - 1 = (\ell-1)^{-1}$. Therefore, $0 = (\ell-1)^{-1}(1 + \alpha + \alpha^2 + ... + \alpha^{n-1})$ which implies that $1 + \alpha + \alpha^2 + ... + \alpha^{n-1} = 0$.

□

Theorem 3.6 *Let $n \geq 2$, $\ell \geq 2$, be two integers, $G = \mathbb{Z}_{\ell^n-(\ell-1)^n}$, and $\alpha = \ell(\ell-1)^{-1}$. Then $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$, $\boldsymbol{\ell} = (\ell, \ell, \dots, \ell)$, $\boldsymbol{k} = (\ell-1, \ell-1, \dots, \ell-1)$, splits G with the splitting sequence $\boldsymbol{\beta} = \beta_1, \beta_2, ..., \beta_n$ defined by*

$$\beta_i = \alpha^{i-1}, \quad 1 \leq i \leq n \ .$$

Proof. We will show by induction that every element in G can be expressed in the form $\mathbf{e} \cdot \boldsymbol{\beta}$, for some $\mathbf{e} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

The basis of induction is $0 = \mathbf{0} \cdot \boldsymbol{\beta}$.

For the induction step we have to show that if $x \in G$ can be presented as $x = \mathbf{e} \cdot \boldsymbol{\beta}$ for some $\mathbf{e} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ (i.e. $\mathbf{e} = (e_1, e_2, ..., e_n) \in \mathbb{Z}^n$, $0 \leq e_i \leq \ell - 1$, $1 \leq i \leq n$, and for some j, $e_j = 0$), then also $x + 1$ can be presented in the same way. In other words, $x + 1 = \tilde{\mathbf{e}} \cdot \boldsymbol{\beta}$, where $\tilde{\mathbf{e}} = (\tilde{e}_1, \tilde{e}_2, ..., \tilde{e}_n) \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

If $e_1 < \ell - 1$ and there exists $j \neq 1$ such that $e_j = 0$ then

$$x + 1 = \tilde{\mathbf{e}} \cdot \boldsymbol{\beta},$$

where $\tilde{e}_1 = e_1 + 1$ and $\tilde{e}_j = \tilde{e}$, for all $2 \leq j \leq n$, and the induction step is proved.

If $e_1 = 0$ and there is no $j \neq 1$ such that $e_j = 0$ then by Lemma 3.5 (P3) we have that $\sum_{i=1}^{n} \beta_i = 0$ and hence

$$x + 1 = (\mathbf{e} + \mathbf{e}_1 - \mathbf{1}) \cdot \beta \ ,$$

i.e. $\tilde{\mathbf{e}} = \mathbf{e} + \mathbf{e}_1 - \mathbf{1}$ is the required element of $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ and the induction step is proved.

Now, assume that $e_1 = \ell - 1$. Let j, $2 \leq j \leq n$ be the smallest index such that $e_j = 0$.

$$x + 1 = \ell\beta_1 + \sum_{i=2}^{n} e_i \beta_i.$$

Note that for each i, $1 \leq i \leq n - 1$,

$$\ell\beta_i = \ell\ell^{i-1}((\ell-1)^{-1})^{i-1} = (\ell-1)\ell^i((\ell-1)^{-1})^i = (\ell-1)\beta_{i+1}.$$

Therefore,

$$x + 1 = (\ell - 1 + e_2)\beta_2 + \sum_{i=3}^{n} e_i \beta_i.$$

If $j = 2$ then $\tilde{\mathbf{e}} = (0, \ell - 1, e_3, \dots, e_n)$ and the induction step is proved. If

$e_2 > 0$, i.e. $j > 2$, then

$$x + 1 = (e_2 - 1)\beta_2 + \ell\beta_2 + \sum_{i=3}^{n} e_i\beta_i = (e_2 - 1)\beta_2 + (\ell - 1 + e_3)\beta_3 + \sum_{i=4}^{n} e_i\beta_i.$$

By iteratively continuing in the same manner we obtain

$$x + 1 = \sum_{i=2}^{j-1}(e_i - 1)\beta_i + (\ell - 1 + e_j)\beta_j + \sum_{i=j+1}^{n} e_i\beta_i$$

and since $e_j = 0$ we have that

$$\tilde{\mathbf{e}} = (0, e_2 - 1, \ldots, e_{j-1} - 1, \ell - 1, e_{j+1}, \ldots, e_n)$$

and the induction step is proved.

Since $|\det G| = |\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}|$, it follows that the set $\{\mathbf{e} \cdot \beta \;:\; \boldsymbol{e} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}\}$ has $|\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}|$ elements.

□

Corollary 3.7 *For each $n \geq 2$ and $\ell \geq 2$ there exists a lattice tiling of $\mathbb{Z}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$, $\boldsymbol{\ell} = (\ell, \ell, \ldots, \ell)$, $\boldsymbol{k} = (\ell - 1, \ell - 1, \ldots, \ell - 1)$.*

The next theorem and its proof are generalizations of Theorem 3.6 and its proof.

Theorem 3.8 *Let $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n)$, $\boldsymbol{k} = (k_1, k_2, ..., k_n)$ be two vectors in $\mathbb{Z}^n$ such that $0 < k_i < \ell_i$ for each i, $1 \leq i \leq n$. Let $\tau = \prod_{i=1}^{n} \ell_i$, $\kappa = \prod_{i=1}^{n} k_i$, $G = \mathbb{Z}_{\tau-\kappa}$ and assume that for each i, $2 \leq i \leq n$, $k_i \in G^*$. Then $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ splits G with the splitting sequence $\boldsymbol{\beta} = \beta_1, \beta_2, ..., \beta_n$ defined by*

$$\begin{aligned}&\beta_1 = 1\\ &\beta_{i+1} = k_{i+1}^{-1}\ell_i\beta_i \quad 1 \leq i \leq n - 1\ .\end{aligned}$$

Proof. First we will show that $k_1\beta_1 = \ell_n\beta_n$. Since $\tau - \kappa$ equals zero in G, it follows that $\tau = \kappa$ in G and hence $k_1 = \ell_1\ell_2 \cdots \ell_n k_2^{-1}k_3^{-1} \cdots k_n^{-1}$. Therefore,

$$\ell_n\beta_n = \ell_n k_n^{-1}\ell_{n-1}\beta_{n-1} = \;\cdots = \ell_n\ell_{n-1}\cdots\ell_1 k_n^{-1}k_{n-1}^{-1}\cdots k_2^{-1}\beta_1 = k_1\beta_1\ .$$

As an immediate consequence from definition we have that for each i, $1 \leq i \leq n - 1$,

$$\ell_i\beta_i = k_{i+1}\beta_{i+1}\ .$$

Next, we will show that

$$(\boldsymbol{\ell} - \boldsymbol{k}) \cdot \boldsymbol{\beta} = 0. \tag{3.1}$$

$$\begin{aligned}(\boldsymbol{\ell} - \boldsymbol{k}) \cdot \boldsymbol{\beta} &= \sum_{i=1}^{n} (\ell_i - k_i)\beta_i = \sum_{i=1}^{n} (\ell_i\beta_i - k_i\beta_i) \\ &= \ell_n\beta_n - k_n\beta_n + \sum_{i=1}^{n-1} (k_{i+1}\beta_{i+1} - k_i\beta_i) \\ &= \ell_n\beta_n - k_n\beta_n + k_n\beta_n - k_1\beta_1 = 0\end{aligned}$$

Since $|\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}| = |\det G|$ it follows that to prove Theorem 3.8, it is sufficient to show that each element in G can be expressed as $\boldsymbol{e} \cdot \boldsymbol{\beta}$, for some $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$. The proof will be done by induction.

The basis of induction is $0 = \mathbf{0} \cdot \boldsymbol{\beta}$.

In the induction step we will show that if $x \in G$ can be presented as $\boldsymbol{e} \cdot \boldsymbol{\beta}$ for some $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ then the same is true for $x + 1$. In other words, $x + 1 = \tilde{\boldsymbol{e}} \cdot \boldsymbol{\beta}$, where $\tilde{\boldsymbol{e}} = (\tilde{e}_1, \tilde{e}_2, ..., \tilde{e}_n) \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

Assume

$$x = \boldsymbol{e} \cdot \boldsymbol{\beta},$$

where $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$, $0 \le e_i < \ell_i$ for each i, and there exists a j such that $e_j < \ell_j - k_j$.

If $e_1 < \ell_1 - k_1 - 1$ or if $e_1 < \ell_1 - 1$ and there exists $j \neq 1$ such that $e_j < \ell_j - k_j$, then since $\beta_1 = 1$ it follows that

$$x + 1 = \tilde{\boldsymbol{e}} \cdot \boldsymbol{\beta},$$

where $\tilde{\boldsymbol{e}} = \boldsymbol{e} + \mathbf{e}_1$. Clearly, $0 \le \tilde{e}_i \le \ell_i - 1$; $\tilde{e}_1 < \ell_1 - k_1$ if $e_1 < \ell_1 - k_1 - 1$ and otherwise $\tilde{e}_j < \ell_j - k_j$. Hence, the induction step is proved.

If $e_1 = \ell_1 - k_1 - 1$ and there is no $j \neq 1$ such that $e_j < \ell_j - k_j$ then by (3.1) we have that $(\boldsymbol{\ell} - \boldsymbol{k}) \cdot \boldsymbol{\beta} = 0$ and hence

$$x + 1 = (\boldsymbol{e} + \mathbf{e}_1 - (\boldsymbol{\ell} - \boldsymbol{k})) \cdot \boldsymbol{\beta}\ ,$$

i.e. $\tilde{\boldsymbol{e}} = \boldsymbol{e} + \mathbf{e}_1 - \boldsymbol{\ell} + \boldsymbol{k}$ is the required element of $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ and the induction step is proved.

Now, assume that $e_1 = \ell_1 - 1$. Let $2 \le j \le n$ be the smallest index such that $e_j < \ell_j - k_j$.

$$x + 1 = \ell_1\beta_1 + \sum_{i=2}^{n} e_i\beta_i = (k_2 + e_2)\beta_2 + \sum_{i=3}^{n} e_i\beta_i.$$

If $j = 2$ then $\tilde{\boldsymbol{e}} = (0, k_2 + e_2, e_3, \ldots, e_n)$ and the induction step is proved. If $e_2 \geq \ell_2 - k_2$ then

$$x + 1 = \ell_2\beta_2 + (e_2 - (\ell_2 - k_2))\beta_2 + \sum_{i=3}^{n} e_i\beta_i$$

$$= (e_2 - (\ell_2 - k_2))\beta_2 + (k_3 + e_3)\beta_3 + \sum_{i=4}^{n} e_i\beta_i.$$

By iteratively continuing in the same manner we obtain

$$x + 1 = \sum_{i=2}^{j-1}(e_i - (\ell_i - k_i))\beta_i + (k_j + e_j)\beta_j + \sum_{i=j+1}^{n} e_i\beta_i \ ,$$

and since $e_j < \ell_j - k_j$ it follows that

$$\tilde{\boldsymbol{e}} = (0, e_2 - \ell_2 + k_2, \ldots, e_{j-1} - \ell_{j-1} + k_{j-1}, k_j + e_j, e_{j+1}, \ldots, e_n)$$

is the element of $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$, and the induction step is proved.

□

Corollary 3.9 *Let $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n)$, $\boldsymbol{k} = (k_1, k_2, ..., k_n)$ be two vectors in $\mathbb{Z}^n$ such that $0 < k_i < \ell_i$ for each i, $1 \leq i \leq n$. Let $\tau = \prod_{i=1}^{n} \ell_i$ and assume that $\gcd(k_i, \tau) = 1$ for at least $n - 1$ of the k_i's. Then there exists a lattice tiling of $\mathbb{Z}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.*

3.2 Tiling based on a Lattice

Next, lattice tiling of $\mathbb{R}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \subset \mathbb{R}^n$, where $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n)$, $\boldsymbol{k} = (k_1, k_2, ..., k_n) \in \mathbb{R}^n$, is considered. As mentioned above, Mihalis Kolountzakis and James H. Schmerl pointed on [52, 75, 87], where this lattice tiling can be found. For completeness and since the presented proof is slightly different, this part is included in this work. The following lemma will be useful in the proof of the next theorem.

Lemma 3.10 *Let $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$. Then, $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \cap (\mathbf{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}) \neq \varnothing$ if and only if $|x_i| < \ell_i$, for $1 \leq i \leq n$, and there exist integers j and r, $1 \leq j, r \leq n$, such that $x_j < \ell_j - k_j$ and $-(\ell_r - k_r) < x_r$.*

Proof. Assume first that $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \cap (\boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{x}}) \neq \varnothing$, i.e. there exists an $\mathbf{a} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \cap (\boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}|})$, $\mathbf{a} = (a_1, a_2, ..., a_n)$. By the definition of $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ it follows that

$$0 \le a_i < \ell_i \ , \quad \text{for each } i, \ 1 \le i \le n \ , \tag{3.2}$$

and there exists a j such that

$$a_j < \ell_j - k_j \ . \tag{3.3}$$

Similarly, for $\boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$ we have

$$x_i \le a_i < x_i + \ell_i \ , \quad \text{for each } i, \ 1 \le i \le n \ , \tag{3.4}$$

and there exists an r such that

$$a_r < x_r + \ell_r - k_r \ . \tag{3.5}$$

It follow from (3.2) and (3.4) that $x_i \le a_i < \ell_i$ and $-\ell_i \le a_i - \ell_i < x_i$ for each i, $1 \le i \le n$. Hence, $|x_i| < \ell_i$ for each i, $1 \le i \le n$. It follow from (3.3) and (3.4) that $x_j \le a_j < \ell_j - k_j$. It follows from (3.5) and (3.2) that $x_r > a_r - (\ell_r - k_r) \ge -(\ell_r - k_r)$.

Now, let $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ such that $|x_i| < \ell_i$ for each i, $1 \le i \le n$, and there exist j, r such that $x_j < \ell_j - k_j$ and $x_r > -(\ell_r - k_r)$. Consider the point $\mathbf{a} = (a_1, a_2, ..., a_n) \in \mathbb{R}^n$, where $a_i = \max\{x_i, 0\}$.

By definition, for each i, $1 \le i \le n$,

$$0 \le a_i < \ell_i$$

and $a_j < \ell_j - k_j$. Hence, $\mathbf{a} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

Clearly, if $x_i < 0$ then $a_i = 0$ and if $x_i \ge 0$ then $a_i = x_i$. In both cases, since $0 < x_i + \ell_i$, it follows that we have

$$x_i \le a_i < x_i + \ell_i \ .$$

We also have $0 < x_r + \ell_r - k_r$, and therefore $x_r \le a_r < x_r + \ell_r - k_r$. Hence, $\boldsymbol{a} \in \boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

Thus, $\boldsymbol{a} \in \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \cap (\boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}})$, i.e. $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \cap (\boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}) \neq \varnothing$.

□

The next Theorem is a generalization of Corollary 3.9.

Theorem 3.11 *Let $\boldsymbol{\ell} = (\ell_1, \ell_2, ..., \ell_n) \in \mathbb{R}^n$ and $\boldsymbol{k} = (k_1, k_2, ..., k_n) \in \mathbb{R}^n$, $0 < k_i < \ell_i$, for all $1 \le i \le n$. Let Λ be the lattice generated by the matrix*

$$\mathbf{G} \overset{\text{def}}{=} \begin{bmatrix} \ell_1 & -k_2 & 0 & 0 & \dots & 0 \\ 0 & \ell_2 & -k_3 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \ell_{n-2} & -k_{n-1} & 0 \\ 0 & 0 & \dots & 0 & \ell_{n-1} & -k_n \\ -k_1 & 0 & \dots & 0 & 0 & \ell_n \end{bmatrix} .$$

Then Λ is a lattice tiling of $\mathbb{R}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

Proof. It is easy to verify that $V(\Lambda) = |\det \mathbf{G}| = \prod_{i=1}^n \ell_i - \prod_{i=1}^n k_i = |\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}|$. We will use Lemma 1.11 to show that Λ is a tiling of $\mathbb{R}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$. For this, it is sufficient to show that Λ is a packing of $\mathbb{R}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

Let $\mathbf{x} \in \Lambda$, $\mathbf{x} \neq \mathbf{0}$, and assume to the contrary that $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}} \cap (\boldsymbol{x} + \mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}) \neq \varnothing$. Since $\boldsymbol{x} \in \Lambda$ it follows that there exist integers $\lambda_0, \lambda_1, \lambda_2, ..., \lambda_n = \lambda_0$, not all zeros, such that $x_i = \lambda_i \ell_i - \lambda_{i-1} k_i$, for every i, $1 \leq i \leq n$. By Lemma 3.10 we have that for each i, $1 \leq i \leq n$,

$$-\ell_i < \lambda_i \ell_i - \lambda_{i-1} k_i < \ell_i \ ,$$

i.e.

$$\frac{\lambda_{i-1} k_i}{\ell_i} - 1 < \lambda_i < \frac{\lambda_{i-1} k_i}{\ell_i} + 1 \ .$$

Since λ_i is an integer it follows that $\lambda_i = \left\lfloor \frac{\lambda_{i-1} k_i}{\ell_i} \right\rfloor$ or $\lambda_i = \left\lceil \frac{\lambda_{i-1} k_i}{\ell_i} \right\rceil$. For each i, $0 \leq i \leq n-1$, if $\lambda_i = \rho \geq 0$ then since $k_{i+1} < \ell_{i+1}$ we have that

$$0 \leq \left\lfloor \frac{\rho k_{i+1}}{\ell_{i+1}} \right\rfloor \leq \lambda_{i+1} \leq \left\lceil \frac{\rho k_{i+1}}{\ell_{i+1}} \right\rceil \leq \rho \ .$$

Hence,

$$0 \leq \lambda_{i+1} \leq \lambda_i \ . \tag{3.6}$$

Similarly, if $\lambda_i \leq 0$ we have that

$$\lambda_i \leq \lambda_{i+1} \leq 0 \ .$$

If $\lambda_0 \geq 0$ then by (3.6) we have

$$\lambda_0 = \lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_1 \leq \lambda_0 \ ,$$

and hence $\lambda_i = \rho$ for each i, $1 \leq i \leq n$. Similarly, we have $\lambda_i = \rho$ for each i, $1 \leq i \leq n$ if $\lambda_0 \leq 0$. If $\rho > 0$ then since ρ is an integer we have that $x_i = \rho(\ell_i - k_i) \geq \ell_i - k_i$, for each i, $1 \leq i \leq n$. Hence, there is no j such that

$x_j < \ell_j - k_j$, which contradicts Lemma 3.10. Similarly, if $\rho < 0$ then for each i, $1 \leq i \leq n$, $x_i = \rho(\ell_i - k_i) \leq -(\ell_i - k_i)$, and hence there is no r such that $x_r > -(\ell_j - k_j)$, which contradicts Lemma 3.10. Therefore, $\rho = 0$, i.e. for each i, $0 \leq i \leq n$, $\lambda_i = 0$, a contradiction. Hence, Λ is a lattice packing of $\mathbb{R}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$

Thus, by Lemma 1.11, Λ is a lattice tiling of $\mathbb{R}^n$ with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$.

□

Remark 3.1 *Note, that the construction (Theorem 3.11) is based on lattices covers all the parameters of integers which are not covered in Section 3.1.*

3.2.1 Asymmetric Errors with Limited-magnitude

The first application for a tiling of $\mathbb{Z}^n$ with an n-dimensional chair is in construction of codes of length n which correct asymmetric errors with limited-magnitude.

Let $Q = \{0, 1, \ldots, q-1\}$ be an alphabet with q letters. A *code* $\mathcal{C}$ of *length* n over the alphabet Q is a subset of Q^n. A vector $\boldsymbol{e} == (e_1, e_2, \ldots, e_n)$ is a *t-asymmetric-error with limited-magnitude* ℓ if the Hamming weight of $\mathbf{e}$, $w_H(\boldsymbol{e})$ (i.e. the number of nonzero entries in $\mathbf{e}$), is at most t and $0 \leq e_i \leq \ell$ for each $1 \leq i \leq n$. The sphere $\mathcal{S}(n, t, \ell)$ is the set of all t- asymmetric-errors with limited-magnitude ℓ. A code $\mathcal{C} \subseteq Q^n$ can correct t-asymmetric-errors with limited-magnitude ℓ if for any two codewords $\boldsymbol{x}, \boldsymbol{y}$, and any two t-asymmetric-errors with limited-magnitude ℓ, $\boldsymbol{e}$, $\boldsymbol{f}$, such that $\boldsymbol{x} + \boldsymbol{e} \in Q^n$, $\boldsymbol{y} + \boldsymbol{f} \in Q^n$, we have that $\boldsymbol{x} + \boldsymbol{e} \neq \boldsymbol{y} + \boldsymbol{f}$.

The size of the sphere $\mathcal{S}(n, t, \ell)$ is easily computed.

Lemma 3.12 $|\mathcal{S}(n, t, \ell)| = \sum_{i=0}^{t} \binom{n}{i} \ell^i$.

Corollary 3.13 $|\mathcal{S}(n, n-1, \ell)| = (\ell + 1)^n - \ell^n$.

For simplicity it is more convenient to consider the code $\mathcal{C}$ as a subset of $\mathbb{Z}_q^n$, where all the additions are performed modulo q. Recall, that a code $\mathcal{C}$ can be viewed also as a subset of $\mathbb{Z}^n$ formed by the expanded code of $\mathcal{C}$, $E(\mathcal{C})$. Note, in this code there is a wrap around (of the alphabet) which does not exist if the alphabet is Q, as in the previous code.

A linear code $\mathcal{C}$, over $\mathbb{Z}_q^n$, which corrects t-asymmetric-errors with limited-magnitude ℓ, viewed as a subset of $\mathbb{Z}^n$, is equivalent to an integer lattice packing of $\mathbb{Z}^n$ with the shape $\mathcal{S}(n, t, \ell)$. Therefore, we will call this lattice a *lattice code*.

Let $\mathcal{A}(n, t, \ell)$ denote the set of lattice codes in $\mathbb{Z}^n$ which correct t-asymmetric-errors with limited-magnitude ℓ. A code $\mathcal{L} \in \mathcal{A}(n, t, \ell)$ is called *perfect* if it forms a lattice tiling with the shape $\mathcal{S}(n,t,\ell)$. By Corollary 3.4 we have

Corollary 3.14 *A perfect lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ exists if and only if there exists an Abelian group G of order $|\mathcal{S}(n,t,\ell)|$ such that $\mathcal{S}(n,t,\ell)$ splits G.*

A code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ is formed as an extension of a code over $\mathbb{Z}_q^n$. Assume we want to form a code $\mathcal{C} \subseteq \Sigma^n$, where $\Sigma \overset{\text{def}}{=} \{0,1,\ldots,\sigma-1\}$, which corrects t asymmetric errors with limited-magnitude ℓ. Assume that a construction with a large linear code $\mathcal{C} \subset \Sigma^n$ does not exist. One can take a lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ over an alphabet with q letters $q > \sigma$. Then a code over the alphabet Σ is formed by $\mathcal{C} \overset{\text{def}}{=} \mathcal{L} \cap \Sigma^n$. Note that the code $\mathcal{C}$ is usually not linear. This is a simple construction which always works. Of course, we expect that there will be many alphabets in which better constructions can be found.

There exists a perfect lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ for various parameters with $t = 1$ [48, 50]. Such codes also exist for $t = n$ and all $\ell \geq 1$ and for the parameters of the Golay codes and the binary repetition codes of odd length [58].

The existence of perfect codes which correct $(n-1)$-asymmetric-errors with limited magnitude ℓ was proved in [50]. The related sphere $\mathcal{S}(n,n-1,\ell)$ is an n-dimensional chair $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$, where $\boldsymbol{\ell} = (\ell+1,\ell+1,\ldots,\ell+1)$ and $\boldsymbol{k} = (\ell,\ell,\ldots,\ell)$. Sections 3.1 and 3.2 provide constructions for such codes with simpler description and simpler proofs that these codes are such perfect codes.

In fact, the constructions in these sections provide tilings of many other related shapes. More than that, there might be scenarios in which different flash cells can have different limited magnitude. For example, if for some cells we want to increase the number of charge levels. In this case we might need a code which correct asymmetric errors with different limited magnitudes for different cells. Assume that for the i-th cell the limited magnitude is ℓ_i. Our lattice tiling with $\mathcal{S}_{\boldsymbol{\ell},\boldsymbol{k}}$, $\boldsymbol{\ell} = (\ell_1+1,\ell_2+1,\ldots,\ell_n+1) \in \mathbb{Z}^n$, $\boldsymbol{k} = (\ell_1,\ell_2,\ldots,\ell_n)$, produces the required perfect code for this scenario.

3.3 Nonexistence of some Perfect Codes

Next, we ask whether perfect codes, which correct asymmetric errors with limited-magnitude, exist for $t = n-2$. Unfortunately, such codes cannot exist. The proof for this claim is the goal of this section. Most of the proof is devoted to the case in which the limited magnitude ℓ is equal to one. We conclude the section with a proof for $\ell > 1$.

For a word $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$, we define

$$N_+(\boldsymbol{x}) = |\{x_i \mid x_i > 0\}|, \qquad N_-(\boldsymbol{x}) = |\{x_i \mid x_i < 0\}|.$$

We say that a codeword $\boldsymbol{x} \in \mathcal{L}$, $\mathcal{L} \in \mathcal{A}(n, t, \ell)$, *covers* a word $\boldsymbol{y} \in \mathbb{Z}^n$ if there exists an element $\boldsymbol{e} \in \mathcal{S}(n, t, \ell)$ such that $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$.

Lemma 3.15 *Let $\mathcal{L} \in \mathcal{A}(n, t, \ell)$, and assume that there exists $\boldsymbol{x} \in \mathcal{L}$, $\boldsymbol{x} = x_1, x_2, \ldots, x_n)$, $\boldsymbol{x} \neq \mathbf{0}$, such that $|x_i| \leq \ell$, for every i, $1 \leq i \leq n$. Then, $N_+(\boldsymbol{x}) \geq t + 1$ or $N_-(\boldsymbol{x}) \geq t + 1$.*

Proof. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathcal{L}$, $\boldsymbol{x} \neq \mathbf{0}$, such that $|x_i| \leq \ell$, for every i, $1 \leq i \leq n$. Assume to the contrary that $N_+(\boldsymbol{x}) \leq t$ and $N_-(\boldsymbol{x}) \leq t$. Let $\boldsymbol{e}^+ = (e_1^+, e_2^+, \ldots, e_n^+)$ where $e_i^+ = \max\{x_i, 0\}$ and $\boldsymbol{e}^- = (e_1^-, e_2^-, \ldots, e_n^-)$ where $e_i^- = \max\{-x_i, 0\}$. Clearly, $\boldsymbol{e}^+$, $\boldsymbol{e}^- \in \mathcal{S}(n, t, \ell)$ and $\boldsymbol{x} + \boldsymbol{e}^- = \boldsymbol{e}^+$.

Therefore, $\mathcal{S}(n, t, \ell) \cap (\boldsymbol{x} + \mathcal{S}(n, t, \ell)) \neq \varnothing$, which contradicts the fact that $\mathcal{L} \in \mathcal{A}(n, t, \ell)$. Thus, $N_+(\boldsymbol{x}) \geq t + 1$ or $N_-(\boldsymbol{x}) \geq t + 1$.

□

Lemma 3.16 *Let $\mathcal{L} \in \mathcal{A}(n, n-2, \ell)$ be a lattice code. The word $\mathbf{1} \in \mathbb{Z}^n$, the all-one vector, can be covered only by a codeword of the form $\mathbf{1} - \lambda \cdot \mathbf{e}_i$, for some i, $1 \leq i \leq n$; where λ is an integer, $0 \leq \lambda \leq \ell$.*

Proof. Assume that $\boldsymbol{x} \in \mathcal{L}$ is the codeword that covers $\mathbf{1}$. Then there exists $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathcal{S}(n, n-2, \ell)$ such that $\boldsymbol{x} + \boldsymbol{e} = \mathbf{1}$, i.e. $x_i = 1 - e_i$ and therefore, $1 - \ell \leq x_i \leq 1$ for each i, $1 \leq i \leq n$. Since $w_H(\boldsymbol{e}) \leq n - 2$ it follows that there are at least two entries which are equal to one in $\boldsymbol{x}$. By Lemma 3.15, it follows that $N_+(\boldsymbol{x}) \geq n - 1$. Hence, there are at least $n - 1$ entries of $\boldsymbol{x}$ which are equal to one. Therefore, $\boldsymbol{x} = \mathbf{1} - \lambda \mathbf{e}_i$ for some i, $1 \leq i \leq n$; where λ is an integer, $0 \leq \lambda \leq \ell$.

□

Lemma 3.17 *Let $\mathcal{L} \in \mathcal{A}(n, n-2, \ell)$ be a lattice code. For every j, $1 \leq j \leq n$, the word $\boldsymbol{w}_j = \mathbf{1} - \mathbf{e}_j$ can be covered only by a codeword of the form $\mathbf{1} - \lambda \mathbf{e}_j$, where λ is an integer, $1 \leq \lambda \leq \ell + 1$.*

Proof. Assume that $\boldsymbol{x} \in \mathcal{L}$ is a codeword that covers $\boldsymbol{w}_j$. Then there exists $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathcal{S}(n, n-2, \ell)$ such that $\boldsymbol{x} + \boldsymbol{e} = \boldsymbol{w}_j$. Clearly, $x_j = -e_j \leq 0$, and for each $i \neq j$, $x_i = 1 - e_i$ and therefore $-\ell \leq x_i \leq 1$ for each i, $1 \leq i \leq n$. Since $w_H(\boldsymbol{e}) \leq n - 2$ it follows that there are at most

$n-2$ negative coordinates in $\boldsymbol{x}$. Therefore, by Lemma 3.15, it follows that $N_+(\boldsymbol{x}) \geq n-1$. Hence, there are at least $n-1$ coordinates of $\boldsymbol{x}$ which are equal to *one*. Thus, $\boldsymbol{x} = \mathbf{1} - \lambda \mathbf{e}_j$, where $1 \leq \lambda \leq \ell + 1$.

□

Lemma 3.18 *If there exists a perfect lattice code in* $\mathcal{A}(n, n-2, \ell)$ *then* $|\mathcal{S}(n, n-2, \ell)|$ *divides* $(\ell+1)^{n-2}(\ell+1+\lambda(n-2-\ell))$ *for some integer* λ, $0 \leq \lambda \leq \ell$.

Proof. Let $\mathcal{L} \in \mathcal{A}(n, n-2, \ell)$ be a perfect lattice code. By Lemma 3.16 and w.l.o.g we can assume that $\mathbf{1}$ is covered by the codeword $\boldsymbol{x} = \mathbf{1} - \lambda \mathbf{e}_n$, where $0 \leq \lambda \leq \ell$. Combining this with Lemma 3.17 we deduce that for all i, $1 \leq i \leq n-1$, the word $\boldsymbol{w}_i = \mathbf{1} - \mathbf{e}_i$ is covered by the codeword $\boldsymbol{y}_i = \mathbf{1} - (\ell+1) \cdot \mathbf{e}_i$ ($\boldsymbol{y}_i$ cannot be equal $\mathbf{1} - \alpha \mathbf{e}_i$, $1 \leq \alpha \leq \ell$ since it would cover $\mathbf{1}$ which is already covered by $\boldsymbol{x}$). We have n distinct codewords in $\mathcal{L}$, and since $\mathcal{L}$ is a lattice, the lattice $\mathcal{L}'$ generated by the set $\{\boldsymbol{x}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{n-1}\}$ is a sublattice of $\mathcal{L}$, and therefore $V(\mathcal{L}) = |\mathcal{S}(n, n-2, \ell)|$ divides $V(\mathcal{L}')$. Let $\mathbf{G}$ be the matrix whose rows are $\boldsymbol{x}, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{n-1}$.

$$\det \mathbf{G} = \begin{vmatrix} 1 & 1 & 1 & \ldots & 1 & 1-\lambda \\ -\ell & 1 & 1 & \ldots & 1 & 1 \\ 1 & -\ell & 1 & \ldots & 1 & 1 \\ 1 & 1 & -\ell & \ddots & 1 & 1 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \ldots & -\ell & 1 \end{vmatrix}$$

Subtracting the first row from every other row, we obtain the determinant

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 & 1-\lambda \\ -(\ell+1) & 0 & 0 & \ldots & 0 & \lambda \\ 0 & -(\ell+1) & 0 & \ldots & 0 & \lambda \\ 0 & 0 & -(\ell+1) & \ddots & 0 & \lambda \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & -(\ell+1) & \lambda \end{vmatrix}.$$

Subtracting the first column from all the other columns, except from the last one, we obtain the determinant

$$\begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 1-\lambda \\ -(\ell+1) & \ell+1 & \ell+1 & \dots & \ell+1 & \lambda \\ 0 & -(\ell+1) & 0 & \dots & 0 & \lambda \\ 0 & 0 & -(\ell+1) & \ddots & 0 & \lambda \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -(\ell+1) & \lambda \end{vmatrix} .$$

Finally, replacing the second row by the sum of all the rows, except for the first one, we obtain the determinant

$$\begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 1-\lambda \\ -(\ell+1) & 0 & 0 & \dots & 0 & \lambda(n-1) \\ 0 & -(\ell+1) & 0 & \dots & 0 & \lambda \\ 0 & 0 & -(\ell+1) & \ddots & 0 & \lambda \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -(\ell+1) & \lambda \end{vmatrix} .$$

Now, it is easy to verify that $V(\mathcal{L}') = |\det \mathbf{G}| = |\lambda(n-1)(\ell+1)^{n-2} + (1-\lambda)(\ell+1)^{n-1}| = |(\ell+1)^{n-2}(\ell+1+\lambda(n-2-\ell))|$.

□

Theorem 3.19 *There are no perfect lattice codes in $\mathcal{A}(n, n-2, 1)$ for all $n \geq 4$.*

Proof. By Lemma 3.18, it is sufficient to show that $|\mathcal{S}(n, n-2, 1)| = 2^n - n - 1$ does not divide $2^{n-2}(2 + \lambda(n-3))$, for $\lambda = 0, 1$.

If $\lambda = 0$ then we have to show that $2^n - n - 1$ does not divide 2^{n-1}. It can be readily verified that $2^n - n - 1 > 2^{n-1}$ for all $n > 3$, which proves the claim.

If $\lambda = 1$ then we have to show that $2^n - n - 1$ does not divide $2^{n-2}(n-1)$. If $2^r = \gcd(2^n - n - 1, 2^{n-2})$ then $0 \leq r \leq \log_2(n+1)$. Hence, we have to show that $2^{n-r} - \frac{n+1}{2^r}$ does not divide $n-1$. We will show that for all $n \geq 7$, $2^{n-r} - \frac{n+1}{2^r} > n-1$. It is easy to verify that

$$2^{n-r} - \frac{n+1}{2^r} \geq 2^{n-\log_2(n+1)} - (n+1) = \frac{2^n}{n+1} - n - 1 .$$

Therefore, it is sufficient to show that

$$\frac{2^n}{n+1} - n - 1 > n - 1 \ ,$$

or equivalently

$$2^n > 2n(n+1).$$

This is simply proved by induction on n for all $n \geq 7$.

To complete the proof we should only verify that for $n = 4$, 5, and 6, we have that $2^n - n - 1$ does not divide $2^{n-2}(n-1)$.

□

Theorem 3.20 *There are no perfect lattice codes in $\mathcal{A}(n, n-2, \ell)$ if $n \geq 4$ and $\ell \geq 2$.*

Proof. Let $n \geq 4$ and $\ell \geq 2$ and assume to the contrary, that there exists a perfect lattice code $\mathcal{L} \in \mathcal{A}(n, n-2, \ell)$. Without loss of generality, we can assume by Lemma 3.16 that the word $\mathbf{1} \in \mathbb{Z}^n$ is covered by a codeword $\boldsymbol{x} = \mathbf{1} - \lambda \mathbf{e}_n$, where λ is an integer, $0 \leq \lambda \leq \ell$. From the proof of Lemma 3.18 we have that for all i, $1 \leq i \leq n-1$, the word $\boldsymbol{w}_i = \mathbf{1} - \mathbf{e}_i$ is covered by the codeword $\boldsymbol{y}_i = \mathbf{1} - (\ell+1) \cdot \mathbf{e}_i$. Therefore, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) = \boldsymbol{y}_1 + \boldsymbol{y}_2 = 2 \cdot \mathbf{1} - (\ell+1) \cdot \mathbf{e}_1 - (\ell+1) \cdot \mathbf{e}_2$ is a codeword Clearly, $y_1 = y_2 = 2 - (\ell+1) = 1 - \ell$ and since $\ell \geq 2$ it follows that for all i, $1 \leq i \leq n$, $|y_i| \leq \ell$. Moreover, $N_-(\boldsymbol{x}) = 2 \leq n-2$ and $N_+(\boldsymbol{x}) = n-2$, which contradicts Lemma 3.15. Thus, if $n \geq 4$ and $\ell \geq 2$, then there are no perfect lattice codes in $\mathcal{A}(n, n-2, \ell)$.

□

Combining Theorems 3.19 and 3.20 we obtain the main result of this section.

Corollary 3.21 *There are no perfect lattice codes in $\mathcal{A}(n, n-2, \ell)$ if $n \geq 4$ for any limited magnitude $\ell \geq 1$.*

The existence of perfect lattice codes in $\mathcal{A}(n, n-1, \ell)$ and their nonexistence in $\mathcal{A}(n, n-2, \ell)$ might give an evidence that such perfect codes do not exist in $\mathcal{A}(n, n-\epsilon, \ell)$ for $\ell \geq 1$ and some $\epsilon > 1$. It would be interesting to prove such a claim for $n \geq 4$ and $2 \leq \epsilon \leq \lfloor \frac{n}{2} \rfloor$.

3.4 Application to Write-Once Memories

A second possible application for a tiling of $\mathbb{Z}^n$ with an n-dimensional chair is in constructions of multiple writing in n cells write-once memories. Each cell has q charge levels $\{0, 1, \ldots, q-1\}$. A letter from an alphabet of size σ,

$\Sigma = \{0, 1 \ldots, \sigma - 1\}$, is written into the n cells as many times as possible. In each round the charge level in each cell is greater than or equal to the charge level in the previous round. It is desired that the number of rounds for which we can guarantee to write a new symbol from Σ will be maximized.

An optimal solution for the problem can be described as follows. Let A be an $q \times q \times \cdots \times q$ n-dimensional array. Let $\psi : A \to \Sigma$ be a coloring of the array A with the σ alphabet letters. The rounds of writing and raising the charge levels of the n cells can be described in terms of the coloring ψ of the array A. If in the first round the symbol s_1 is written and the charge level in cell i is raised to c_i^1, $1 \leq i \leq n$, then the color in position $(c_1^1, c_2^1, \ldots, c_n^1)$ is s_1. Therefore, we have to find a coloring function ψ such that the number of rounds in which a new symbol can be written will be maximal.

Cassuto and Yaakobi [11] have found that using a coloring ψ based on a lattice tiling Λ with a two-dimensional chair provides the best known writing strategy when there are two cells. A coloring $\tilde{\psi}$ of $\mathbb{Z}^n$ based on a lattice tiling Λ with a shape $\mathcal{S}$ has $|\mathcal{S}|$ colors. The lattice have $|\mathcal{S}|$ cosets, and hence $|\mathcal{S}|$ coset representatives, $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{|\mathcal{S}|-1}$. The points in $\mathbb{Z}^n$ of the coset $\boldsymbol{x}_i + \Lambda$ are colored with the i-th letter of Σ. Now, the coloring of entry $(x_1, x_2, \ldots, x_n)$ of A given by ψ is equal to the color of the point $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ given by the coloring $\tilde{\psi}$. The method given in [11] suggests that a generalization using coloring based on tiling of $\mathbb{Z}^n$ with an n-dimensional chair will be a good strategy for WOM codes with n cells [102]. The analysis with two cells, i.e. two-dimensional tiling was discussed with more details in [11]. The analysis for the n-dimensional case will be discussed in research work which follows by the same authors and another group as well [102].

Part II

Permutation Codes for Rank Modulation

Chapter 4

Preliminaries: Permutations, Multipermutations, and the Kendall's τ-Metric

Basic definitions and properties for permutations, multipermutations, and the Kendall's τ-metric are given in this chapter. These basic concepts will be used throughout this part of the dissertation.

Let S_n be the set of all permutations on the set of n elements $[n]\overset{\text{def}}{=}\{1,2,\ldots,n\}$. For $a,b \in \mathbb{Z}$, where $a<b$, the set $\{a,a+1,\ldots,b\}$ is denoted by $[a,b]$ and the set of all permutations on $[a,b]$ is denoted by $S([a,b])$. A permutation $\sigma \in S_n$ is denoted by $\sigma = [\sigma(1),\sigma(2),\ldots,\sigma(n)]$. For two permutations $\sigma,\pi \in S_n$, their multiplication $\pi \circ \sigma$ is defined as the composition of σ on π, namely, $\pi \circ \sigma(i) = \sigma(\pi(i))$, for all $1 \leq i \leq n$. Under this operation, the set S_n is a noncommutative group known as the symmetric group of order $n!$. The identity permutation of S_n is denoted by $\varepsilon = [1,2,\ldots,n]$.

A more general concept is *multipermutations*, which is also known as permutations with repetitions. A *multiset* $\mathcal{M} = \{v_1^{m_1}, v_2^{m_2}, \cdots, v_\ell^{m_\ell}\}$ is a collection of the elements $\{v_1,v_2,\ldots,v_\ell\}$ in which v_i appears m_i times for each i, $1 \leq i \leq \ell$. The elements of $\{v_1,v_2,\ldots,v_\ell\}$ are called *ranks* while for every i, $1 \leq i \leq \ell$, the positive integer m_i is called the *multiplicity* of the ith rank. If $m_1 = m_2 = \cdots = m_\ell = m$ then $\mathcal{M}$ is called a *balanced multiset*. A multipermutation on the multiset $\mathcal{M}$ is an ordering of all the elements of $\mathcal{M}$. Note, that a permutation is a special case of a multipermutation. By abuse of notation we denote a multiplication σ of length n by $\sigma = [\sigma(1),\sigma(2),\ldots,\sigma(n)]$, $n = \sum_{i=1}^{\ell} m_i$, where it should be clear from the context whether σ is a permutation or not. For example, if $\mathcal{M} = \{1^2,2^3,3\}$, then $\sigma = [1,2,2,1,3,2]$ is a multipermutation on $\mathcal{M}$. We denote by $S(\mathcal{M})$

the set of all multipermutations on $\mathcal{M}$. The size of $S(\mathcal{M})$ is equal to $\frac{n!}{\Pi_{i=1}^{\ell} m_i!}$.

Given a multipermutation $\sigma \in S(\mathcal{M})$, an *adjacent transposition*, $(i, i+1)$, is an exchange of the two distinct adjacent elements $\sigma(i), \sigma(i+1)$ in σ, for some $1 \leq i \leq n-1$. The result is the multipermutation $\pi = [\sigma(1), \dots, \sigma(i-1), \sigma(i+1), \sigma(i), \sigma(i+2), \dots, \sigma(n)]$. If σ is a permutation then the permutation π can also be written as $\pi = (i, i+1) \circ \sigma$, where $(i, i+1)$ is the cycle decomposition of the permutation $[1, 2, \dots, i-1, i+1, i, i+2, \dots, n]$. Two adjacent transpositions $(i, i+1)$ and $(j, j+1)$ are called *disjoint* if either $i+1 < j$ or $j+1 < i$.

For two multipermutations $\sigma, \pi \in S_n$, the Kendall's τ-distance between σ and π, $d_K(\sigma, \pi)$, is defined as the minimum number of adjacent transpositions needed to transform σ into π.

Example 4.1 *If* $\sigma = [1,1,2,2]$ *and* $\pi = [2,1,2,1]$*, then* $d_K(\sigma, \pi) = 3$*, since at least three adjacent transpositions are required to change the multipermutation* σ *to* π*:* $[1,1,2,2] \rightarrow [1,2,1,2] \rightarrow [2,1,1,2] \rightarrow [2,1,2,1]$.

The Kendall's τ-metric was originally defined for permutations [21, 46]. For two permutations $\sigma, \pi \in S_n$ it is known [44, 51] that $d_K(\sigma, \pi)$ can be expressed as

$$d_K(\sigma, \pi) = |\{(i,j) : \sigma^{-1}(i) < \sigma^{-1}(j),\ \pi^{-1}(i) > \pi^{-1}(j)\}|. \tag{4.1}$$

For $\sigma \in S_n$, the Kendall's τ-weight of σ, $w_K(\sigma)$, is defined as the Kendall's τ-distance between σ and the identity permutation ε. The Kendall's τ-metric on S_n is right invariant [20], i.e. for every three permutations $\sigma, \pi, \rho \in S_n$, we have $d_K(\sigma, \pi) = d_K(\sigma \circ \rho, \pi \circ \rho)$.

For a multipermutation $\sigma \in S(\mathcal{M})$, where $\mathcal{M} = \{v_1^{m_1}, v_2^{m_2}, \dots, v_\ell^{m_\ell}\}$, we distinguish between appearances of the same rank in σ, by their positions in σ. We consider the increasing order of these positions. By abuse of notation we sometimes write $\sigma(j) = v_{i,r}$ and $j = \sigma^{-1}(v_{i,r})$ to indicate that the rth appearance of v_i is in the jth position in σ. The computation of the Kendall's τ-distance between two permutations can be generalized to two multipermutations $\sigma, \pi \in S(\mathcal{M})$ as follows

$$d_K(\sigma, \pi) = \left| \left\{ ((i,r),(j,s)) \ : \ \begin{array}{c} \sigma^{-1}(v_{i,r}) < \sigma^{-1}(v_{j,s}) \\ \pi^{-1}(v_{i,r}) > \pi^{-1}(v_{j,s}) \end{array} \right\} \right|. \tag{4.2}$$

Let $n_0 = 0$ and, for all $1 \leq i \leq \ell$, let $n_i = \sum_{j=1}^{i} m_j$, which implies that $n = n_\ell$. For a multipermutation $\sigma \in S(\mathcal{M})$ and permutations $\gamma_1, \gamma_2, \dots, \gamma_\ell$, such that $\gamma_i \in S([n_{i-1}+1, n_i])$, for all $i \in [\ell]$, the assignment of the permutations $\gamma_1, \gamma_2, \ldots, \gamma_\ell$ in the multipermutation σ is the permutation $\alpha = \sigma(\gamma_1, \gamma_2, \ldots, \gamma_\ell) \in S_n$ defined as follows. For all $1 \leq j \leq n$, if $\sigma(j) = v_{i,r}$ then $\alpha(j) = \gamma_i(r)$. For example, let $\sigma = [1, 2, 1, 3, 2, 3] \in S(\{1^2, 2^2, 3^2\})$ and let $\gamma_1 = [2, 1]$, $\gamma_2 = [3, 4]$ and $\gamma_3 = [6, 5]$. Then $\sigma(\gamma_1, \gamma_2, \gamma_3) = [2, 3, 1, 6, 4, 5]$.

Lemma 4.2 *Let $\sigma, \pi \in S(\mathcal{M})$ and let $\gamma_1, \gamma_2, \ldots, \gamma_\ell$, $\delta_1, \delta_2, \ldots, \delta_\ell$, where $\gamma_i, \delta_i \in S([n_{i-1}+1, n_i]$, for all $i \in [\ell]$. If $\sigma(\gamma_1, \gamma_2, \ldots, \gamma_\ell) = \pi(\delta_1, \delta_2, \ldots, \delta_\ell)$, then $\sigma = \pi$ and $\gamma_i = \delta_i$, for $i \in [\ell]$.*

Proof. Let $\alpha = \sigma(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$ and let $j \in [n]$. If $\alpha(j) = s$, then $n_{i-1}+1 \leq s \leq n_i$ for some $i \in [\ell]$ and $\sigma(j) = \pi(j) = i$. Since this is true for every $j \in [n]$, it follows that $\sigma = \phi$. Moreover, if $\gamma_i(r) = s$ then $\alpha(j) = \gamma_i(r)$ which implies that $\sigma(j) = \pi(j) = i_r$. Therefore, $\alpha(j) = \delta_i(r) = s$ and hence, $\gamma_i(r) = \delta_i(r)$. Since this is true for every $r \in [m_i]$ and $i \in [\ell]$, it follows that $\gamma_i = \delta_i$ for all $i \in [\ell]$.

□

Lemma 4.3 *For every two multipermutations $\sigma, \pi \in S(\mathcal{M})$ and permutations $\gamma_1, \gamma_2, \ldots, \gamma_\ell$, $\gamma_i \in S([n_{i-1}+1, n_i])$ for all $i \in [\ell]$, we have*

$$d_K(\sigma, \pi) = d_K(\sigma(\gamma_1, \gamma_2, \ldots, \gamma_\ell), \pi(\gamma_1, \gamma_2, \ldots, \gamma_\ell)).$$

Proof. Let $\alpha = \sigma(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$ and $\beta = \pi(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$. Let

$$I_1 = \left\{ ((i,r),(j,s)) \; : \; \begin{array}{c} \sigma^{-1}(v_{i,r}) < \sigma^{-1}(v_{j,s}) \\ \pi^{-1}(v_{i,r}) > \pi^{-1}(v_{j,s}) \end{array} \right\}$$

and

$$I_2 = \left\{ (a,b) : \alpha^{-1}(a) < \alpha^{-1}(b), \; \beta^{-1}(a) > \beta^{-1}(b) \right\}.$$

By equations (7.3) and (4.2) it follows that $d_K(\sigma, \pi) = |I_1|$ and $d_K(\alpha, \beta) = |I_2|$. Let $((i,r),(j,s)) \in I_1$, i.e. $\sigma^{-1}(v_{i,r}) < \sigma^{-1}(v_{j,s})$ and $\pi^{-1}(v_{i,r}) > \pi^{-1}(v_{j,s})$. By definition, if $v_{i,r}$ is in the kth position in σ, then $\gamma_i(r)$ is in kth position in α. Hence, $\alpha^{-1}(\gamma_i(r)) = \sigma^{-1}(v_{i,r})$. Similarly, $\alpha^{-1}(\gamma_j(s)) = \sigma^{-1}(v_{j,s})$, $\beta^{-1}(\gamma_i(r)) = \pi^{-1}(v_{i,r})$, and $\beta^{-1}(\gamma_j(s)) = \pi^{-1}(v_{j,s})$. It follows that $\alpha^{-1}(\gamma_i(r)) < \alpha^{-1}(\gamma_j(s))$ and similarly, $\beta^{-1}(\gamma_i(r)) > \beta^{-1}(\gamma_j(s))$. This implies that $(\gamma_i(r), \gamma_j(s)) \in I_2$. Conversely, let $(a,b) \in I_2$, i.e. $\alpha^{-1}(a) < \alpha^{-1}(b)$ and $\beta^{-1}(a) > \beta^{-1}(b)$. There exist $i, j \in [\ell]$, $r \in [m_i]$, and $s \in [m_j]$, such that $a = \gamma_i(r)$ and $b = \gamma_j(s)$. It follows that $\sigma^{-1}(v_{i,r}) = \alpha^{-1}(a) < \alpha^{-1}(b) = \sigma^{-1}(v_{j,s})$ and $\pi^{-1}(v_{i,r}) = \beta^{-1}(a) > \beta^{-1}(b) = \pi^{-1}(v_{j,s})$, which implies that $((i,r),(j,s)) \in I_1$. Hence, the mapping that maps $((i,r),(j,s))$ to $(\gamma_i(r), \gamma_j(s))$ is a bijection of I_1 into I_2. Thus, $d_K(\sigma, \pi) = |I_1| = |I_2| = d_K(\alpha, \beta)$.

□

Example 4.4 *If $\sigma = [1,1,2,2]$, $\pi = [2,1,2,1]$, $\gamma_1 = [2,1]$, and $\gamma_2 = [3,4]$, then $d_K(\sigma,\pi) = 3$ and $d_K(\sigma(\gamma_1,\gamma_2),\pi(\gamma_1,\gamma_2)) = d_K([2,1,3,4],[3,2,4,1]) = 3$.*

The Kendall's τ-metric is graphic, i.e. for every two multipermutations $\sigma,\pi \in S(\mathcal{M})$ their Kendall's τ-distance is equal to the length of the shortest path between σ and π in the graph $G(\mathcal{M})$, whose vertices set is the set $S(\mathcal{M})$, and two vertices are connected by an edge if and only if their Kendall's τ-distance is one. We call the graph $G(\mathcal{M})$ the *graphic representation* of $S(\mathcal{M})$ under the Kendall's τ-distance. The graphic representation of S_n is denoted by $G(n)$. The graphic representation of the Kendall's τ-metric is useful in the proof of the following two lemmas.

Lemma 4.5 *Let $\sigma,\pi \in S(\mathcal{M})$ and let $\gamma_1,\gamma_2,\ldots,\gamma_\ell$, $\delta_1,\delta_2,\ldots,\delta_\ell$, where $\gamma_i,\delta_i \in S([n_{i-1}+1,n_i])$ for all $i \in \ell$. Then*

$$d_K(\sigma(\gamma_1,\gamma_2,\ldots,\gamma_\ell),\pi(\delta_1,\delta_2,\ldots,\delta_\ell)) \geq d_K(\sigma,\pi) + \sum_{i=1}^{\ell} d_K(\gamma_i,\delta_i).$$

Proof.

Let $\alpha = \sigma(\gamma_1,\gamma_2,\ldots,\gamma_\ell)$, $\beta = \pi(\delta_1,\delta_2,\ldots,\delta_\ell)$, and $d_K(\alpha,\beta) = t$. There exists a path $\Gamma : \alpha = \rho_1 \to \rho_2 \to \ldots \to \rho_{t+1} = \beta$ in the graph $G(n)$, where $n = \sum_{i=1}^{\ell} m_i$. Every edge in the path Γ is of the form $e_s = \rho_s \to \rho_{s+1}$ where $\rho_{s+1} = (j,j+1) \circ \rho_s$, for some j, $1 \leq j \leq n-1$.

If there exists an $i \in [\ell]$ such that $\rho_s(j), \rho_s(j+1) \in [n_{i-1}+1,n_i]$ then the edge e_s is correspond to the exchange of two adjacent elements in a permutation $\nu_s \in S([n_{i-1}+1,n_i]$, resulting in a permutation $\nu_{s+1} \in S([n_{i-1}+1,n_i]$. Let $e_{s_{i,1}}, e_{s_{i,2}}, \ldots, e_{s_{i,t_i}}$ be all such edges according to the order of their appearance in the path Γ. Then the path $\Gamma_i : \gamma_i = \nu_{s_{i,1}} \to \nu_{s_{i,2}} \to \ldots \to \nu_{s_{i,t_i}} \to \nu_{s_{i,t_i}+1} = \delta_i$ is a path in the graph $G([n_{i-1}+1,n_i])$ from γ_i to δ_i. Since the length of the path Γ_i is t_i, it follows that $t_i \geq d_K(\gamma_i,\delta_i)$.

If there exist $i,\tilde{i} \in [\ell]$, $i \neq \tilde{i}$, such that $\rho_s(j) \in [n_{i-1}+1,n_i]$, $\rho_s(j+1) \in [n_{\tilde{i}-1}+1,n_{\tilde{i}}]$, then the edge e_s is correspond to the exchange of two adjacent elements in a multipermutation $\mu_s \in S(\mathcal{M})$, resulting in a multipermutation $\mu_{s+1} \in S(\mathcal{M})$. Let $e_{s_1}, e_{s_2}, \ldots, e_{s_{\tilde{t}}}$ be all such edges according to the order of their appearance in the path Γ. Then the path $\tilde{\Gamma} : \sigma = \mu_{s_1} \to \mu_{s_2} \to \ldots \to \mu_{s_{\tilde{t}}} \to \mu_{s_{\tilde{t}}+1} = \pi$ is a path in the graph $G(\mathcal{M})$ from σ to π. Since the length of the path $\tilde{\Gamma}$ is $\tilde{t}$, it follows that $\tilde{t} \geq d_K(\sigma,\pi)$.

The paths $\Gamma_1, \Gamma_2, \dots, \Gamma_\ell$, and $\tilde{\Gamma}$ are correspond to a partition of the edges of Γ into disjoint sets. Thus,

$$d_K(\alpha, \beta) = t = \tilde{t} + \sum_{i=1}^{\ell} t_i \geq d_K(\sigma, \pi) + \sum_{i=1}^{\ell} d_K(\gamma_i, \delta_i).$$

□

A distance measure $d(\cdot, \cdot)$ over a space $\mathcal{V}$, is called *bipartite* if every three elements $x, y, z \in \mathcal{V}$ satisfies the equality $d(x, y) + d(y, z) \equiv d(x, z) \pmod 2$. The Kendall's τ-metric on S_n is bipartite as stated in the next lemma.

Lemma 4.6 *If ρ_1, ρ_2 and ρ_3 are three multipermutations in $S(\mathcal{M})$ then*

$$d_K(\rho_1, \rho_2) + d_K(\rho_2, \rho_3) \equiv d_K(\rho_1, \rho_3) \ (mod\ 2).$$

Proof. Let $t_1 = d_K(\rho_1, \rho_2)$, $t_2 = d_K(\rho_2, \rho_3)$, and $t_3 = d_K(\rho_1, \rho_3)$. There exist paths $\Gamma_1, \Gamma_2, \Gamma_3$, in the graph $G(\mathcal{M})$, where Γ_1 is a path of length t_1 between ρ_1 and ρ_2, Γ_2 is a path of length t_2 between ρ_2 and ρ_3, and Γ_3 is a path of length t_3 between ρ_3 and ρ_2. By concatenating these paths we obtain a cycle, Δ, of length $t_1 + t_2 + t_3$ in $G(\mathcal{M})$. Every edge in the cycle Δ is of the form $\gamma \to \delta$, $\gamma, \delta \in S(\mathcal{M})$, where δ is obtained from γ by exactly one adjacent transposition. For every $i, j \in [n]$, where $i < j$, there must be an even number of edges in the cycle Δ that correspond to an adjacent transposition that exchanges the elements i and j. Therefore, the number of edges in the cycle Δ must be even i.e. $d_K(\sigma, \pi) + d_K(\pi, \rho) + d_K(\sigma, \rho) \equiv 0 \pmod 2$, and the lemma follows.

□

Lemma 4.7 *Let $\sigma, \rho \in S_n$ be two permutations. Then*

$$w_K(\sigma \circ \rho) \equiv w_K(\sigma) + w_K(\rho) (\ mod\ 2).$$

Proof. Since the Kendall's τ-distance on S_n is right invariant it follows that $w_K(\sigma \circ \rho) = d_K(\sigma, \rho^{-1})$ and $d_K(\rho^{-1}, \varepsilon) = d_K(\varepsilon, \rho) = w_K(\rho)$. By Lemma 4.6 we have that $d_K(\rho^{-1}, \sigma) \equiv d_K(\sigma, \varepsilon) + d_K(\rho^{-1}, \varepsilon)(\text{ mod } 2)$. Thus, $w_K(\sigma \circ \rho) \equiv w_K(\sigma) + w_K(\rho)(\text{ mod } 2)$.

□

For a permutation $\sigma \in S_n$, the *sphere* of radius t centered at σ is the set

$$\mathbb{S}_K(n, t, \sigma) = \{\pi \in S_n \ : \ d_K(\sigma, \pi) \leq t\}.$$

We denote by $\mathbb{S}_K(n, t)$ the sphere of radius t centered at ε. Since the Kendall's τ-distance on S_n is right invariant it follows that the size of a sphere of radius t is S_n does not depend on its center, i.e. for all $\sigma \in S_n$, $|\mathbb{S}_K(n,t,\sigma)| = |\mathbb{S}_K(n,t)|$.

A code $\mathcal{C} \subseteq S_n$ is a *t-error-correcting code with the Kendall's τ-distance* if for every $\rho \in S_n$ there exists at most one codeword $\sigma \in \mathcal{C}$ such that $d_K(\sigma,\rho) \leq t$. Equivalently, $\mathcal{C}$ is a t-error-correcting code with the Kendall's τ- distance if for every $\sigma, \pi \in \mathcal{C}$ such that $\sigma \neq \pi$ we have that $\mathbb{S}_K(n,t,\sigma) \cap \mathbb{S}_K(n,t,\pi) = \varnothing$.

Given a code $\mathcal{C}$, where $|\mathcal{C}| \geq 2$, in a space $\mathcal{V}$ endowed with a distance measure (a metric) $d(\cdot,\cdot)$, the *minimum distance* of $\mathcal{C}$ is the minimum distance between two distinct codewords in $\mathcal{C}$, i.e.

$$\min\{d(x,y) \ : \ x,y \in \mathcal{C},\ x \neq y\}.$$

A code $\mathcal{C} \subseteq S_n$ is a t-error-correcting code with the Kendall's τ-distance if and only if the minimum distance of $\mathcal{C}$ is at least $2t+1$. The following theorem is known as the *sphere packing bound*.

Theorem 4.8 *If $\mathcal{C} \subseteq S_n$ is a t-error-correcting code then*

$$|\mathcal{C}| \cdot |\mathbb{S}_K(n,t)| \leq n!.$$

A code $\mathcal{C} \subseteq S_n$ is called a *perfect* t-error-correcting code if $\mathcal{C}$ is a t-error-correcting code and the size of $\mathcal{C}$ achieves the sphere packing bound with equality, i.e. $|\mathcal{C}| \cdot |\mathbb{S}_K(n,t)| = n!$. A code $\mathcal{C} \subseteq S_n$ is a t-error-correcting code if and only if for every $\pi \in S_n$ there exists exactly one codeword $\sigma \in \mathcal{C}$ for which $d_K(\sigma,\pi) \leq t$.

Chapter 5

Permutation Codes

The rank modulation scheme has been proposed for efficient writing and storing data in non-volatile memory storage [43]. In this model codes are subsets of S_n, the set of all permutations on n elements, where each permutation corresponds to a ranking of n cells' levels. Permutation codes were mainly studied in this context using two metrics, the infinity metric and the Kendall's τ-metric. In this chapter error-correcting codes using the Kendall's τ-metric and some variation of the Kendall's τ-metric are considered. Under the Kendall's τ-metric, codes in S_n with minimum distance d should correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors that are caused by charge leakage and read disturbance [44]. Error-correcting codes using codes in the Lee metric were constructed in [5, 61, 61]. In [108], systematic-error-correcting codes were proposed. In particular, they constructed a systematic single-error-correcting code in S_n of size $(n-2)!$, which is of optimal size, assuming that a perfect single-error-correcting code does not exist. But, they only prove the nonexistence of perfect single-error-correcting codes for $n = 4$.

The first section of this chapter is devoted to perfect codes in S_n that correct a single error, using the Kendall's τ-metric. It is proved that perfect single-error-correcting codes in S_n, where $n > 4$ is a prime or $4 \leq n \leq 10$, do not exist. It is also proved that if such a code exists for n which is not a prime then the code should have some uniform structure.

In Section 5.2 we establish a Delsarte's code-anticode type of bound for the Kendall's τ-metric and examine diameter perfect codes in S_n for this metric. We find the sizes of optimal anticodes in S_n with diameter 2 and diameter 3. We combine these results with the code-anticode bound to improve some known upper bounds on the size of a code in S_n for even minimum distances. In Section 5.3 we first present the cyclic Kendall's τ-metric and show the existence of a perfect single-error-correcting code in S_5, using the cyclic Kendall's τ-distance. Furthermore, we consider the set of $(n-1)!$ necklaces of permutations of length n and define the Kendall's τ-metric on this set. We present one perfect code in S_5 in this setting, and using this setting we also show larger codes than the known ones in S_5 and S_7 with the Kendall's τ-metric. These codes have a large automorphism group. An algorithm that computes the cyclic Kendall's τ-distance between two permutations $\sigma, \pi \in S_n$ is also presented in Section 5.3. The algorithm running time is $O(n^2)$.

5.1 Uniform Codes and the Nonexistence of Some Perfect Codes

In this section it is proved that a perfect single-error-correcting code in S_n is r-uniform for $r < \frac{n}{4}$, i.e. each r distinct symbols in $[n]$ appear in each r positions the same number of times. As a consequence it is proved that there are no perfect single-error-correcting codes in S_n, where n is a prime greater than 4. By using similar techniques we also show that there are no perfect single-error-correcting codes in S_n for $4 \leq n \leq 10$.

For each i, $1 \leq i \leq n$, let $S_{n,i} = \{\sigma \ : \ \sigma \in S_n,\ \sigma(i) = 1\}$, i.e. $S_{n,i}$ consists of all the permutations $\sigma \in S_n$ for which 1 appears in the ith position of σ. Clearly, $|S_{n,i}| = (n-1)!$.

Assume that there exists a perfect single-error-correcting code $\mathcal{C} \subset S_n$. For each i, $1 \leq i \leq n$, let

$$\mathcal{C}_i = \mathcal{C} \cap S_{n,i} \qquad \text{and} \qquad x_i = |\mathcal{C}_i|.$$

A codeword $\sigma \in \mathcal{C}$ *covers* a permutation $\pi \in S_n$ if $d_K(\sigma, \pi) \leq 1$. Since $\mathcal{C}$ is a single-error-correcting code, it follows that every permutation in $S_{n,1}$ must be at distance at most one from exactly one codeword of $\mathcal{C}$ and this codeword must belong either to $\mathcal{C}_1$ or $\mathcal{C}_2$. Every codeword $\sigma \in \mathcal{C}_1$ covers exactly $n-1$ permutations in $S_{n,1}$. It covers itself and the $n-2$ permutations in $S_{n,1}$ obtained from σ by exactly one adjacent transposition $(i, i+1)$, $1 < i < n$. Each codeword $\sigma \in \mathcal{C}_2$ covers exactly one permutation $\pi \in S_{n,1}$, $\pi = (1,2) \circ \sigma$. Therefore,

$$(n-1)x_1 + x_2 = (n-1)! \ . \tag{5.1}$$

Similarly, by considering how the permutations of $S_{n,n}$ are covered by codewords of $\mathcal{C}$, it follows that

$$x_{n-1} + (n-1)x_n = (n-1)! \ . \tag{5.2}$$

For each i, $2 \leq i \leq n-1$, each permutation in $S_{n,i}$ is covered by exactly one codeword that belongs to either $\mathcal{C}_{i-1}$, $\mathcal{C}_i$, or $\mathcal{C}_{i+1}$. Each codeword $\sigma \in \mathcal{C}_i$ covers exactly $n-2$ permutations in $S_{n,i}$. It covers itself and the $n-3$ permutations in $S_{n,i}$ obtained from σ by exactly one adjacent transposition $(j, j+1)$, where $1 \leq j < i-1$ or $i < j < n$. Each codeword in $\mathcal{C}_{i-1} \cup \mathcal{C}_{i+1}$ covers exactly one permutation from $S_{n,i}$. Therefore, for each i, $2 \leq i \leq n-1$, we have the equation

$$x_{i-1} + (n-2)x_i + x_{i+1} = (n-1)! \ . \tag{5.3}$$

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and let $\mathbf{1}$ denote the all-ones vector. Equations (5.1), (5.2), and (5.3) can be written in matrix form as

$$A\mathbf{x} = (n-1)! \cdot \mathbf{1}, \tag{5.4}$$

where $A = (a_{i,j})$ is defined by

$$A = \begin{pmatrix} n-1 & 1 & 0 & 0 & \cdots & 0 & 0 & \ldots & 0 \\ 1 & n-2 & 1 & 0 & \cdots & 0 & 0 & \ldots & 0 \\ 0 & 1 & n-2 & 1 & \cdots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 & \cdots & 1 & n-2 & 1 & 0 \\ 0 & \ldots & 0 & 0 & \cdots & 0 & 1 & n-2 & 1 \\ 0 & \ldots & 0 & 0 & \cdots & 0 & 0 & 1 & n-1 \end{pmatrix}.$$

Since the sum of every row in A is equal to n it follows that the linear equation system (5.4) has a solution $\mathbf{y} = \frac{(n-1)!}{n} \cdot \mathbf{1}$. We will show that if $n > 3$ then A is a nonsingular matrix and hence $\mathbf{y}$ is the unique solution of (5.4), i.e. $\mathbf{x} = \mathbf{y}$. To this end, we need the following lemma, that can be easily verified (a sketch of the proof is given), and is also an immediate conclusion of the well known Gerschgorin circle theorem [34].

Lemma 5.1 *Let $B = (b_{i,j})$ be an $n \times n$ matrix. If $|b_{i,i}| > \sum_{j \neq i} |b_{i,j}|$ for all i, $1 \leq i \leq n$, then B is nonsingular.*

Proof. Let $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ be a nonzero vector and let s be an index such that $|z_s| \geq |z_i$ for each i, $1 \leq i \leq n$. Clearly, the sth entry of $B\mathbf{z}$ is not zero.

□

For $n > 4$, we have that for each i, $1 \leq i \leq n$, $A_{i,i} \geq n-2 > 2 \geq \sum_{j \neq i} A_{i,j}$. By Lemma 5.1 it follows that A is nonsingular. For $n = 4$ it can be readily verified that the matrix A is nonsingular. Hence, $\mathbf{x} = \frac{(n-1)!}{n} \cdot \mathbf{1}$ for $n \geq 4$. If $n = 4$ or n is a prime greater than 4, then $\frac{(n-1)!}{n}$ is not an integer and therefore, a perfect single-error-correcting code does not exist.

Theorem 5.2 *There is no perfect single-error-correcting code in S_n, where $n > 4$ is a prime or $n = 4$.*

Theorem 5.3 *Assume that there exists a perfect single-error-correcting code $\mathcal{C} \subset S_n$, where $n > 11$. If $r < \frac{n}{4}$, then for ezch sequence of r distinct elements of $[n]$, $i_1, i_2, \ldots, i_r$, and for each set of r positions $1 \leq j_1 < j_2 < \ldots < j_r \leq n$, there are exactly $\frac{(n-r)!}{n}$ codewords in cC, such that for each such codeword σ we have $\sigma(j_\ell) = i_\ell$, for each ℓ, $1 \leq \ell \leq r$.*

Proof. Let $i_1, i_2, \ldots, i_r$ be a sequence of r distinct elements of $[n]$. For every $J = \{j_1, j_2, \ldots, j_r\} \subset [n]$, where $1 \leq j_1 < j_2 < \ldots < j_r \leq n$, let $S_{n,J} = \{\sigma \in S_n \; : \; \sigma(j_\ell) = i_\ell, \text{ for all } 1 \leq \ell \leq r\}$. Clearly, $|S_{n,J}| = (n-r)!$. Let

$$\mathcal{C}_J = \mathcal{C} \cap S_{n,J} \qquad \text{and} \qquad x_J = |\mathcal{C}_J|.$$

Since $\mathcal{C}$ is a single-error-correcting code, it follows that every permutation in $S_{n,J}$ must be at distance at most one from exactly one codeword of $\mathcal{C}$. For every $J, L \subset [n]$, $|J| = |L| = r$, let $a_{J,L}$ be the number of permutations in $S_{n,J}$ which are covered by a given codeword in $\mathcal{C}_L$. Therefore, we have the following linear equations system

$$\sum_{L \subset [n],\ |L|=r} a_{J,L} x_L = |S_{n,J}| = (n-r)!, \qquad \text{for all } J \subset [n],\ |J| = r. \tag{5.5}$$

Each codeword $\sigma \in \mathcal{C}_J$ covers at least $n - 2r$ permutations in $S_{n,J}$. It covers itself and at least $n - 2r - 1$ permutations in $S_{n,J}$ which are obtained from σ by exactly one adjacent transposition $(i, i+1)$, where $i, i+1 \in [n] \setminus J$. Hence, $a_{J,J} \geq n - 2r$ and since the size of a sphere of radius one is n, it follows that

$$\sum_{L \subset [n],\ |L|=r} a_{J,L} = n, \qquad \text{for all } J \subset [n],\ |J| = r. \tag{5.6}$$

Therefore,

$$\sum_{L \subset [n],\ |L|=r,\ L \neq J} a_{J,L} = \sum_{L \subset [n],\ |L|=r} a_{J,L} - a_{J,J} \leq n - (n-2r) = 2r.$$

If $r < \frac{n}{4}$ then

$$a_{J,J} \geq n - 2r > 2r \geq \sum_{L \subset [n],\ |L|=r,\ L \neq J} a_{J,L}.$$

Hence, by Lemma 5.1 it follows that the linear equations system (5.5) has a unique solution and by (5.6) we have that $x_J = \frac{(n-r)!}{n}$, for every $J \subset [n]$, $|J| = r$. Thus, for each sequence of r distinct elements of $[n]$, $i_1, i_2, \ldots, i_r$, and for each set of r positions $1 \leq j_1 < j_2 < \ldots < j_r \leq n$, there are exactly $\frac{(n-r)!}{n}$ codewords in $\mathcal{C}$, such that for each such codeword σ we have $\sigma(j_\ell) = i_\ell$, for each ℓ, $1 \leq \ell \leq r$.

□

Theorem 5.3 implies that perfect single-error-correcting codes must have a very symmetric structure. This might be useful to rule out the existence of these codes for other parameters as well.

For the case $n = 6, 8, 10$, we use similar arguments and obtain systems of linear equations. We use a computer to show that these systems have no solutions over the non negative integers, and conclude that perfect single-error-correcting codes in S_n do not exist for these values of n. More details on these cases can be found in Appendix A.

5.2 Anticodes and Diameter Perfect Codes

In all the perfect codes the minimum distance of the code is an odd integer. If the minimum distance of the code $\mathcal{C}$ is an even integer then $\mathcal{C}$ cannot be a perfect code. The reason is that for any two codewords $c_1, c_2 \in \mathcal{C}$ such that $d(c_1, c_2) = 2\delta$, there exists a word x such that $d(x, c_1) = \delta$ and $d(x, c_2) = \delta$. For this case another concept is used, a diameter perfect code, as was defined in [1]. This concept is based on the code-anticode bound presented by Delsarte [19]. An *anticode* $\mathcal{A}$ of *diameter* D in a space $\mathcal{V}$ is a subset of words from $\mathcal{V}$ such that $d(x, y) \leq D$ for all $x, y \in \mathcal{A}$.

Theorem 5.4 *If a code $\mathcal{C}$, in a space $\mathcal{V}$ of a distance regular graph, has minimum distance d and in an anticode $\mathcal{A}$ of the space $\mathcal{V}$ the maximum distance is $d-1$ then $|\mathcal{C}| \cdot |\mathcal{A}| \leq |\mathcal{V}|$.*

Theorem 5.4 which is proved in [19] is a generalization of Theorem 4.8 and it can be applied to the Hamming scheme since the related graph is distance regular. It cannot be applied to the Kendall's τ-metric since the related graph is not distance regular if $n > 3$. This can be easily verified by considering the three permutations $\sigma = [1, 2, 3, 4, 5, \ldots, n]$, $\pi =$

$[3,1,2,4,5,\ldots,n]$, and $\rho = [2,1,4,3,5,\ldots,n]$ in S_n. Clearly, $d_K(\sigma,\pi) = d_K(\sigma,\rho) = 2$ and there exists exactly one permutation α for which $d_K(\sigma,\alpha) = 1$ and $d_K(\alpha,\pi) = 1$, while there exist exactly two permutations α,β for which $d_K(\sigma,\alpha) = 1$, $d_K(\alpha,\rho) = 1$, $d_K(\sigma,\beta) = 1$, and $d_K(\beta,\rho) = 1$. Fortunately, an alternative proof which was given in [1] and was modified in [27] will work for the Kendall's τ-metric.

Theorem 5.5 *Let $\mathcal{C}_\mathcal{D}$ be a code in S_n with Kendall's τ-distances between codewords taken from a set $\mathcal{D}$. Let $\mathcal{A} \subset S_n$ and let $\mathcal{C}'_\mathcal{D}$ be the largest code in $\mathcal{A}$ with Kendall's τ-distances between codewords taken from the set $\mathcal{D}$. Then*

$$\frac{|\mathcal{C}_\mathcal{D}|}{n!} \leq \frac{|\mathcal{C}'_\mathcal{D}|}{|\mathcal{A}|} \ .$$

Proof. Let $\mathcal{B} \overset{\text{def}}{=} \{(\sigma,\pi) \ : \ \sigma \in \mathbb{C}_\mathcal{D}, \ \pi \in S_n, \ \sigma \circ \pi \in \mathcal{A}\}$. For a given codeword $\sigma \in \mathbb{C}_\mathcal{D}$ and a word $\alpha \in \mathcal{A}$, there is exactly one element $\pi \in S_n$ such that $\alpha = \sigma \circ \pi$. Therefore, $|\mathcal{B}| = |\mathbb{C}_\mathcal{D}| \cdot |\mathcal{A}|$.

Since the Kendall's τ-metric is right invariant it follows that for every $\pi \in S_n$, the set $\{\sigma \circ \pi \ : \ \sigma \in \mathbb{C}'_\mathcal{D}\}$ has Kendall's τ-distances between codewords taken from the set $\mathcal{D}$. Together with the fact that $\mathbb{C}'_\mathcal{D}$ is the largest code in $\mathcal{A}$, with Kendall's τ-distances between codewords taken from the set $\mathcal{D}$, it follows that for any given word $\pi \in S_n$ the set $\{\sigma \ : \ \sigma \in \mathbb{C}_\mathcal{D}, \ \sigma \cdot \pi \in \mathcal{A}\}$ has at most $|\mathbb{C}'_\mathcal{D}|$ codewords. Hence, $|\mathcal{B}| \leq |\mathbb{C}'_\mathcal{D}| \cdot n!$.

Thus, $|\mathbb{C}_\mathcal{D}| \cdot |\mathcal{A}| \leq |\mathbb{C}'_\mathcal{D}| \cdot n!$ and the claim is proved.

□

Corollary 5.6 *Theorem 5.4 holds for the Kendall's τ-metric, i.e. if a code $\mathcal{C} \subseteq S_n$, has minimum Kendall's τ-distance d and in an anticode $\mathcal{A} \subset S_n$ the maximum Kendall's τ-distance is $d-1$ then $|\mathcal{C}| \cdot |\mathcal{A}| \leq n!$.*

Proof. Let $\mathcal{D} = \{d, d+1, \ldots, \binom{n}{2}\}$ and let $\mathcal{C}_\mathcal{D} \subseteq S_n$ be a code with minimum Kendall's τ-distance d. Let $\mathcal{A}$ be a subset of S_n with Kendall's τ-distances between words of $\mathcal{A}$ taken from the set $\{1,2,\ldots,d-1\}$, i.e. $\mathcal{A}$ is an anticode with diameter $d-1$. Clearly, the largest code in $\mathcal{A}$ with Kendall's τ-distances from $\mathcal{D}$ has only one codeword. Applying Theorem 5.5 on $\mathcal{D}$, $\mathcal{C}_\mathcal{D}$, and $\mathcal{A}$, implies that $|\mathcal{C}_\mathcal{D}| \cdot |\mathcal{A}| \leq n!$.

□

If there exists a code $\mathcal{C} \subset S_n$ with minimum Kendall's τ-distance $d = D+1$, and an anticode $\mathcal{A}$ with diameter D such that $|\mathcal{C}| \cdot |\mathcal{A}| = n!$, then $\mathcal{C}$ is called a *D-diameter perfect* code. In that case, $\mathcal{A}$ must be an anticode with maximum distance (diameter) D of largest size, and $\mathcal{A}$ is called an *optimal* anticode of diameter D. Thus, it is important to determine the optimal anticodes in S_n and their sizes. Using the size of such optimal anticodes we can obtain by Corollary 5.6 an upper bound on the size of the related code in S_n.

Let $S(\sigma, t) \subseteq S_n$ be the sphere of radius t centered at $\sigma \in S_n$. An intriguing question is whether a sphere with radius t in S_n, using the Kendall's τ-metric, is an optimal anticode of diameter $2t$. Such types of questions for other metrics were considered in [3]. For $n = 4$, the sphere with radius 1 has size 4 and it is an optimal anticode of diameter 2. There exists an optimal anticode of diameter 2 in S_4, which is not a sphere with radius 1. For example, the set $\mathcal{A} = \{[1, 2, 3, 4], [2, 1, 3, 4], [1, 2, 4, 3], [2, 1, 4, 3]\}$ is an optimal anticode of diameter 2. A similar example exists for an optimal anticode of size 9 and diameter 4 in S_4. However, for $n \geq 5$, it is showed that every optimal anticode of diameter 2 in S_n is a sphere of radius 1. To this end, the following lemma will be useful.

Lemma 5.7 *Let $\mathcal{A}$ be an anticode in S_n with diameter 2 such that $\varepsilon \in \mathcal{A}$, and let $\mathcal{B}$ be the set of all permutations of weight two in $\mathcal{A}$. If $|\mathcal{B}| \geq 4$ then $\mathcal{B}$ is contained in a sphere of radius one centered at some permutation $\sigma \in S_n$ of weight one.*

Proof. If there exists some $i \in [n-2]$ such that $(i, i+1) \circ (i+1, i+2), (i+1, i+2) \circ (i, i+1) \in \mathcal{B}$, then one can easily verify that any other permutation of weight two is at distance at least four from either $(i, i+1) \circ (i+1, i+2)$ or $(i+1, i+2) \circ (i, i+1)$ and therefore $|\mathcal{B}| = 2$.

If for some $i \in [n-2]$ either $(i, i+1) \circ (i+1, i+2)$ or $(i+1, i+2) \circ (i, i+1)$ belongs to $\mathcal{B}$, say w.l.o.g. $(i, i+1) \circ (i+1, i+2) \in \mathcal{B}$, then every element of $\mathcal{B} \setminus \{(i, i+1) \circ (i+1, i+2)\}$ must be at distance 2 from $(i, i+1) \circ (i+1, i+2)$ and therefore, must be of the form $(j, j+1) \circ (i+1, i+2)$ for some $j \notin \{i, i+1\}$. It follows that $\mathcal{B} \subset S((i+1, i+2), 1)$.

If each element of $\mathcal{B}$ is a multiplication of two disjoint adjacent transpositions then let $\rho = (i, i+1) \circ (j, j+1) \in \mathcal{B}$, where $j \notin \{i-1, i, i+1\}$. Hence, all elements of $\mathcal{B}$ are of the form $(\ell, \ell+1) \circ (j, j+1)$, where $\ell \notin \{j, j+1\}$, or $(\ell, \ell+1) \circ (i, i+1)$, where $\ell \notin \{i, i+1\}$. Assume w.l.o.g. that $\pi = (\ell, \ell+1) \circ (j, j+1) \in \mathcal{B}$, $\pi \neq \rho$. If every element of $\mathcal{B}$ is of the form $(k, k+1) \circ (j, j+1)$ then $\mathcal{B} \subset S((j, j+1), 1)$. Otherwise, the only possible other element of $\mathcal{B}$ is $(i, i+1) \circ (\ell, \ell+1)$ and hence $|\mathcal{B}| \leq 3$.

Thus, if $|\mathcal{B}| \geq 4$ then $\mathcal{B} \subset S(\sigma, 1)$, for some σ of weight one.

□

Theorem 5.8 *Every optimal anticode with diameter 2 (using the Kendall's τ-distance) in S_n, $n \geq 5$, is a sphere with radius one whose size is n.*

Proof. Let $\mathcal{A} \subset S_n$, $n \geq 5$, be an anticode of diameter 2. The Kendall's τ-metric is right invariant and hence w.l.o.g. we can assume that $\varepsilon \in \mathcal{A}$. Therefore, all the elements of $\mathcal{A}$ are of weight at most two. We distinguish between four cases:

Case 1: If $\mathcal{A}$ does not contain a permutation of weight one then by Lemma 5.7 it follows that $\mathcal{A}$ is contained in a sphere of radius one centered at a permutation of weight one or $|\mathcal{A}| \leq 4$.

Case 2: If $\mathcal{A}$ contains exactly one permutation $\sigma \in S_n$ of wight one then by Lemma 4.6, the distance between σ and any permutation of weight two is an odd integer and therefore, all permutations of weight two in $\mathcal{A}$ must be at distance one from σ. Thus, $\mathcal{A} \subseteq S(\sigma, 1)$.

Case 3: If $\mathcal{A}$ contains two elements of weight one then it can be readily verified that $\mathcal{A}$ cannot contain more than one element of weight two and hence $|\mathcal{A}| \leq 4$.

Case 4: If $\mathcal{A}$ contains at least three elements of weight one then $\mathcal{A}$ cannot contain elements of weight two and therefore $\mathcal{A} \subseteq S(\varepsilon, 1)$.

Thus, we proved that either $\mathcal{A}$ is contained in a sphere of radius one or $|\mathcal{A}| \leq 4$. Since the size of a sphere of radius one in S_n is n, it follows that if $n \geq 5$ then every optimal anticode of diameter 2 in S_n is a sphere of radius one.

□

Theorem 5.9 *Let $n \geq 4$. Then the set*

$$\mathcal{A} = S(\varepsilon, 1) \cup S((1,2), 1)$$

is an optimal anticode of diameter 3, whose size is $2(n-1)$.

Proof. The claim can be easily verified for $n = 4$. It can be readily verified that $\mathcal{A}$ is an anticode of diameter 2 and of size $2(n-1)$.

Let $\mathcal{A}$ be an optimal anticode of diameter 3 in S_n, where $n \geq 5$, and let

$$\mathcal{A}_e = \{\sigma \in \mathcal{A} \,:\, w_K(\sigma) \equiv 0 \pmod 2\}, \quad \mathcal{A}_o = \{\sigma \in \mathcal{A} \,:\, w_K(\sigma) \equiv 1 \pmod 2\}.$$

Since the Kendall's τ-metric is bipartite, it follows that $\mathcal{A}_e$ and $\mathcal{A}_o$ are anticodes of diameter 2. If $n \geq 5$ then by Theorem 5.8 it follows that

$|\mathcal{A}_e| \leq n$ ($|\mathcal{A}_o| \leq n$, respectively) and $|\mathcal{A}_e| = n$ ($|\mathcal{A}_0| = n$, respectively) if and only if $\mathcal{A}_e$ ($\mathcal{A}_0$, respectively) is a sphere of radius one. The anticodes $\mathcal{A}_e$ and $\mathcal{A}_o$ cannot be spheres of radius one and therefore, $|\mathcal{A}_e| \leq n-1$ and $|\mathcal{A}_o| \leq n-1$. Thus, $|\mathcal{A}| = |\mathcal{A}_e| + |\mathcal{A}_o| \leq 2(n-1)$, for $n \geq 5$.

□

The following corollary is derived by a combination of Corollary 5.6 and Theorem 5.9.

Corollary 5.10 *If $\mathcal{C} \subset S_n$ is a code with minimum Kendall's τ-distance* 4*, then*

$$|\mathcal{C}| \leq \frac{n!}{2(n-1)}.$$

For a permutation $\sigma \in S_n$ we define the *reverse of* σ to be the permutation $\sigma^R = [\sigma(n), \sigma(n-1), \ldots, \sigma(2), \sigma(1)]$. The following lemma is an immediate consequence from the expression to compute the Kendall's τ-distance given in (7.3).

Lemma 5.11 *For every $\sigma \in S_n$, the reverse of σ, σ^R, is the unique permutation in S_n at distance $\binom{n}{2}$ from σ. Moreover, for every $\pi \in S_n$,*

$$d_K(\sigma, \pi) + d_K(\pi, \sigma^R) = d_K(\sigma, \sigma^R) = \binom{n}{2}.$$

Theorem 5.12 *If $t < \frac{\binom{n}{2}}{2}$ then every sphere of radius t in S_n is a maximal anticode of diameter $2t$.*

Proof. Since the Kendall's τ-metric is right invariant, it is sufficient to prove that $S(\varepsilon, t)$ is a maximal anticode of diameter $2t$. For any given $\pi \in S_n \setminus S(\varepsilon, t)$ we show that the diameter of $S(\varepsilon, t) \cup \{\pi\}$ is greater than $2t$. If the reverse of π, π^R, belongs to $S(\varepsilon, t)$, then by Lemma 5.11 the anticode $S(\varepsilon, t) \cup \{\pi\}$ has diameter $\binom{n}{2} > 2t$. Hence, we can assume that $\pi^R \notin S(\varepsilon, t)$, i.e. $w_K(\pi^R) > t$. By Lemma 5.11, there exists a simple path (no repeat of vertices) Γ of length $\binom{n}{2}$ on the graph $G(n)$, from π^R to π, that passes through ε. Let ρ be the first vertex on Γ that belongs to $S(\varepsilon, t)$. Then $w_K(\rho) = t$ and by Lemma 5.11 $d_K(\pi, \rho) = \binom{n}{2} - d_K(\pi^R, \rho) = w_K(\rho) + w_K(\pi) > 2t$.

□

Theorem 5.13 *$\mathcal{A} \subset S_n$ is an optimal anticode of diameter $\binom{n}{2} - 1$ if and only if $\mathcal{A}$ contains either σ or σ^R, for each $\sigma \in S_n$.*

Proof. If $\mathcal{A}$ is an optimal anticode of diameter $\binom{n}{2}-1$ then by Lemma 5.11, for every $\sigma \in S_n$, $\mathcal{A}$ cannot contain both σ and σ^r. On the other hand, if $\pi \neq \sigma^r$ then $d_K(\sigma,\pi) \leq \binom{n}{2} - 1$. Thus, the theorem follows.

□

5.3 The Cyclic Kendall's τ-metric

In this section we discuss a new metric, a "subclass" of S_n, and a metric on this subclass. The new definitions will be related to the the Kendall's τ-metric. The motivation for these definitions is to find larger codes, than the known ones, in S_n with the Kendall's τ-metric. These codes will have considerably large automorphism groups. Two such codes will be presented in this section.

Given a permutation $\sigma \in S_n$, a *c-adjacent transposition* is either an adjacent transposition or the exchange of the elements $\sigma(1)$ and $\sigma(n)$. For two permutations $\sigma, \pi \in S_n$, the *cyclic Kendall's τ-distance* between σ and π, $d_\kappa(\sigma,\pi)$, is defined as the minimum number of c-adjacent transpositions needed to transform σ into π. For example, if $\sigma = [0,1,2,3]$ and $\pi = [3,2,1,0]$, then $d_\kappa(\sigma,\pi) = 2$, since two c-adjacent transpositions are enough to change σ into π: $[0,1,2,3] \rightarrow [3,1,2,0] \rightarrow [3,2,1,0]$, and we cannot transform σ into π with only one c-adjacent transposition.

Remark 5.1 *Since c-adjacent transpositions refer to elements that are adjacent on a cycle of length n it is more convenient to consider the positions and elements of the permutations as residues modulo n. Hence, throughout this section the positions and elements of permutations of length n are taken from the set $\{0,1,2,\ldots,n-1\}$ (instead of the set $[n]$).*

Clearly, $d_\kappa(\sigma,\rho) \leq d_K(\sigma,\rho)$ and therefore, if $\mathcal{C}$ has minimum cyclic Kendall's τ-distance d then $\mathcal{C}$ also has minimum Kendall's τ-distance at least d. For a permutation $\sigma \in S_n$, the *cyclic Kendall's τ-weight* of σ, $w_\kappa(\sigma)$, is defined as the cyclic Kendall's τ-distance between σ and the identity permutation in S_n, ε. The cyclic Kendall's τ-distance is also graphic, right invariant, and bipartite. Jerrum [42] showed that for every permutation $\sigma \in S_n$, $w_\kappa(\sigma)$ can be computed by solving a certain optimization problem, which can be solve with running time $O(n^2)$. A simpler and explicit algorithm that computes $w_\kappa(\sigma)$ with running time $O(n^2)$ is proved in Appendix B. The algorithm consists of the following five steps.

1) For every $i \in [0, n-1]$, compute

$$dist_\sigma(i) \overset{\text{def}}{=} \min\{i - \sigma^{-1}(i) \pmod n, \sigma^{-1}(i) - i \pmod n\}$$

and

$$sign_\sigma(i) \overset{\text{def}}{=} \begin{cases} 0 & \text{if } \sigma(i) = i \\ + & \text{if } \sigma(i) \neq i \text{ and } dist_\sigma(i) = i - \sigma^{-1}(i) (\bmod n) \\ - & \text{otherwise} \end{cases} .$$

2) Compute

$$r_\sigma \overset{\text{def}}{=} \frac{\sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i)}{n}.$$

3) Choose a set $M \subset [0, n-1]$ of $|r_\sigma|$ elements such that for every $i \in M$, $sign_\sigma(i) r_\sigma \geq 0$ and for every $j \in [0, n-1] \setminus M$, for which $sign_\sigma(j) sign(r_\sigma) \geq 0$, we have that $dist_\sigma(j) \leq dist_\sigma(i)$.

4) For every $i \in [0, n-1]$ compute

$$d_{M,\sigma}(i) \overset{\text{def}}{=} \begin{cases} n - dist_\sigma(i) & \text{if } i \in M \\ dist_\sigma(i) & \text{otherwise} \end{cases}$$

and

$$s_{M,\sigma}(i) \overset{\text{def}}{=} \begin{cases} -sign_\sigma(i) & \text{if } i \in M \\ sign_\sigma(i) & \text{otherwise} \end{cases} .$$

5) For every $i, j \in [0, n-1]$ compute

$$f_{M,\sigma}(i,j) \overset{\text{def}}{=} \begin{cases} 1 & \text{if } s_{M,\sigma}(i) > 0,\ s_{M,\sigma}(j) \geq 0, \text{ and } [\sigma^{-1}(j), j] \subset [\sigma^{-1}(i), i] \\ 1 & \text{if } s_{M,\sigma}(i) < 0,\ s_{M,\sigma}(j) < 0, \text{ and } [j, \sigma^{-1}(j)] \subset [i, \sigma^{-1}(i)] \\ 0 & \text{otherwise} \end{cases} ,$$

where $[a, b]$ is the set of elements $\{a \pmod n, a+1 \pmod n, \ldots, b \pmod n\}$.

Finally,

$$w_\kappa(\sigma) = \sum_{i \in [0,n-1] \text{ s.t. } s_{M,\sigma}(i) > 0} d_{M,\sigma}(i) + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\sigma}(i,j).$$

By Theorem 5.2, there is no perfect single-error-correcting code in S_5, using the Kendall's τ-distance. However, there exists a perfect single-error-correcting code in S_5, using the cyclic Kendall's τ-distance. The following 20 codewords form such a code.

$$\begin{array}{llll}
[0,1,2,3,4], & [0,2,4,1,3], & [0,3,1,4,2], & [0,4,3,2,1] \\
[1,2,3,4,0], & [2,4,1,3,0], & [3,1,4,2,0], & [4,3,2,1,0] \\
[2,3,4,0,1], & [4,1,3,0,2], & [1,4,2,0,3], & [3,2,1,0,4] \\
[3,4,0,1,2], & [1,3,0,2,4], & [4,2,0,3,1], & [2,1,0,4,3] \\
[4,0,1,2,3], & [3,0,2,4,1], & [2,0,3,1,4], & [1,0,4,3,2].
\end{array}$$

Note, that the permutations in each column are cyclic shifts of the first permutation in the column. Moreover, the permutations in the first row are of the form $[0, \alpha, 2\alpha, 3\alpha, 4\alpha]$, where $1 \leq \alpha \leq 4$ and the multiplication is taken modulo 5. These 20 codewords also form a code with minimum Kendall's τ-distance three in S_5, which is the largest known such code.

Another related distance measure is defined when we consider the following equivalence relation E on S_n. For two permutations $\sigma, \pi \in S_n$, $(\sigma, \pi) \in E$ if there exist an integer i, $1 \leq i \leq n$, such that $\sigma = [\pi(i), \pi(i+1), \ldots, \pi(n-1), \pi(0), \ldots, \pi(i-1)]$. If $\theta = [1, 2, \ldots, n-1, 0]$ then the permutation σ can be written as the multiplication $\theta^i \circ \pi$. Clearly, E is an equivalence relation on S_n with $(n-1)!$ equivalence classes, each one of size n. Each such equivalence class can be regarded as a necklace with the integers $0, 1, \ldots, n-1$. Let S_n^c denote the set of these $(n-1)!$ equivalence classes (necklaces). Two elements of S_n^c are at Kendall's τ-distance one if there exist two representatives of the two necklaces whose Kendall's τ-distance in one. The Kendall's τ-distance on S_n^c is also bipartite. Note that, the size of a sphere of radius one in this metric space is n (similarly to the size of a sphere of radius one in the cyclic Kendall's τ-metric on S_n), but there cannot be any distinction between the Kendall's τ-metric and the cyclic Kendall's τ-metric on S_n^c.

One can easily verified that

Lemma 5.14 *For a given $\sigma \in S_n$, $n \geq 2$, the minimum cyclic Kendall's τ-distance of the equivalence class of σ, i.e. $\{\pi \in S_n \ : \ (\sigma, \pi) \in E\}$, is $n-1$.*

Let $\mathcal{C} \subset S_n^c$ be a code with minimum Kendall's τ-distance $d \leq n-1$. Lemma 5.14 implies that the union of the equivalence classes of codewords from $\mathcal{C}$ is a code in S_n with minimum Kendall's τ-distance at least d. For example, $[0,1,2,3,4], [0,2,4,1,3], [0,3,1,4,2]$, and $[0,4,3,2,1]$ are four representatives of four equivalence classes in S_5^c, and the union of their equivalence classes forms the perfect single-error-correcting code in S_5 with minimum cyclic Kendall's τ-distance 3.

Example 5.15 *Let* $\mu = [0, 1, 2, 4, 3, 6, 5]$ *and let* $\nu = [0, 1, 2, 3, 6, 4, 5]$*. For a scalar* $x \in \{1, 2, 3, 4, 5, 6\}$ *and a permutation* $\sigma \in S_7$*, let* $x \cdot \sigma \overset{\text{def}}{=} [x \cdot \sigma(0), x \cdot \sigma(1), \ldots, x \cdot \sigma(6)]$*, where the multiplication is taken modulo* 7*. The code*

$$\mathcal{C} = \{\theta^i \circ (x \cdot \sigma) \circ \theta^j \ : \ \sigma \in \{\mu, \nu\}, \ 1 \leq x \leq 6, \ 0 \leq i, j \leq 6\}$$

is a code in S_7 *of size* $2 \cdot 7 \cdot 7 \cdot 6 = 588$ *whose minimum cyclic Kendall's* τ*-distance is* 3*. The code* $\mathcal{C}$ *is the largest known single-error-correcting code in* S_7 *(the previous known lower bound on the size of a single-error-correcting code in* S_7 *was* 526 *[44]. The upper bound on the size of such code is less than 720 since there is no perfect single-error-correcting code in* S_7 *with the Kendall's* τ*-distance). Clearly, this code has a very large automorphism group.*

Chapter 6

Systematic Codes for Permutations with Kendall's τ-Metric

The rank modulation scheme has motivated the study of permutation codes in S_n, with the Kendall's τ-metric [43, 44]. Recently, to improve the number of rewrites, the model of rank modulation was extended such that multiple cells can share the same ranking [24, 25]. Thus, the cells no longer determine permutations but rather multipermutations, which are also known as permutations with repetitions. Error-correcting codes for multipermutations subject to the Kendall's τ-metric were presented in [74] and also studied in [7].

The main goal of this chapter is to construct *systematic* error-correcting codes for permutations. This concept for permutations was proposed in [108, 109]. A systematic code $\mathcal{C}$ for permutations in S_n is a code consists of $k!$ codewords. Each permutation of S_k is a sub-permutation of exactly one codeword of $\mathcal{C}$. The k symbols of $[k]$ are called *information symbols* while the $n-k$ symbols of $[n] \setminus [k]$ are called *redundancy symbols.*

In this work some of the results in [108, 109] are improved. A construction of systematic t-error-correcting codes for permutations that uses r redundancy symbols is presented in Section 6.2. This construction is based on two ingredients. The first is a partition of S_k into t-error-correcting codes. The second is a code $\mathcal{C}_r$ for multipermutations from the multiset $\{0^k, k+1, \ldots, k+r\}$ with minimum Kendall's τ-distance $2t$, whose size is the number of parts in the partition. Each code from the partition of S_k will be substituted into a different codeword of $\mathcal{C}_r$. We will also perform some analysis for the number of redundancy symbols of these codes. For a given large enough number of information symbols k, and for any integer t, the construction uses less redundancy symbols than the number of redundancy symbols in the codes of the known constructions. In particular, for a given t and for sufficiently large k we can obtain $r = t + 1$. The construction will be generalized in Section 6.3 to systematic codes for multipermutations.

6.1 Error-Correcting Codes

For the construction of systematic error-correcting codes for permutations and multipermutations given in Sections 6.2 and 6.3, general error-correcting codes for multipermutations are needed. In this section constructions for such error-correcting codes for multipermutations with the Kendall's τ-distance are discussed. Such a construction was given in [74]. It is based on a metric embedding (mapping) of $S(\mathcal{M})$, where $\mathcal{M}$ is a balanced multi-set, into the metric space $\mathbb{Z}^{n-m}$, where m is the multiplicity of the ranks. The *Manhattan distance* (also called the L_1-distance) is used in $\mathbb{Z}^{n-m}$. This construction is a generalization of the constructions in [5, 44] for error-correcting codes for permutations.

Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^N$, $\mathbf{x} = (x_1, x_2, \ldots, x_N)$, $\mathbf{y} = (y_1, y_2, \ldots, y_N)$. Recall, that the Manhattan distance $d_M(\mathbf{x}, \mathbf{y})$ is defined by

$$d_M(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} \sum_{i=1}^{N} |x_i - y_i|.$$

This metric embedding (mapping) is injective and for every two multipermutations σ and π in $S(\mathcal{M})$, $d_K(\sigma, \pi)$ is greater or equal to the Manhattan distance between their images in $\mathbb{Z}^{n-m}$. These properties allow to construct error-correcting codes in $S(\mathcal{M})$ from error-correcting codes in the Manhattan metric over $\mathbb{Z}^{n-m}$.

We present a slightly modified version of this mapping. It will be defined on $S(\mathcal{M})$, where $\mathcal{M}$ is any multi-set, not necessarily a balanced multi-set. We will also restrict its range to its image, in order to obtain a bijective mapping. This is important for encoding purpose. We will show an encoding of $S(\mathcal{M})$, based on the enumerative encoding algorithm of Cover [17] in the full version of this paper.

A vector $\mathbf{x} = (x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k$ is *monotone* if $x_1 \geq x_2 \geq \ldots \geq x_k$. For a set S of integers let $[S]^k$ be the set of all monotone vectors of length k over S. Let

$$[\mathbb{Z}]^{\mathcal{M}} \overset{\text{def}}{=} [\mathbb{Z}_{n_1+1}]^{m_2} \times [\mathbb{Z}_{n_2+1}]^{m_3} \times \ldots \times [\mathbb{Z}_{n_{\ell-1}+1}]^{m_\ell}.$$

The mapping $\psi : S(\mathcal{M}) \to [\mathbb{Z}]^{\mathcal{M}}$ is defined as follows. For every $\sigma \in S(\mathcal{M})$, $\psi(\sigma)$ is the vector $\mathbf{x} \in [\mathbb{Z}]^{\mathcal{M}}$, $\mathbf{x} = (\mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_\ell)$, where for each i, $2 \leq i \leq \ell$, $\mathbf{x}_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,m_i})$, and for each r, $1 \leq r \leq m_i$,

$$x_{i,r} \overset{\text{def}}{=} |\{k \ : \ k > \sigma^{-1}(v_{i,r}) \wedge \sigma(k) < v_i\}|.$$

Namely, $x_{i,r}$ counts the number of ranks, v_j, where $v_j < v_i$, which appear to the right of the rth appearance of v_i. For example, if $\sigma = [2, 1, 3, 4, 3, 2, 1, 4]$ then $\psi(\sigma) = (\mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) = ((2, 1), (2, 2), (3, 0))$.

Lemma 6.1 *The mapping ψ is bijective.*

Proof. Let $\sigma, \pi \in S(\mathcal{M})$, $\sigma \neq \pi$, and let $\psi(\sigma) = \mathbf{x}$, $\psi(\pi) = \mathbf{y}$, where $\mathbf{x} = (\mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_m)$ and $\mathbf{y} = (\mathbf{y}_2, \mathbf{y}_3, \ldots, \mathbf{y}_m)$. Let k be the largest integer in $[n]$ such that $\sigma(k) \neq \pi(k)$, and let $\sigma(k) = v_{i,r}$, $\pi(k) = v_{j,s}$. Assume with out loss of generality that $v_i < v_j$. Let $\sigma^{-1}(v_{j,s}) = k'$. By definition, $x_{j,s}$ is the number of positions $a \in \{k'+1, k'+2, \ldots, n\}$, where $\sigma(a) < v_j$. Similarly, $y_{j,s}$ is the number of positions $a \in \{k+1, k+2, \ldots, n\}$, where $\pi(a) < v_j$. Since $\sigma(\hat{k}) = \pi(\hat{k})$ for all $\hat{k} < k \leq n$ and since $\sigma(k) = v_i$, where $v_i < v_j$, it follows that $k < k'$ and $x_{j,r} < y_{j,r}$. Hence, $\mathbf{x} \neq \mathbf{y}$. This proves that ψ is injective. To complete the proof, the reader can readily verified that $|[\mathbb{Z}]^{m,\overrightarrow{r}}| = \frac{n!}{\prod_{i=1}^{m} r_i!} = |S(\mathcal{M})|$, and therefore, ψ is bijective.

□

Lemma 6.2 *For every two multipermutations $\sigma, \pi \in S(\mathcal{M})$, if $d_K(\sigma, \pi) = 1$ then $d_M(\psi(\sigma), \psi(\pi)) = 1$.*

Proof. Let $\sigma, \pi \in S(\mathcal{M})$ such that $d_K(\sigma, \pi) = 1$. Then there exists a $k \in [n]$ such that $\sigma = [\pi(1), \pi(2), \ldots, \pi(k-1), \pi(k+1), \pi(k), \pi(k+2), \ldots, \pi(n)]$ and $\pi(k) \neq \pi(k+1)$. Let $\pi(k) = v_{i,r}$, $\pi(k+1) = v_{j,s}$, and assume w.l.o.g. that $v_i < v_j$. Let $\psi(\sigma) = \mathbf{x}$ and $\psi(\pi) = \mathbf{y}$, $\mathbf{x} = (\mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_m)$, $\mathbf{y} = (\mathbf{y}_2, \mathbf{y}_3, \ldots, \mathbf{y}_m)$. For every $k' \notin \{k, k+1\}$, $1 \leq k' \leq n$, we have that $\sigma(k') = \pi(k') = v_{i',r'}$ for some $1 \leq i' \leq \ell$ and $1 \leq r' \leq m_{i'}$, and if $i' > 1$ then $x_{i',r'} = y_{i',r'}$. Since $v_{i,r} = \sigma(k+1) = \pi(k) < \pi(k+1) = \sigma(k) = v_{j,s}$ and $\sigma(k') = \pi(k')$ for all $k+1 < k' \leq n$, it follows that if $i > 1$ then $x_{i,r} = y_{i,r}$. Moreover, since $v_i < v_j$ it follows that $x_{j,s} = y_{j,s} + 1$. Then

$$d_M(\mathbf{x}, \mathbf{y}) = \sum_{i'=2}^{m} \sum_{b=1}^{r_{i'}} |x_{i',b} - y_{i',b}| = |x_{i,a} - y_{i,a}| = 1.$$

This completes the proof.

□

Lemma 6.3 *For any two multipermutations $\sigma, \pi \in S(\mathcal{M})$ we have*

$$d_M(\psi(\sigma), \psi(\pi)) \leq d_K(\sigma, \pi).$$

Proof. Let $d_K(\sigma, \pi) = s$. Then there exists a path $\Gamma : sigma = \rho_1 \to \rho_2 \to \ldots \to \rho_{s-1} \to \rho_{s+1} = \pi$ in the graphic representation of $S(\mathcal{M})$ under the Kendall's τ-distance, $G(\mathcal{M})$, i.e. $d_K(\rho_u, \rho_{u+1}) = 1$ for all $1 \leq u \leq s$. By Lemma 6.2 it follows that $d_M(\psi(\rho_u), \psi(\rho_{u+1})) = 1$ for all $1 \leq u \leq s$. By the triangle inequality it follows that

$$d_M(\psi(\sigma), \psi(\pi)) \leq \sum_{u=1}^{s} d_M(\psi(\rho_u), \psi(\rho_{u+1})) = s.$$

□

Let $\mathbb{Z}_q^N$ be the set of all vectors of length N over the alphabet $\mathbb{Z}_q$. For every two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^N$, the Lee distance $d_L(\mathbf{x}, \mathbf{y})$ is defined by

$$d_L(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} \sum_{i=1}^{N} \min\{|x_i - y_i|, q - |x_i - y_i|\}.$$

Clearly, $d_M(\mathbf{x}, \mathbf{y}) \geq d_L(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^N$. The set $[\mathbb{Z}]^{\mathcal{M}}$ is a subset of $\mathbb{Z}_q^{n-m_1}$, where $q > n_{\ell-1}$. Hence, $d_L(\psi(\sigma), \psi(\pi)) \leq d_K(\sigma, \pi)$ for every two multipermutations $\sigma, \pi \in S(\mathcal{M})$. We are now in a position to present a construction which transfers codes with the Lee metric to codes with the Kendall's τ-metric. The related theorem is a slight generalization of the result in [74]. This construction will be a major component in the main construction of systematic codes, which is the primary goal of this chapter.

Theorem 6.4 *If there exists a code $\mathcal{C}_L \subseteq \mathbb{Z}_q^{n-m_1}$, $q > n_{\ell-1}$, with minimum Lee distance d then there exists a code $\mathcal{C}_K \subseteq S(\mathcal{M})$ with minimum Kendall's τ-distance at least d and of size $|\mathcal{C}_K| = |\mathcal{C}_L \cap [\mathbb{Z}]^{\mathcal{M}}|$.*

Proof. Let $\mathcal{C}_K = \{\sigma \in S(\mathcal{M}) \ : \ \psi(\sigma) \in \mathcal{C}_L\}$. By Lemma 6.3 , the minimum distance of $\mathcal{C}_K$ is at least d. Since ψ is a bijection on $[\mathbb{Z}]^{\mathcal{M}}$ it follows that the size of $\mathcal{C}_K$ is exactly $|\mathcal{C}_L \cap [\mathbb{Z}]^{\mathcal{M}}|$.

□

By Theorem 6.4, error-correcting codes in $S(\mathcal{M})$ with the Kendall's τ-metric can be constructed from error-correcting codes over $\mathbb{Z}_q^{n-m_1}$ in the Lee metric. Next, we present some of the known constructions of error-correcting codes in the Lee metric and use Theorem 6.4 to obtain error-correcting codes in $S(\mathcal{M})$ and to estimate the size of these codes. First, we consider single-error-correcting codes in the Lee metric. Golomb and Welch [36] presented the following construction of a perfect linear single-error-correcting code in the Lee metric.

Theorem 6.5 *For every positive integer N, the code*

$$\mathcal{C}_L = \left\{ \mathbf{x} \in \mathbb{Z}_{2N+1}^N \;:\; \sum_{i=1}^{N} i \cdot x_i \equiv 0 \ (mod\ 2N+1) \right\}$$

is a perfect linear single-error-correcting code in $\mathbb{Z}_{2N+1}^N$ with the Lee metric.

The construction in Theorem 6.5 was used in [44] to construct single-error-correcting codes for permutations with the Kendall's τ-distance. Combining this construction with Theorem 6.4 implies the following corollary.

Corollary 6.6 *There exists a single-error-correcting code $\mathcal{C}_K \subset S(\mathcal{M})$ of size $|\mathcal{C}_K| \geq \frac{|S(\mathcal{M})|}{2(n-m_1)+1}$.*

The following construction was first proposed by Varshamov and Tenengolts [98] (see also [5]) for codes which correct a single asymmetric error. Let $||\mathbf{x}||$ denote the Manhattan weight of $\mathbf{x}$.

Theorem 6.7 *Let $q \geq N$ and let $h_1, h_2, \dots, h_N$ be integers, $0 < h_i < q$ for all $1 \leq i \leq N$. Assume that for every $\mathbf{e} \in \mathbb{Z}^N$ with $||\mathbf{e}|| \leq t$, the sums $\sum_{i=1}^{N} e_i \cdot h_i$ are all distinct modulo q. Then the code*

$$C = \left\{ \mathbf{x} \in \mathbb{Z}_q^N \mid \sum_{i=1}^{N} x_i \cdot h_i \equiv 0 \ (mod\ q) \right\}$$

is a linear t-error-correcting code in $\mathbb{Z}_q^N$ with the Lee metric.

In order to use the construction in Theorem 6.7 we need the following theorem of Barg and Mazumdar [5].

Theorem 6.8 *Let q be a power of a prime and $M = (q^{t+1}-1)/(q-1)$. Let*

$$M_t = \begin{cases} t(t+1)M, & t \text{ is odd} \\ t(t+2)M, & t \text{ is even} \end{cases}$$

Then there exist integers $h_1, h_2, \dots, h_{q+1}$ such that for all $\mathbf{e} \in \mathbb{Z}^{q+1}$, $||\mathbf{e}|| \leq t$, the sums $\sum_{i=1}^{q+1} e_i h_i$ are all distinct modulo M_t.

The construction in Theorem 6.7 of a t-error-correcting code in the Lee metric, combined with Theorem 6.8, was used in [5] to construct t-error-correcting codes for permutations with the Kendall's τ-metric, and also used in [74] to construct t-error-correcting codes with the Kendall's τ-metric for multipermutations over a balanced multi-set. Other constructions of codes with the Kendall's τ-distance that might useful in this context can be found in [61]. By combining the construction in Theorems 6.4, 6.7, and 6.8 we obtain the following Corollary.

Corollary 6.9 *Let $M = ((n-m_1-1)^{t+1}-1)/(n-m_1-2)$, where $n-m_1-1$ is a power of a prime. There exists a t-error-correcting code $\mathcal{C} \subset S(\mathcal{M})$ in the Kendall's τ-metric, whose size satisfies*

$$|\mathcal{C}| \geq \begin{cases} \frac{|S(\mathcal{M})|}{t(t+1)M}, & t \textit{ is odd} \\ \frac{|S(\mathcal{M})|}{t(t+2)M}, & t \textit{ is even} \end{cases}$$

Now, after presenting the concepts and ideas in constructions of error-correcting codes for multipermutations, we are ready to present our main results on systematic error-correcting codes for permutations and multipermutations in the next two sections.

6.2 Systematic ECC for Permutations

In this section we present systematic t-error-correcting codes for permutations. Let k, n be integers such that $n \geq k \geq 1$. For a permutation $\alpha \in S_n$, we define $\alpha_{\downarrow k}$ to be the permutation obtained from α by deleting all the elements of $\{k+1, k+2, \ldots, n\}$ from α. We also define $\alpha_{k \mapsto 0}$ to be the multipermutation obtained from α by replacing in α every element of $\{1, 2, \ldots, k\}$ by 0. For example, if $\alpha = [2, 5, 4, 1, 3, 6]$ and $k = 3$ then $\alpha_{\downarrow k} = [2, 1, 3]$ and $\alpha_{k \mapsto 0} = [0, 5, 4, 0, 0, 6]$. In [108], the authors define systematic codes in the following way. A code $\mathcal{C} \subseteq S_n$ is an (n, k) *systematic* code if for every $\sigma \in S_k$ there exists exactly one $\alpha \in \mathcal{C}$ such that $\alpha_{\downarrow k} = \sigma$, which implies that $|\mathcal{C}| = k!$. The number of *redundancy symbols* of an (n, k) systematic code is $r = n - k$.

Let r be a positive integer and let $\mathcal{M}_{k,r} \overset{\text{def}}{=} \{0^k, k+1, k+2, \ldots, k+r\}$. For every permutation $\sigma \in S_k$ and multipermutation $\rho \in S(\mathcal{M}_{k,r})$, we define the permutation $\sigma * \rho$ to be the permutation in S_{k+r} obtained from ρ by replacing the k zeros in ρ by the k elements of $\{1, 2, \ldots, k\}$, in the same order as in σ. For example, if $k = 4$, $r = 3$, $\rho = [0, 6, 0, 0, 5, 7, 0]$, and $\sigma = [2, 4, 1, 3]$, then $\sigma * \rho = [2, 6, 4, 1, 5, 7, 3]$.

Lemma 6.10 *For every $\rho \in S(\mathcal{M}_{k,r})$ and $\sigma \in S_k$ we have*

1) $(\sigma * \rho)_{\downarrow k} = \sigma$.

2) $(\sigma * \rho)_{k\mapsto 0} = \rho$.

By Lemma 4.5 we have.

Lemma 6.11 *Let $\sigma, \pi \in S_k$ and $\rho_1, \rho_2 \in S(\mathcal{M}_{k,r})$. Then*

$$d_K(\sigma * \rho_1, \pi * \rho_2) \geq d_K(\sigma, \pi) + d_K(\rho_1, \rho_2) \ .$$

We are now in a position to present our construction for systematic error-correcting codes for permutations.

Theorem 6.12 *Let $h_1, h_2, \ldots, h_{k-1}$, and M_t, be integers such that for every $\mathbf{e} \in \mathbb{Z}^{k-1}$ with $||\mathbf{e}|| \leq t$, the sums $\sum_{i=1}^{k-1} e_i h_i$ are all distinct modulo M_t. Assume further that there exists a code $\mathcal{C}_r \subset S(\mathcal{M}_{k,r})$ with minimum Kendall's τ-distance $2t$ and of size $|\mathcal{C}_r| \geq M_t$. Let $\rho_0, \rho_1, \ldots, \rho_{M_t-1}$ be distinct multipermutations in $\mathcal{C}_r$. Let $\mathcal{C}$ be the code in S_{k+r} defined as follows.*

$$\mathcal{C} = \{\sigma * \rho_j \ : \ \sigma \in S_k, \ \sum_{i=1}^{k-1} (\psi(\sigma))_{i+1} h_i \equiv j \ (\ mod \ M_t)\}.$$

Then the code $\mathcal{C}$ is a $(k+r, k)$ systematic t-error-correcting code.

Proof. The code $\mathcal{C}$ from Theorem 6.12 is clearly a $(k+r, k)$-systematic code. We have to show that the minimum Kendall's τ-distance of $\mathcal{C}$ is at least $2t+1$. Let $\alpha, \beta \in \mathcal{C}$ be two distinct codewords and let $\alpha_{\downarrow k} = \sigma$, $\alpha_{k\mapsto 0} = \rho_{j_1}$, $\beta_{\downarrow k} = \beta$, $\beta_{k\mapsto 0} = \rho_{j_2}$. By definition of $\mathcal{C}$ we have

$$\sum_{i=1}^{k-1} (\psi(\sigma))_{i+1} h_i \equiv j_1 \ (\ \mathrm{mod} \ M_t),$$

and

$$\sum_{i=1}^{k-1} (\psi(\pi))_{i+1} h_i \equiv j_2 \ (\ \mathrm{mod} \ M_t).$$

We have to show that $d_K(\alpha, \beta) \geq 2t+1$. By Lemma 6.11

$$d_K(\alpha, \beta) \geq d_K(\sigma, \pi) + d_K(\rho_{j_1}, \rho_{j_2}).$$

If $d_K(\sigma, \pi) \geq 2t+1$ then $d_K(\alpha, \beta) \geq 2t+1$. Assume $d_K(\sigma, \pi) \leq 2t$. We show that $j_1 \neq j_2$. Assume to the contrary that $j_1 = j_2$. Then

$$\sum_{i=1}^{k-1} ((\psi(\sigma))_{i+1} - (\psi(\pi))_{i+1}) h_i \equiv 0 \ (\ \mathrm{mod} \ M_t).$$

Since $d_K(\sigma,\pi) \leq 2t$ it follows that $d_M(\psi(\sigma),\psi(\pi)) \leq 2t$. This implies that there exist $\mathbf{e},\mathbf{f} \in \mathbb{Z}^{k-1}$, where $\mathbf{e} = (e_1,e_2,\ldots,e_{k-1})$, $\mathbf{f} = (f_1,f_2,\ldots,f_{k-1})$, and $||\mathbf{e}|| \leq t$, $|\mathbf{f}| \leq t$, such that $\psi(\sigma)+\mathbf{e} = \psi(\pi)+\mathbf{f}$.

Then

$$\sum_{i=1}^{k-1}(f_i - e_i)h_i \equiv 0 \text{ (mod } M_t).$$

It follows that

$$\sum_{i=1}^{k-1} f_i h_i \equiv \sum_{i=1}^{k-1} e_i h_i \equiv 0 \text{ (mod } M_t),$$

which is a contradiction to the assumption on the integers $h_1, h_2, \ldots, h_{k-1}$. Hence, $j_1 \neq j_2$, and therefore, $d_K(\rho_{j_1},\rho_{j_2}) \geq 2t$ which implies that

$$d_K(\alpha,\beta) \geq d_K(\sigma,\pi) + d_K(\rho_{j_1},\rho_{j_2}) \geq 1+2t.$$

This completes the proof.

□

Example 6.13 *Let k be an integer, let $r=2$, and let $M_1 = 2(k-1)+1$. As in Theorem 6.5, for every $\mathbf{e} \in \mathbb{Z}^{k-1}$, $||\mathbf{e}|| \leq 1$, the sums $\sum_{i=1}^{k-1} e_i i$ are all distinct modulo M_1. For the construction, we need a code in $S(\mathcal{M}_{k,2})$ with minimum distance 2 and of size at least M_1. To this end, fix a multipermutation $\rho \in S(\mathcal{M}_{k,2})$ and consider the codes $\mathcal{C}_2^e = \{\gamma \in S(\mathcal{M}_{k,2}) \ : \ d_K(\rho,\gamma) \equiv 0 \text{ (} mod \text{ } 2)\}$ and $\mathcal{C}_2^o = \{\gamma \in S(\mathcal{M}_{k,2}) \ : \ d_K(\rho,\gamma) \equiv 1 \ (mod \ 2)\}$. By Lemma 4.6, the minimum distance of both $\mathcal{C}_2^e$ and $\mathcal{C}_2^o$ is 2. Clearly, the size of either $\mathcal{C}_2^e$ or $\mathcal{C}_2^o$ is at least $\frac{|S(\mathcal{M}_{k,2})|}{2} = \frac{(k+2)!}{k!\cdot 2} = \frac{(k+2)(k+1)}{2}$. For all $k \geq 1$ we have that $\frac{(k+2)(k+1)}{2} \geq 2(k-1)+1$ and hence by Theorem 6.12 there exists a $(k+2,k)$ systematic single-error-correcting code.*

Example 6.14 *Let k be an integer such that $k-2$ is a power of a prime, let $r=3$, and let $M_2 = 8((k-2)^3-1)/(k-3) = 8((k-2)^2+k-1)$. By Theorem 6.8, it follows that there exist $h_1,h_2,\ldots,h_{k-1}$ such that for all $\mathbf{e} \in \mathbb{Z}^{k-1}$, $||\mathbf{e}|| \leq 2$, the sums $\sum_{i=1}^{k-1} e_i h_i$ are all distinct modulo M_2. We have to show the existence of a code in $S(\mathcal{M}_{k,3})$ with minimum distance 4 and of size at least M_2. By Corollary 6.6, there exists a single-error-correcting code $\mathcal{C}_K \subset S(\mathcal{M}_{k,3})$ of size $|\mathcal{C}_K| \geq \frac{|S(\mathcal{M}_{k,3})|}{2\cdot 3+1}$. We fix a multipermutation $\rho \in S(\mathcal{M}_{k,3})$ and consider the codes $\mathcal{C}_3^e = \{\gamma \in \mathcal{C}_K \ : \ d_K(\rho,\gamma) \equiv 0 \ (mod \ 2)\}$ and $\mathcal{C}_3^o = \{\gamma \in \mathcal{C}_K \ : \ d_K(\rho,\gamma) \equiv 1 \ (mod \ 2)\}$. By Lemma 4.6, it follows that the minimum distance of the codes $\mathcal{C}_3^e$ and $\mathcal{C}_3^o$ is 4. One of these codes* *must be of size at least* $\frac{|\mathcal{C}_K|}{2}$. *If* $\mathcal{C}_3$ *is this code then* $|\mathcal{C}_3| \geq \frac{|S(\mathcal{M}_{k,3})|}{14} = \frac{(k+3)!}{k!\cdot 14} = \frac{(k+3)(k+2)(k+1)}{14}$. *For all* $k \geq 113$ *we have that* $\frac{(k+3)(k+2)(k+1)}{14} \geq 8((k-2)^2+k-1)$ *and hence by Theorem 6.12, if* $k \geq 113$ *such that* $k-2$ *is a power of a prime then there exists a* $(k+3,k)$ *systematic double-error-correcting code.*

In [108, 109] a construction of systematic $(k, k+2)$ single-error-correcting codes for permutations with two redundancy symbols, which is the same number of redundancy symbols as in Example 6.13, was given. The authors in [108, 109] construct (n, k) systematic t-error-correcting codes with at most $2t+1$ redundancy symbols. If k and t have the same magnitude then our construction uses the same number of redundancy symbols, but for most parameters the number of redundancy symbols of the codes in our construction is considerably better. Our main theorem is stated as follows.

Theorem 6.15 *Let* k *be an integer, let* $t = k^\epsilon$ *be a positive integer, and let* $r = \lceil \mu t \rceil$, *where*

$$\begin{cases} \mu > 1+\epsilon & \textit{for} \quad 0 \leq \epsilon \leq 1 \\ \mu > 1+\frac{1}{\epsilon} & \textit{for} \quad 1 < \epsilon \ . \end{cases}$$

If k *is large enough then there exists a* $(k+r, k)$ *systematic* t*-error-correcting code.*

Proof. Let $k' = 2^{\lceil \log_2 k \rceil}$, let $M = ((k'-2)^{t+1}-1)/(k'-3)$, and let

$$M_t = \begin{cases} t(t+1)M, & t \text{ is odd} \\ t(t+2)M, & t \text{ is even} \end{cases}$$

Since $k' \geq k$ and by Theorem 6.8, it follows that there exist $h_1, h_2, \ldots, h_{k-1}$ such that for all $\mathbf{e} \in \mathbb{Z}^{k-1}$, $||\mathbf{e}|| \leq t$, the sums $\sum_{i=1}^{k-1} e_i h_i$ are all distinct modulo M_t. We have to show the existence of a code in $S(\mathcal{M}_{k,r})$ with minimum distance $2t$ and of size at least M_t. Let $r' = 2^{\lceil \log_2 r \rceil}$, and let $M_r = ((r'-1)^{t+1}-1)/(r'-2)$. Since $r \leq r'$ and by corollary 6.9 it follows that there exists a t-error-correcting code $\mathcal{C}_K \subset S(\mathcal{M}_{k,r})$ in the Kendall's τ-metric, whose size satisfies

$$|\mathcal{C}_K| \geq \begin{cases} \frac{|S(\mathcal{M}_{k,r})|}{t(t+1)M_r}, & t-1 \text{ is odd} \\ \frac{|S(\mathcal{M}_{k,r})|}{t(t+2)M_r}, & t-1 \text{ is even} \end{cases}$$

We have to show that if k is large enough then $|\mathcal{C}_K| \geq M_t$. Since

$$|\mathcal{C}_K| \geq \frac{|S(\mathcal{M}_{k,r})|}{2(t-1)(t+1)M_r} \geq \frac{(k+r)!(r-2)}{k! \cdot 2(t-1)(t+1)((2r-1)^{t+1}-1)},$$

and

$$M_t \leq t(t+2)(2k)^t$$

It is sufficient to show that if k is large enough then

$$(k+r)! > t^4 k^t k! 4^t r^t. \tag{6.1}$$

By the Stirling approximation, $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$, and therefore, the right hand side of inequality (6.1) is approximately

$$\sqrt{2\pi k}\left(\frac{k}{e}\right)^k t^4 k^t (4\mu t)^t \leq \sqrt{2\pi k} e^{-k} k^{k+4\epsilon+k^\epsilon+\epsilon k^\epsilon} (4\mu)^{k^\epsilon}.$$

Similarly, the left hand side of inequality (6.1) is approximately

$$\sqrt{2\pi(k+\mu k^\epsilon)}\left(\frac{k+\mu k^\epsilon}{e}\right)^{k+\mu k^\epsilon}$$

Hence, it is enough to show that

$$(k+\mu k^\epsilon)^{k+\mu k^\epsilon} > (4e^\mu \mu)^{k^\epsilon} k^{k+4\epsilon+k^\epsilon+\epsilon k^\epsilon} \tag{6.2}$$

The left hand side of inequality (6.2) is at least $k^{k+\mu k^\epsilon}$.
For $0 \leq \epsilon \leq 1$, we show that

$$k^{k+\mu k^\epsilon} > (4e^\mu \mu)^{k^\epsilon} k^{k+4\epsilon+k^\epsilon+\epsilon k^\epsilon}.$$

If k is large enough and

$$k + \mu k^\epsilon > k + k^\epsilon + \epsilon k^\epsilon,$$

i.e. $\mu > 1+\epsilon$, then inequality (6.1) is satisfied.
For $\epsilon > 1$, the left hand side of inequality (6.2) is at least $(\mu k^\epsilon)^{k+\mu k^\epsilon}$.
If k is large enough and

$$\epsilon k + \epsilon \mu k^\epsilon > k + k^\epsilon + \epsilon k^\epsilon,$$

i.e. $\mu > 1 + \frac{1}{\epsilon}$, then inequality (6.1) is satisfied.

□

The following corollary is a special case of Theorem 6.15.

Corollary 6.16 *Let t be an integer and let $r = t+1$. Then there exists an integer K_t such that for every integer $k \geq K_t$ there exists a $(k+r,k)$ systematic t-error-correcting code.*

6.3 Systematic ECC for Multipermutations

In this section we generalize the construction in Section 6.2 to obtain systematic error-correcting codes for multipermutations. In the most general definition of systematic codes for multipermutations we have a multiset $\mathcal{K}$ with k elements (with repetitions) serving as the information symbols and a multiset $\mathcal{R}$ with r elements serving as the redundancy symbols. The intersection between $\mathcal{K}$ and $\mathcal{R}$ must be empty. The codewords are multipermutations over the multiset $\mathcal{K} \cup \mathcal{R}$. The number of codewords in the error-correcting code must be the number of distinct multipermutations over the multiset $\mathcal{K}$. In the systematic code $\mathcal{C}$ each multipermutation over the multiset $\mathcal{K}$, appears as a sub-multipermutation of exactly one codeword from $\mathcal{C}$. The construction for systematic multipermutations will be a direct generalization of the construction in Theorem 6.12. Instead of the set $\mathcal{M}_{k,r}$ we use the set $\mathcal{M}$ defined by $\mathcal{M} \overset{\text{def}}{=} \{0^k\} \cup \mathcal{R}$, where 0 is a symbol which does not appear in $\mathcal{R}$. The size of the code $\mathcal{C}_r \subset S(\mathcal{M})$ is at least M_t.

The challenge for systematic permutations codes is to minimize the number of redundancy symbols of the codes. For systematic error-correcting codes for multipermutations there is a tradeoff between the number of redundancy ranks and the magnitudes of their multiplicities. For example, in a systematic code for multipermutations with only one redundancy rank, the multiplicity of the redundancy rank might be large. However, by allowing two redundancy ranks, the multiplicity of each redundancy rank should be smaller. The construction in Theorem 6.12 allows any desirable number of redundancy ranks.

Example 6.17 *Let $\mathcal{K} = \{1^{m_1}, 2^{m_2}, \ldots, \ell^{m_\ell}\}$ be a multi-set which consists of $k = \sum_{i=1}^{\ell} m_i$ information symbols, let $\mathcal{R} = \{\ell+1, \ell+1\}$ and $\mathcal{M} = \{0^k, \ell+1, \ell+1\}$. Let $M_1 = 2(k-m_1)+1$. For every $\mathbf{e} \in \mathbb{Z}^{k-m_1}$, $||\mathbf{e}|| \leq 1$, the sums $\sum_{i=1}^{k-m_1} e_i i$ are all distinct modulo M_1. For the construction, we need a code in $S(\mathcal{M})$ with minimum distance 2 and of size at least M_1. To this end, fix a multipermutation $\rho \in S(\mathcal{M})$ and consider the codes $\mathcal{C}_2^e = \{\gamma \in S(\mathcal{M}) \ : \ d_K(\rho,\gamma) \equiv 0 \ (mod\ 2)\}$ and $\mathcal{C}_2^o = \{\gamma \in S(\mathcal{M}) \ : \ d_K(\rho,\gamma) \equiv 1 \ (mod\ 2)\}$. By Lemma 4.6 it follows that the minimum distance of both $\mathcal{C}_2^e$ and $\mathcal{C}_2^o$ is 2. Clearly, the size of either $\mathcal{C}_2^e$ or $\mathcal{C}_2^o$ is at least $\frac{|S(\mathcal{M})|}{2} = \frac{(k+2)!}{k! \cdot 2! \cdot 2} = \frac{(k+2)(k+1)}{4}$. For all $k \geq 1$ we have that $\frac{(k+2)(k+1)}{4} \geq 2(k-m_1)+1$ and hence by Theorem 6.12 there exists a systematic single-error-correcting code in $S(\mathcal{K} \cup \mathcal{R})$.*

Chapter 7

Constrained Codes for Rank Modulation

Motivated by the rank modulation scheme, a recent study by Sala and Dolecek explored the idea of constrained codes for permutations. The constraint studied by them is inherited by the inter-cell interference phenomenon in flash memories, where high-level cells can inadvertently increase the level of low-level cells. It was said that a permutation $\sigma \in S_n$ satisfies the *single-neighbor k-constraint* if $|\sigma_i - \sigma_{i+1}| \leq k$ for all $1 \leq i \leq n-1$. In this chapter, the model studied by Sala and Dolecek is extended into two constraints.

Definition 7.1 *Let n and k be positive integers such that $k < n$. A permutation $\sigma \in S_n$ is said to satisfy the* two-neighbor k-constraint *if for all i, $2 \leq i \leq n-1$, either $|\sigma(i-1) - \sigma(i)| \leq k$ or $|\sigma(i) - \sigma(i+1)| \leq k$. We denote by $A_{n,k}$ the set of all permutations in S_n satisfying the two-neighbor k-constraint. A* two-neighbor k-constrained code *is a subset of $A_{n,k}$. Finally, for $0 \leq \epsilon \leq 1$, the* capacity *of the two-neighbor k-constraint, where $k = \lceil n^\epsilon \rceil$, is defined as*

$$C(\epsilon) = \limsup_{n\to\infty} \frac{\log |A_{n,k}|}{\log n!}.$$

For example, the permutation $\sigma = [4, 7, 5, 3, 1, 2, 6]$ satisfies the two-neighbor 2-constraint but not the two-neighbor 1-constraint. Clearly, if $k = n-1$ then $A_{n,k} = S_n$. Note that the two-neighbor constraint does not distinguish between high-low-high and low-high-low patterns and thus eliminates them both. A weaker constraint which may fit better to the inter-cell interference problem is defined next.

Definition 7.2 *Let n and k be positive integers such that $k < n$. A permu-*

tation $\sigma \in S_n$ is said to satisfy the asymmetric two-neighbor k-constraint *if for all i, $2 \leq i \leq n-1$, either $\sigma(i-1)-\sigma(i) \leq k$ or $\sigma(i+1)-\sigma(i) \leq k$. The set of all permutations satisfying the asymmetric two-neighbor k-constraint is denoted by $B_{n,k}$. An* asymmetric two-neighbor k-constrained code *is a subset of $B_{n,k}$ and the constraint's capacity, where $k = \lceil n^{\epsilon} \rceil$, for $0 \leq \epsilon \leq 1$, is defined as*

$$\widetilde{C}(\epsilon) = \limsup_{n\to\infty} \frac{\log |B_{n,k}|}{\log n!}.$$

For example, the permutation $[5,3,1,6,4,2]$ satisfies the asymmetric two-neighbor 2-constraint but not the asymmetric two-neighbor 1-constraint. Note that every permutation which satisfies the two-neighbor k-constraint satisfies the asymmetric two-neighbor k-constraint as well and thus for any $0 \leq \epsilon \leq 1$, $C(\epsilon) \leq \widetilde{C}(\epsilon)$.

We show that the capacity of the first constraint is $(1+\epsilon)/2$ in case that $k = \Theta(n^{\epsilon})$ and the capacity of the second constraint is 1 regardless to the value of k. We also extend our results and study the capacity of these two constraints combined with error-correction codes in the Kendall's τ-metric.

7.1 The Two-Neighbor Constraint

In this section we study the two-neighbor constraint and in particular find its capacity. This will be done first by a construction of two-neighbor k-constrained codes which provides a lower bound on the capacity. The construction is based upon assigning permutations into a special family of multipermutations. Then, we will show how to bound the size of the set $A_{n,k}$ which will result with an upper bound on the capacity that will coincide with the lower bound.

We denote by $\mathcal{M}_{\ell,m} = \{1^m, 2^m, \ldots, \ell^m\}$ the balanced multiset whose ranks are the elements of $[\ell]$, each rank appears m times (definition of a balanced multiset can be found in 4. The set of all multipermutations over $\mathcal{M}_{\ell,m}$ is denoted by $P_{\ell,m}$.

Note, that multipermutations, besides of being a tool in our solutions, find interest also in flash memory applications. The rank modulation scheme was recently generalized such that multiple cells can hold the same rank and thus represent a multipermutation; see e.g. [24, 25]. As a consequence, error-correction codes for multipermutations have attracted attention as well [7, 74]. Hence, the generalization of the aforementioned constraints and similar ones for multipermutations is also very important and interesting, however is out of the scope of this work.

For an even integer m, the set $D_{\ell,m} \subseteq P_{\ell,m}$ is defined as follows. A multipermutation $\rho \in P_{\ell,m}$ belongs to $D_{\ell,m}$ if for every j, $1 \leq j \leq \ell m/2$, $\rho(2j-1) = \rho(2j)$. For example, let $\rho = [1,1,2,2,2,2,3,3,1,1,3,3]$. Then $\rho \in k = D_{3,4}$ since $\rho(1) = \rho(2)$, $\rho(3) = \rho(4)$, and so on. The size of $D_{\ell,m}$ is equal to the size of $P_{\ell,m/2}$.

Recall that for a multipermutation $\rho \in P_{\ell,m}$ and permutations γ_1, γ_2, $\ldots$, γ_ℓ, such that $\gamma_i \in S([(i-1)m+1, im])$ for $i \in [\ell]$, the assignment of the permutations $\gamma_1, \gamma_2, \ldots, \gamma_\ell$ in the multipermutation ρ is the permutation $\alpha = \rho(\gamma_1, \gamma_2, \ldots, \gamma_\ell) \in S_{\ell m}$ defined as follows. For all $1 \leq j \leq n$, if $\rho(j) = i_r$ then $\alpha(j) = \gamma_i(r)$. Recall, also that by Lemma 4.2 the assignment of the permutations γ_i in the multipermutation ρ is an injective operation. This fact will be useful in the following construction of a two-neighbor k-constrained code.

Construction 7.3 *Let $n = \ell(k+1)$, where k is an odd positive integer and ℓ is a positive integer. Let $\mathcal{C}_{n,k}^{sym} \subseteq S_n$ be the code consists of all the permutations $\sigma \in S_n$ of the form $\sigma = \rho(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$, where $\rho \in D_{\ell,k+1}$ and $\gamma_i \in S([(i-1)(k+1)+1, i(k+1)])$, for $i \in [\ell]$. That is,*

$$\mathcal{C}_{n,k}^{sym} = \left\{ \rho(\gamma_1, \ldots, \gamma_\ell) : \begin{array}{c} \rho \in D_{\ell,k+1}, \text{ and for all } i \in [\ell], \\ \gamma_i \in S([(i-1)(k+1)+1, i(k+1)]) \end{array} \right\}.$$

The correctness of Construction 7.3 as well as the code cardinality are proved in the next lemma.

Lemma 7.4 *Let n, k, ℓ be as specified in Construction 7.3. Then, the code $\mathcal{C}_{n,k}^{sym}$ is a two-neighbor k-constrained code and its cardinality is*

$$|\mathcal{C}_{n,k}^{sym}| = \frac{\left(\frac{n}{2}\right)!(k+1)!^\ell}{\left(\frac{k+1}{2}\right)!^\ell}.$$

Proof. Let $\sigma \in \mathcal{C}_{n,k}^{sym}$. Then there exist $\rho \in D_{\ell,k+1}$, and $\gamma_1, \gamma_2, \ldots, \gamma_\ell$, where $\gamma_i \in S([(i-1)(k+1)+1, i(k+1)])$, for all $i \in [\ell]$, such that $\sigma = \rho(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$. Let $2 < j \leq n-1$ be an odd integer and assume that $\rho(j) = i_r$ for some $i \in [\ell]$ and $r \in [k+1]$. By the definition of $D_{\ell,k+1}$, it follows that $\rho(j+1) = i_{r+1}$. Hence, $\sigma(j) = \gamma_i(r) \in [(i-1)(k+1)+1, i(k+1)]$ and similarly $\sigma(j+1) = \gamma_i(r+1) \in [(i-1)(k+1)+1, i(k+1)]$. It follows that $|\sigma(j) - \sigma(j+1)| \leq k$. The case of j even is handled the same with respect to the symbol in position $j-1$. Thus, σ satisfies the two-neighbor k-constraint.

For the computation of the cardinality of $\mathcal{C}_{n,k}^{sym}$, note that by Lemma 4.2 it follows that every choice of $\rho \in D_{\ell,k+1}$ and $\gamma_1, \gamma_2, \ldots, \gamma_\ell$, where $\gamma_i \in S([(i-1)(k+1)+1, i(k+1)])$, for $i \in [\ell]$, generates a different codeword of the form $\rho(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$. Therefore,

$$|\mathcal{C}_{n,k}^{sym}| = |D_{\ell,k+1}| \cdot (k+1)!^{\ell} = \frac{(\frac{n}{2})!(k+1)!^{\ell}}{(\frac{k+1}{2})!^{\ell}}.$$

□

Even though Construction 7.3 provides two-neighbor constrained codes only to the case where k is odd, it can be easily modified for the case that k is even as well. In any event, we will not need this modification in order to calculate a lower bound on the capacity, which is stated in the next theorem.

Theorem 7.5 *For all* $0 \le \epsilon \le 1$, $C(\epsilon) \ge \frac{1+\epsilon}{2}$.

Proof. Assume that $k = \lceil n'^{\epsilon} \rceil$ that $n' = \ell(k+1)$, for some integer ℓ. By Lemma 7.4 we have that

$$|A_{n',k}| = \Omega\left(\frac{\left(\frac{n'}{2}\right)!(k+1)!^{\frac{n'}{k+1}}}{\left(\frac{k+1}{2}\right)!^{\frac{n'}{k+1}}}\right) = \Omega\left(n'^{\left(\frac{1+\epsilon}{2}\right)n'}\right).$$

Then,

$$\lim_{n'\to\infty} \frac{\log |A_{n',k}|}{\log n'!} \ge \lim_{n'\to\infty} \frac{\log\left(n'^{\left(\frac{1+\epsilon}{2}\right)n'}\right)}{\log n'!} = \frac{1+\epsilon}{2}.$$

, where the limit is over values of n' that are divided by k. Thus, $\frac{1+\epsilon}{2}$ is a partial limit of the sequence $\frac{\log|A_{n,k}|}{\log n!}$ and therefore $C(\epsilon) \ge \frac{1+\epsilon}{2}$

□

In order to derive an upper bound on the capacity $C(\epsilon)$ we show an upper bound on the size of $A_{n,k}$.

Lemma 7.6 *For all positive integers* n, k *such that* $k < n$,

$$|A_{n,k}| \le 4^{n-1} k^{\frac{n}{2}} n^{\frac{n}{2}+1}.$$

Proof. Let $\psi : A_{n,k} \to \mathbb{Z}^n$ be the following mapping. For a permutation $\sigma \in A_{n,k}$, $\psi(\sigma) = \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$, where $x_1 = \sigma(1)$, and for each i, $2 \le i \le n$, $x_i = \sigma(i) - \sigma(i-1)$. Clearly, ψ is an injection and therefore, the size of the set $A_{n,k}$ is equal to the size of the image of ψ, $\psi(A_{n,k}) = \{\psi(\sigma) : \sigma \in A_{n,k}\}$. We will show an upper bound on the size of $\psi(A_{n,k})$.

Let $\mathbf{x} = \psi(\sigma)$ for some $\sigma \in A_{n,k}$. For any position j, $2 \leq j \leq n-1$, either $|\sigma(j) - \sigma(j-1)| \leq k$ or $|\sigma(j+1) - \sigma(j)| \leq k$. Therefore, at least $\left\lfloor \frac{n-1}{2} \right\rfloor$ of the $n-1$ elements $x_2, x_3, \ldots, x_n$ are in the range $[-k, k] \setminus \{0\}$. Let $I \subseteq [2, n]$ be a set with at least $\left\lfloor \frac{n-1}{2} \right\rfloor$ elements and let D_I be the set of all vectors $\mathbf{x} \in \psi(A_{n,k})$ for which $x_i \in [-k, k] \setminus \{0\}$, for every $i \in I$ and $x_j \in [-n, n] \setminus [-k, k]$, for every $j \in [2, n] \setminus I$. Then,

$$|\psi(A_{n,k})| \leq \sum_{I \subseteq [2,n],\ |I| \geq \left\lfloor \frac{n-1}{2} \right\rfloor} |D_I|. \tag{7.1}$$

For each $i \in I$ there are $2k$ choices for x_i and for each $j \in [2, n] \setminus I$ there are at most $2(n-k) < 2n$ choices for x_j. Finally, there are n choices for x_1. Therefore,

$$|D_I| \leq n \cdot (2k)^{\left\lfloor \frac{n-1}{2} \right\rfloor} \cdot (2n)^{\left\lceil \frac{n-1}{2} \right\rceil} = 2^{n-1} k^{\left\lfloor \frac{n-1}{2} \right\rfloor} n^{\left\lceil \frac{n-1}{2} \right\rceil + 1}.$$

Since the number of choices for I is less than 2^{n-1}, according to (7.1), the following upper bound on the cardinality of $A_{n,k}$ and $\psi(A_{n,k})$ is derived

$$\begin{aligned} &|A_{n,k}| = |\psi(A_{n,k})| \leq 2^{n-1} \cdot 2^{n-1} k^{\left\lfloor \frac{n-1}{2} \right\rfloor} n^{\left\lceil \frac{n-1}{2} \right\rceil + 1} \\ &\leq 4^{n-1} k^{\frac{n}{2}} n^{\frac{n}{2}+1}. \end{aligned}$$

□

As a result of the last lemma we derive the following which provides an upper bound on the capacity.

Theorem 7.7 *For all* $0 \leq \epsilon \leq 1$, $C(\epsilon) \leq \frac{1+\epsilon}{2}$.

Proof. By Lemma 7.6, $|A_{n,k}| \leq 4^{n-1} k^{\frac{n}{2}} n^{\frac{n}{2}+1}$ and thus, if $k = \lceil n^\epsilon \rceil$ then

$$\begin{aligned} C(\epsilon) &\leq \lim_{n \to \infty} \frac{\log(4^{n-1} k^{\frac{n}{2}} n^{\frac{n}{2}+1})}{\log n!} \\ &= \lim_{n \to \infty} \frac{\log(4^{n-1} k^{\frac{n}{2}} n^{\frac{n}{2}+1})}{n \log n} \\ &= \lim_{n \to \infty} \frac{2n - 2 + \frac{n}{2} \log k + \frac{n}{2} \log n + \log n}{n \log n} \\ &= \lim_{n \to \infty} \frac{\frac{n}{2} \epsilon \log n + \frac{n}{2} \log n}{n \log n} = \frac{1+\epsilon}{2}. \end{aligned}$$

□

The following Corollary, which is an immediate result of Theorems 7.5 and 7.7, summarizes the discussion of this section.

Corollary 7.8 *For all* $0 \leq \epsilon \leq 1$, $C(\epsilon) = \frac{1+\epsilon}{2}$.

7.2 The Asymmetric Two-Neighbor Constraint

In this section we find the capacity of the asymmetric two-neighbor constraint. Our main result states that for all $0 \leq \epsilon \leq 1$, $\widetilde{C}(\epsilon) = 1$. Since the capacity is at most 1, and the capacity is nondecreasing when ϵ increases, we will need to show that $\widetilde{C}(0) = 1$. This will be done by a construction of an asymmetric two-neighbor 1-constrained code that confirms this capacity result.

For a set I, let $I^{\nearrow}$, respectively $I^{\searrow}$, denote the ordering of all elements in I according to their increasing, respectively decreasing, order. For the construction of an asymmetric two-neighbor 1-constrained code we will need the code $\mathcal{C}^{sym}_{r',1}$, where r' is even, from Construction 7.3. Recall that a permutation $\pi \in \mathcal{C}^{sym}_{r',1}$ is of the form

$$\pi = \rho(\gamma_1, \gamma_2, \ldots, \gamma_{\frac{r'}{2}}),$$

where $\rho(2i-1) = \rho(2i)$ and $\gamma_i \in S([2i-1, 2i])$, for all $1 \leq i \leq \frac{r'}{2}$. In other words, for every j, $1 \leq j \leq \frac{r'}{2}$, there exists $1 \leq i \leq \frac{r'}{2}$ such that $\{\pi(2j-1), \pi(2j)\} = \{2i-1, 2i\}$.

Construction 7.9 *Let m be an integer,* $1 \leq m < \frac{n}{4}$.

For $r = 2m+1$, let the code $\mathcal{C}_r \subset S_n$ defined as follows. A permutation $\sigma \in S_n$ belongs to $\mathcal{C}_r$ if there exists a partition of the set $[r, n]$ into r nonempty sets $I_1, I_2, \ldots, I_r$, and a permutation $\pi \in \mathcal{C}^{sym}_{r-1,1}$ such that

$$\sigma = [I_1^{\nearrow}, I_2^{\searrow}, \pi(1), \pi(2), I_3^{\nearrow}, I_4^{\searrow}, \ldots, \pi(r-2), \pi(r-1), I_r^{\nearrow}].$$

For $r = 2m+2$, the code $\mathcal{C}_r \subset S_n$ is defined in a similar way. A permutation $\sigma \in S_n$ belongs to $\mathcal{C}_r$ if there exists a partition of the set $[r-1, n]$ into r nonempty sets $I_1, I_2, \ldots, I_r$, and a permutation $\pi \in \mathcal{C}^{sym}_{r-2,1}$ such that

$$\sigma = [I_1^{\nearrow}, I_2^{\searrow}, \pi(1), \pi(2), I_3^{\nearrow}, I_4^{\searrow}, \ldots, \pi(r-3), \pi(r-2), I_{r-1}^{\nearrow}, I_r^{\searrow}].$$

Finally, let $\mathcal{C}^{asym}_n \subset S_n$ be the code

$$\mathcal{C}^{asym}_n = \bigcup_{m=1}^{\lfloor n/4-1 \rfloor} \mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}.$$

Example 7.10 *For $n = 15$ and $r = 5$, let $I_1 = \{5, 8, 10\}$, $I_2 = \{6, 12\}$, $I_3 = \{7, 15\}$, $I_4 = \{9, 13\}$, $I_5 = \{11, 14\}$ be a partition of $[5, 14]$ into 5 nonempty sets and let $\pi = [4, 3, 1, 2]$. Note, that $\pi = \rho(\gamma_1, \gamma_2)$ where $\rho = [2, 2, 1, 1]$, $\gamma_1 = [1, 2] \in S([1, 2])$, and $\gamma_2 = [4, 3] \in S([3, 4])$, hence, π is a codeword in $\mathcal{C}^{sym}_{4,1}$. Let $\sigma \in S_{14}$ be a permutation of the form*

$$\sigma = [I_1^{\nearrow}, I_2^{\searrow}, \pi(1), \pi(2), I_3^{\nearrow}, I_4^{\searrow}, \pi(3), \pi(4), I_5^{\nearrow}]$$

$$= [5, 8, 10, 12, 6, 4, 3, 7, 15, 13, 9, 1, 2, 11, 14].$$

. Then $\sigma \in \mathcal{C}_5$. Note, that σ can also be obtained from other partitions such as $\tilde{I}_1 = \{5, 8, 10, 12\}$, $\tilde{I}_2 = \{6\}$, and $\tilde{I}_i = I_i$, for all $3 \le i \le 5$.

A position i, $2 \le i \le n - 1$, is called a *valley* in a permutation $\sigma \in S_n$ if $\sigma(i - 1) > \sigma(i)$ and $\sigma(i) < \sigma(i + 1)$. For example, in the permutation $\sigma = [4, 7, 5, 6, 1, 2, 3]$, the third and fifth positions are valleys. The next lemma will be used in proving the correctness of the construction, which will be proved next.

Lemma 7.11 *Let m be an integer, $0 \le m \le \frac{n-2}{4}$. Then, every permutation $\sigma \in \mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$ has exactly m valleys.*

Proof. Let $\sigma \in \mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$. Then σ is formed as described in Construction 7.9 by a permutation $\pi \in \mathcal{C}_{2m,1}$ and a partition of the set $[2m+1, n]$, $I_1, I_2, \ldots, I_r$, where $r \in \{2m+1, 2m+2\}$. If $\sigma(i) \in I_s$ for some $2 \le i \le n-1$ and $1 \le s \le r$, then either $\sigma(i - 1) < \sigma(i)$ or $\sigma(i + 1) < \sigma(i)$, and hence i cannot be a valley in σ. Therefore, if i is a valley then $\sigma(i) = \pi(j)$ for some $1 \le j \le 2m$. Since for every j', $1 \le j' \le \frac{n}{2}$, there exists an i', $1 \le i' \le \frac{n}{2}$, such that $\{\pi(2j' - 1), \pi(2j')\} = \{2i - 1, 2i\}$ and since $\pi(2j' - 1)$ and $\pi(2j')$ are adjacent elements in σ, it follows that i is a valley in σ if and only if $\pi(j)$ is odd. Hence, every element in $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$ has exactly m valleys. □

The correctness of the construction of the code $\mathcal{C}_A$ is proved in the next lemma.

Lemma 7.12 *For all $n \ge 1$, the code $\mathcal{C}^{asym}_n$ is an asymmetric two-neighbor 1-constrained code.*

Proof. Let $\sigma \in \mathcal{C}^{asym}_n$ and let m be the number of valleys in σ. By Lemma 7.11 it follows that $\sigma \in \mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$. According to Construction 7.9 it follows that there exists a permutation $\pi \in \mathcal{C}^{sym}_{2m,1}$ such that the valleys of σ are the positions i where $\sigma(i) = \pi(j)$, for some $1 \le j \le 2m$, and $\pi(j)$ is odd.

It follows that either $\sigma(i-1) = \sigma(i)+1$ or $\sigma(i+1) = \sigma(i)+1$. Then the valleys in σ do not violate the asymmetric two-neighbor 1-constraint and therefore σ satisfies the asymmetric two-neighbor 1-constraint.

□

Next, we will analyze a lower bound on the cardinalities of the codes from Construction 7.9. First, we use the following observation.

Lemma 7.13 *For all $n \geq 1$, let $\sigma \in \mathcal{C}_n^{asym}$ and let m be the number of valleys in σ. Then there exist at most 2^{m+1} different ways to obtain σ as described in Construction 7.9.*

Proof. By Lemma 7.11 it follows that σ belongs to $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$. Let $i_1 < i_2 < \cdots < i_{2m}$ be the $2m$ positions in which the elements of the set $[2m]$ appear in σ. If $\pi \in C_{2m,1}$ is a permutation from which σ is obtained as described in Construction 7.9 then $\pi = [\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_{2m})]$, and hence π is uniquely determined by σ. If $I_1, I_2, \ldots, I_{2m+1}, I_{2m+2}$ is a partition of the set $[2m+1, n]$ into either $2m+1$ or $2m+2$ nonempty sets (we allow only the set I_{2m+2} to be empty), then $[I_1^{\nearrow}, I_2^{\searrow}] = [\sigma(1), \sigma(2), \ldots, \sigma(i_1 - 1)]$. Let j, $1 \leq j \leq i_1 - 1$ be the position such that $\sigma(j) \geq \sigma(i)$ for all $1 \leq i \leq i_1 - 1$. If $\sigma(j) \in I_1$ then $I_1 = \{\sigma(1), \sigma(2), \ldots, \sigma(j)\}$ and $I_2 = \{\sigma(j+1), \sigma(j+2), \ldots, \sigma(i_1 - 1)]$, and if $\sigma(j) \in I_2$ then $I_1 = \{\sigma(1), \sigma(2), \ldots, \sigma(j-1)\}$ and $I_2 = \{\sigma(j), \sigma(j+1), \ldots, \sigma(i_1 - 1)]$. Hence, there are at most two ways to determine the sets I_1 and I_2 from σ. Similarly, there are at most two ways to determine each of the pair of sets I_{2i+1}, I_{2i+2}, where $1 \leq i \leq m-1$, and at most two ways to determine the sets I_{2m+1}, I_{2m+2}, where I_{2m+2} may be an empty set.

Thus, there exist at most 2^{m+1} different ways to obtain σ as described in Construction 7.9.

□

For two positive integers ℓ, r, where $r \leq \ell$, the number of partitions of ℓ elements into r nonempty sets is denoted by $S(\ell, r)$ and is known as the Stirling number of the second kind.

Lemma 7.14 *For all $n \geq 1$, the cardinality of the code $\mathcal{C}_n^{asym}$ satisfies*

$$|\mathcal{C}_n^{asym}| \geq \sum_{r=1}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{2} r! S\Big(n - 2\Big\lfloor \frac{r-1}{2} \Big\rfloor, r\Big) \Big\lfloor \frac{r-1}{2} \Big\rfloor !.$$

Proof. For every m, $0 \leq m \leq \frac{n-2}{4}$, we compute a lower bound on the size of $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$. There are $r! S(n-2m, r)$ choices for the partition

$I_1, I_2, \ldots, I_r$, where $r = 2m+1$ or $r = 2m+2$, and there are $m! \cdot 2^m$ choices for the permutation $\pi \in \mathcal{C}_{2m,1}$. The expression

$$[(2m+1)!S(n-2m, 2m+1) + (2m+2)!S(n-2m, 2m+2)]m!2^m$$

counts codewords in $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$ and by Lemma 7.13, each codeword in $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$ is counted at most 2^{m+1} times. Hence, the size of $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$ is at least

$$[(2m+1)!S(n-2m, 2m+1) + (2m+2)!S(n-2m, 2m+2)]\frac{m!}{2}.$$

By Lemma 7.11 it follows that the sets $\mathcal{C}_{2m+1} \cup \mathcal{C}_{2m+2}$ and $\mathcal{C}_{2m'+1} \cup \mathcal{C}_{2m'+2}$ are disjoint if $m' \neq m$, and therefore

$$|\mathcal{C}_n^{asym}| \geq \sum_{r=1}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{2} r! S\Big(n - 2\Big\lfloor \frac{r-1}{2} \Big\rfloor, r\Big) \Big\lfloor \frac{r-1}{2} \Big\rfloor !.$$

□

In order to show that $\widetilde{C}(0) = 1$, we will need to use the following lower bound on the Stirling numbers of the second kind, which is taken from [69].

Lemma 7.15 *For* $1 \leq r \leq \ell$,

$$S(\ell, r) \geq \frac{1}{2}(r^2 + r + 2) r^{\ell - r - 1} - 1.$$

Finally, the next theorem, which is a direct result of Lemma 7.14 and a lower bound on the Stirling numbers of the second kind, highlights the result of this section.

Theorem 7.16 *For all* $0 \leq \epsilon \leq 1$, $\widetilde{C}(\epsilon) = 1$.

Proof. Clearly $\widetilde{C}(0) \leq 1$. We will show that

$$\lim_{n \to \infty} \frac{\log |B_{n,1}|}{\log n!} \geq 1,$$

by proving that for every $0 < \delta < \frac{1}{2}$,

$$\widetilde{C}(0) = \lim_{n \to \infty} \frac{\log |B_{n,1}|}{\log n!} > 1 - \delta.$$

Let δ be such that $0 < \delta < \frac{1}{2}$ and let $r = \lceil \delta n \rceil$. From Lemma 7.14 it follows that

$$|B_{n,1}| > \frac{1}{2} r! S(n-r, r) \left\lfloor \frac{r-1}{2} \right\rfloor !,$$

and by Lemma 7.15 and by the Stirling approximation, $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$,

$$|B_{n,1}| > \frac{1}{4} r! r^{n-2r+1} \left\lfloor \frac{r-1}{2} \right\rfloor ! \geq \frac{1}{4} \lceil \delta n \rceil ! (\delta n)^{n(1-2\delta)+1} \left\lfloor \frac{\delta n - 1}{2} \right\rfloor !$$
$$\geq \frac{1}{4} \left(\frac{\delta n}{e}\right)^{\delta n} (\delta n)^{n(1-2\delta)+1} \left(\frac{\delta n}{2e}\right)^{\frac{\delta n}{2}} \geq (\delta n)^{n - \frac{1}{2}\delta n} (2e)^{-\frac{3\delta n}{2}}.$$

It follows that

$$\lim_{n\to\infty} \frac{\log |B_{n,1}|}{\log n!} \geq \lim_{n\to\infty} \frac{\log (\delta n)^{n(1-\frac{1}{2}\delta)} (2e)^{-\frac{3\delta n}{2}}}{\log n^n} = 1 - \frac{\delta}{2} > 1 - \delta.$$

This shows that $\widetilde{C}(0) \geq 1$ and consequently $\widetilde{C}(\epsilon) = 1$, for all $0 \leq \epsilon \leq 1$.

□

7.3 The Capacity of Error-Correcting Constrained Codes

The two-neighbor constraint and the asymmetric two-neighbor constraint were proposed to combat errors that are caused by the inter-cell interference in flash memory cells. However, constrained codes should also be restricted to have error-correction capabilities, which is the topic of this section. A similar problem for the one-neighbor constraint was studied in [72].

For two permutations $\sigma, \pi \in S_n$, the *inversion distance*, denoted by $d_I(\sigma, \pi)$, between σ and π is the Kendall's τ-distance between their inverses, i.e.

$$d_I(\sigma, \pi) = d_K(\sigma^{-1}, \pi^{-1}).$$

Recall that $d_K(\sigma^{-1}, \pi^{-1})$ can be expressed as

$$d_I(\sigma, \pi) = d_K(\sigma^{-1}, \pi^{-1}) = |\{(i,j) : \sigma(i) < \sigma(j),\ \pi(i) > \pi(j)\}|.$$

Even though this distance was studied before, see e.g. [21], we are not aware of any formal name for this metric and thus call it here the inversion distance. In this section we study the capacity of the constraints in this paper combined with a requirement of a minimum inversion distance.

Remark 7.1 *We study the inversion distance and not the Kendall's τ one since, according to our representation of the cells ranking in a permutation, this metric fits better with the error behavior in flash memory cells. The motivation in studying codes in the Kendall's τ-metric originated from the observation that cells with adjacent levels may interchange their rankings [44]. Therefore, codes in the Kendall's τ-metric should be invoked over the inverses of the permutations. However, in order to study these codes with constrained codes, one should take the inversion distance applied for the permutations.*

Let $E(n,k,d)$ be the maximum size of a code in $A_{n,k}$ with minimum inversion distance d. For $0 \le \epsilon_1 \le 1$ and $0 \le \epsilon_2 \le 2$, let $k = \lceil n^{\epsilon_1} \rceil$ and $d = \lceil n^{\epsilon_2} \rceil$, and define the capacity of two-neighbor k-constrained codes with minimum inversion distance d by

$$C(\epsilon_1, \epsilon_2) = \lim_{n\to\infty} \frac{\log E(n,k,d)}{\log n!}.$$

We will compute this capacity in terms of ϵ_1 and ϵ_2 by following some of the methods used in [5] and later in [73]. We distinguish between three cases:

1. $0 \le \epsilon_2 \le 1$ and $0 \le \epsilon_1 \le 1$,
2. $1 < \epsilon_2 \le 1 + \epsilon_1$, and $0 \le \epsilon_1 \le 1$,
3. $1 + \epsilon_1 < \epsilon_2 \le 2$ and $0 \le \epsilon_1 \le 1$.

We will find upper and lower bounds on the size of $E(n,k,d)$ in each case and use these bounds in order to compute the capacity of these codes.

For a permutation $\sigma \in S_n$, the *sphere* of radius t centered at σ is the set

$$\mathbb{S}_I(n,t,\sigma) = \{\pi \in S_n \ : \ d_I(\sigma,\pi) \le t\}.$$

The size of the sphere $\mathbb{S}_I(n,\sigma,r)$ does not depend on σ and thus we denote it by $s_I(n,r)$. For $\sigma \in A_{n,k}$, the *sphere* in $A_{n,k}$ of radius r centered at σ is defined by

$$\mathbb{S}_I(A_{n,k},\sigma,r) \overset{\text{def}}{=} \{\pi \in A_{n,k} \ : \ d_I(\sigma,\pi) \le r\}.$$

A code in $A_{n,k}$ with minimum inversion distance d can be constructed by a greedy approach which leads to the following Gilbert-Varshamov type of lower bound.

Lemma 7.17 *For every $1 \leq k < n$, $1 \leq d \leq \binom{n}{2}$, the following lower bound on $E(n,k,d)$ holds*

$$E(n,k,d) \geq \frac{|A_{n,k}|}{s_I(n,d-1)}.$$

The next theorem is a combination of results from [5], [56], and [59].

Theorem 7.18 *Let $r = \Theta(n^{\delta})$, where $0 \leq \delta \leq 2$. Then there exist constants c_1 and c_2 such that*

$$s_I(n,r) \leq \begin{cases} e^{c_1 n} & \text{if } 0 \leq \delta \leq 1 \\ (c_2 n^{\delta-1})^n & \text{if } 1 < \delta \leq 2 \end{cases}.$$

We are now in a position to compute the capacity $C(\epsilon_1,\epsilon_2)$ for the first case.

Theorem 7.19 *For $0 \leq \epsilon_1, \epsilon_2 \leq 1$, $C(\epsilon_1,\epsilon_2) = \frac{1}{2} + \frac{\epsilon_1}{2}$.*

Proof. Since $E(n,k,d) \subseteq A_{n,k}$ it follows that

$$\frac{\log E(n,k,d)}{\log n!} \leq \frac{\log |A_{n,k}|}{\log n!},$$

and hence from Corollary 7.8, $C(\epsilon_1,\epsilon_2) \leq C(\epsilon_1) = \frac{1}{2} + \frac{\epsilon_1}{2}$.

By Lemma 7.17 and Theorem 7.18 there exists a constant c such that

$$\frac{\log E(n,k,d)}{\log n!} \geq \frac{\log |A_{n,k}|}{\log n!} - \frac{\log e^{cn}}{\log n!}.$$

Then, $C(\epsilon_1,\epsilon_2) \geq C(\epsilon_1) = \frac{1}{2} + \frac{\epsilon_1}{2}$, and thus, $C(\epsilon_1,\epsilon_2) = \frac{1}{2} + \frac{\epsilon_1}{2}$.

□

Before proceeding to the second case, let us introduce some more tools that we will use in solving this case. Let $H_n = \{1,2,\ldots,n\}^n$. Recall that for $\mathbf{x},\mathbf{y} \in H_n$, the Manhattan distance between $\mathbf{x}$ and $\mathbf{y}$, $d_M(\mathbf{x},\mathbf{y})$, is defined as

$$d_M(\mathbf{x},\mathbf{y}) \overset{\text{def}}{=} \sum_{i=1}^{n} |x_i - y_i|.$$

The next lemma was proved in [21].

Lemma 7.20 *For every $\sigma, \pi \in S_n$,*

$$\frac{1}{2} d_M(\sigma,\pi) \leq d_I(\sigma,\pi) \leq d_M(\sigma,\pi).$$

The definition of the two-neighbor k-constraint can be trivially extended to H_n. A vector $\mathbf{x} \in H_n$ satisfies the two-neighbor k-constraint if either $|x_i - x_{i-1}| \leq k$ or $|x_{i+1} - x_i| \leq k$, for all $2 \leq i \leq n-1$. Let $\mathcal{A}_{n,k}$ be the set of all elements of H_n that satisfy the two-neighbor k-constraint.

For a subset $S \subseteq H_n$ and $\mathbf{x} \in S$, the Manhattan *sphere* in S of radius r centered at $\mathbf{x}$ is defined by

$$\mathbb{S}_M(S, \mathbf{x}, r) \overset{\text{def}}{=} \{\mathbf{y} \in S \ : \ d_M(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Combining the previous results along with the sphere packing upper bound and Gilbert-Varshamov lower bound provides us with the following lemma.

Lemma 7.21 *For every* $1 \leq k < n$, $1 \leq d \leq \binom{n}{2}$,

$$E(n,k,d) \leq \frac{|\mathcal{A}_{n,k}|}{\min_{\mathbf{x} \in \mathcal{A}_{n,k}} \{\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, \lfloor \frac{d-1}{2} \rfloor)|\}}.$$

and

$$E(n,k,d) \geq \frac{|A_{n,k}|}{\max_{\mathbf{x} \in \mathcal{A}_{n,k}} \{|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, 2d-1)|\}}.$$

Proof. From Lemma 7.20 it follows that every code in $A_{n,k}$ with minimum inversion distance d is also a code in $\mathcal{A}_{n,k}$ with minimum Manhattan distance d. Hence, by the sphere packing bound for codes in $\mathcal{A}_{n,k}$ the following upper bound holds

$$E(n,k,d) \leq \frac{|\mathcal{A}_{n,k}|}{\min_{\mathbf{x} \in \mathcal{A}_{n,k}} \{|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, \lfloor \frac{d-1}{2} \rfloor)|\}}.$$

From Lemma 7.20 it follows that every code in $A_{n,k}$ with minimum Manhattan distance $2d$ is also a code in $A_{n,k}$ with minimum inversion distance d. Hence,

$$E(n,k,d) \geq \frac{|A_{n,k}|}{\max_{\mathbf{x} \in A_{n,k}} \{|\mathbb{S}_M(A_{n,k}, \mathbf{x}, 2d-1)|\}}.$$

and since

$$\max_{\mathbf{x} \in A_{n,k}} \{|\mathbb{S}_M(A_{n,k}, \mathbf{x}, 2d-1)|\} \leq \max_{\mathbf{x} \in \mathcal{A}_{n,k}} \{|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, 2d-1)|\},$$

we get

$$E(n,k,d) \geq \frac{|A_{n,k}|}{\max_{\mathbf{x} \in \mathcal{A}_{n,k}} \{|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, 2d-1)|\}}.$$

□

In order to apply the upper bound from Lemma 7.21, we state in the next lemma a lower bound on the size of a Manhattan ball in $\mathcal{A}_{n,k}$.

Lemma 7.22 *Let $k = \lceil n^{\epsilon} \rceil$ and $r = \lceil n^{\delta} \rceil$, where $0 \leq \epsilon \leq 1$ and $0 \leq \delta \leq 2$. Then there exists a constant c such that*

$$\min_{\mathbf{x} \in \mathcal{A}_{n,k}} \{ \mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, r) | \} \geq \begin{cases} \left(\frac{n^{\delta-1}}{2} \right)^n & \textit{if } 1 < \delta < 1+\epsilon < 2 \\ \left(\frac{n^{\delta-1+\epsilon}}{c} \right)^{\frac{n}{2}} & \textit{if } 1+\epsilon \leq \delta < 2 \end{cases}.$$

Proof. Let $\mathbf{x} \in \mathcal{A}_{n,k}$. We will show a construction of a subset of $\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, r)$ that verifies the lower bound stated in the lemma. Let $m = \lceil n/2 \rceil$ and let

$$D_1 = \left\{ (y_1, y_2, \ldots, y_m) \ : \ \sum_{i=1}^{m} y_i = \frac{r}{4}, 0 \leq y_i \leq m-k \right\},$$

$$D_2 = \left\{ (z_1, z_2, \ldots, z_{n-m}) \ : \ \sum_{i=1}^{n-m} z_i = \frac{r}{4}, 0 \leq z_i \leq k \right\}.$$

For every $\mathbf{y} \in D_1$, let $\mathbf{w} \in H_n$ be the following vector. For every $1 \leq i \leq m$

$$w_{2i-1} = \begin{cases} x_{2i-1} + y_i & \text{if } x_{2i-1} \leq m \\ x_{2i-1} - y_i & \text{if } x_{2i-1} > m \end{cases}.$$

Since $\mathbf{x} \in \mathcal{A}_{n,k}$, for every $1 \leq i < n-m$, $|x_{2i} - x_{2i-1}| \leq k$ or $|x_{2i+1} - x_{2i}| \leq k$, and accordingly the even entries in $\mathbf{w}$ are defined to be

$$w_{2i} = \begin{cases} x_{2i} + w_{2i-1} - x_{2i-1} & \text{if } |x_{2i} - x_{2i-1}| \leq k \\ x_{2i} + w_{2i+1} - x_{2i+1} & \text{if } |x_{2i} - x_{2i-1}| > k \end{cases}.$$

According to the construction of the vector $\mathbf{w}$ we get that $\mathbf{w} \in \mathcal{A}_{n,k}$ and $d_M(\mathbf{x}, \mathbf{w}) \leq \frac{3r}{4}$, that is, $\mathbf{w} \in \mathcal{B}_M(\mathcal{A}_{n,k}, \mathbf{x}, \frac{3r}{4})$.

Similarly, for every $\mathbf{z} \in D_2$, we define $\mathbf{u} \in H_n$ as follows. For every $1 \leq i \leq n-m$, if $|w_{2i} - w_{2i-1}| \leq k$ then

$$u_{2i} = \begin{cases} w_{2i} - z_i & \text{if } 0 \leq w_{2i} - w_{2i-1} \leq k, w_{2i} > k \\ z_i & \text{if } 0 \leq w_{2i} - w_{2i-1} \leq k, w_{2i} < k \\ w_{2i} + z_i & \text{if } -k \leq w_{2i} - w_{2i-1} \leq 0, w_{2i} \leq n-k \\ n - z_i & \text{if } -k \leq w_{2i} - w_{2i-1} \leq 0, w_{2i} > n-k \end{cases}$$

and if $|w_{2i} - w_{2i-1}| > k$ then

$$u_{2i} = \begin{cases} w_{2i} - z_i & \text{if } 0 \leq w_{2i} - w_{2i+1} \leq k, w_{2i} > k \\ z_i & \text{if } 0 \leq w_{2i} - w_{2i+1} \leq k, w_{2i} < k \\ w_{2i} + z_i & \text{if } -k \leq w_{2i} - w_{2i+1} \leq 0, w_{2i} \leq n-k \\ n - z_i & \text{if } -k \leq w_{2i} - w_{2i+1} \leq 0, w_{2i} > n-k \end{cases}.$$

Lastly, for every $1 \leq i \leq m$, we set $u_{2i-1} = w_{2i-1}$. It can be readily verified that $\mathbf{u}$ belongs to $\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, r)$ and that $\mathbf{y}, \mathbf{z}$ are reconstructible from $\mathbf{x}$ and $\mathbf{u}$. Therefore,

$$|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, r)| \geq |D_1| \cdot |D_2|.$$

For every three positive integers $\tilde{n}, \tilde{k}, \tilde{r}$ we define

$$Q_{\tilde{n},\tilde{k},\tilde{r}} \overset{\text{def}}{=} \left| \left\{ (y_1, y_2, \ldots, y_{\tilde{n}}) \in \mathbb{Z}^{\tilde{n}} : \sum_{i=1}^{\tilde{n}} y_i = \tilde{r}, 0 \leq y_i \leq \tilde{k} \right\} \right|.$$

According to the last definition, we get that $|D_1| = Q_{m,m-k,\frac{r}{4}}$ and $|D_2| = Q_{n-m,k,\frac{r}{4}}$. In [73] the authors proved that if $\tilde{k} = \Theta(\tilde{n}^{\tilde{\epsilon}})$ and $\tilde{r} = \Theta(\tilde{n}^{\tilde{\delta}})$, where $1 + \tilde{\epsilon} > \tilde{\delta}$, then

$$Q_{\tilde{n},\tilde{k},\tilde{r}} \geq \frac{(\tilde{n} + \tilde{r})^{\tilde{n}}}{\tilde{n}^{\tilde{n}}}.$$

Since $\epsilon < 1$ it follows that $m - k = \Theta(n)$, and since $\delta < 2$ we get

$$|D_1| \geq \frac{\left(\frac{n}{2} + \frac{r}{4}\right)^{\frac{n}{2}}}{\left(\frac{n}{2}\right)^{\frac{n}{2}}} \geq \left(\frac{n^{\delta-1}}{2}\right)^{\frac{n}{2}}.$$

If $1 \leq \delta < 1 + \epsilon < 2$ we have that

$$|D_2| \geq \frac{\left(\frac{n}{2} + \frac{r}{4}\right)^{\frac{n}{2}}}{\left(\frac{n}{2}\right)^{\frac{n}{2}}} \geq \left(\frac{n^{\delta-1}}{2}\right)^{\frac{n}{2}}.$$

Therefore,

$$|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, t)| = \left(\frac{n^{\delta-1}}{2}\right)^{n}.$$

If $1 + \epsilon \leq \delta < 2$ then since $\frac{n}{2}k = \Theta(n^{1+\epsilon}) = O(r)$, there exist a constant c such that $\frac{n}{2}\left\lceil\frac{k}{c}\right\rceil \leq r$ where n is sufficiently large, and therefore

$$|D_2| \geq \left(\frac{k}{c}\right)^{\frac{n}{2}} = \left(\frac{n^{\epsilon}}{c}\right)^{fracn2}.$$

Therefore,

$$|\mathbb{S}_M(\mathcal{A}_{n,k},\mathbf{x},t)| \geq \left(\frac{n^{\delta-1+\epsilon}}{2c}\right)^{\frac{n}{2}}.$$

□

We are ready to prove the capacity for the second case.

Theorem 7.23 *For* $0 \leq \epsilon_1 \leq 1$ *and* $1 < \epsilon_2 \leq 1+\epsilon_1$*,*

$$C(\epsilon_1,\epsilon_2) = \frac{3}{2} + \frac{\epsilon_1}{2} - \epsilon_2.$$

Proof. Let $k = \lceil n^{\epsilon_1} \rceil$ and $d = \lceil n^{\epsilon_2} \rceil$. By Lemma 7.17 and Theorem 7.18 it follows that there exists a constant c such that

$$\frac{\log E(n,k,d)}{\log n!} \geq \frac{\log |A_{n,k}|}{\log n!} - \frac{\log c^n n^{(\epsilon_2-1)n}}{\log n!}.$$

Therefore,

$$C(\epsilon_1,\epsilon_2) \geq \frac{1}{2} + \frac{\epsilon_1}{2} + 1 - \epsilon_2 = \frac{3}{2} + \frac{\epsilon_1}{2} - \epsilon_2.$$

Similarly, by Lemmas 7.21 and 7.22 it follows that

$$\frac{\log E(n,k,d)}{\log n!} \leq \frac{\log |\mathcal{A}_{n,k}|}{\log n!} - \frac{\log \left(\frac{n^{\epsilon_2-1}}{2}\right)^n}{\log n!},$$

and hence,

$$C(\epsilon_1,\epsilon_2) \leq \frac{1}{2} + \frac{\epsilon_1}{2} + 1 - \epsilon_2.$$

Together we get, $C(\epsilon_1,\epsilon_2) = \frac{3}{2} + \frac{\epsilon_1}{2} - \frac{\epsilon_2}{2}$.

□

For the last case, where $1+\epsilon_1 < \epsilon_2 \leq 2, 0 \leq \epsilon_1 \leq 1$ we will need one more lemma.

Lemma 7.24 *Let* $k = \lceil n^{\epsilon} \rceil$ *and* $r = \lceil n^{\delta} \rceil$*, where* $0 \leq \epsilon \leq 1$ *and* $1 \leq \delta \leq 2$*. Then, there exists a constant* c *such that*

$$\max_{\mathbf{x}\in\mathcal{A}_{n,k}} \{|\mathbb{S}_M(\mathcal{A}_{n,k},\mathbf{x},r)|\} \leq c^n n^{(\delta-1+\epsilon)\frac{n}{2}}.$$

Proof. Let $\mathbf{x} \in \mathcal{A}_{n,k}$, and $m = \left\lceil \frac{n}{2} \right\rceil$. For every $\mathbf{y} \in \mathbb{S}_M(\mathcal{A}_{n,k},\mathbf{x},r)$, define the vectors $(\mathbf{u},\mathbf{b}) \in \{0,1,\ldots,n-1\}^m \times \{0,1\}^m$ such that $\sum_{i=1}^m u_i \leq r$ and $(\mathbf{z},\mathbf{c}) \in \{0,1,2,\ldots,k\}^{n-m} \times \{0,1,2,3\}^{n-m}$ as follows. For $1 \leq i \leq m$,

$$(u_i,b_i) = \begin{cases} (y_{2i-1} - x_{2i-1}, 0) & \text{if } 0 \leq y_{2i-1} - x_{2i-1} \\ (x_{2i-1} - y_{2i-1}, 1) & \text{if } y_{2i-1} - x_{2i-1} < 0 \end{cases}.$$

For $1 \leq i \leq n-m$, if $|y_{2i} - y_{2i-1}| \leq k$ then

$$(z_i, c_i) = \begin{cases} (y_{2i} - y_{2i-1}, 0) & \text{if } 0 \leq y_{2i} - y_{2i-1} \leq k \\ (y_{2i-1} - y_{2i}, 1) & \text{if } -k \leq y_{2i} - y_{2i-1} \leq 0 \end{cases}.$$

Otherwise, if $|y_{2i} - y_{2i-1}| > k$ then

$$(z_i, c_i) = \begin{cases} (y_{2i} - y_{2i+1}, 2) & \text{if } 0 \leq y_{2i} - y_{2i+1} \leq k \\ (y_{2i+1} - y_{2i}, 3) & \text{if } -k \leq y_{2i} - y_{2i+1} \leq 0 \end{cases}.$$

Note that $\mathbf{y}$ is reconstructible from $(\mathbf{u}, \mathbf{b}), (\mathbf{z}, \mathbf{c})$ and $\mathbf{x}$, hence the mapping $y \rightarrow ((\mathbf{u}, \mathbf{b}), (\mathbf{z}, \mathbf{c}))$ is an injection. Hence, the size of $\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, r)$ is at most the number of different choices of $((\mathbf{u}, \mathbf{b}), (\mathbf{z}, \mathbf{c}))$ and therefore

$$|\mathbb{S}_M(\mathcal{A}_{n,k}, \mathbf{x}, r)| \leq 2^{\frac{n}{2}+1} \binom{\lceil \frac{n}{2} \rceil + r + 2}{r} (4(k+1))^{\frac{n}{2}}.$$

We will show that there exists a constant b such that

$$\binom{\lceil \frac{n}{2} \rceil + r + 2}{r} \leq b^n n^{(\delta-1)\frac{n}{2}}.$$

By the Stirling approximation, $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$, we have

$$\binom{\lceil \frac{n}{2} \rceil + r + 2}{r} \leq \frac{\left(\frac{n+5}{2} + r\right)^{\frac{n+5}{2}+r}}{r^r \left(\frac{n+4}{2}\right)^{\frac{n+4}{2}}} \leq .$$

$$\frac{2^{\frac{n+4}{2}} r^{\frac{n+5}{2}} \left(\frac{n+5}{2r} + 1\right)^{\frac{n+5}{2}+r}}{n^{\frac{n+4}{2}}} \leq$$

$$b_1^n n^{(\delta-1)\frac{n}{2}} \left(\left(\frac{1}{\frac{2r}{n+5}} + 1 \right)^{\frac{2r}{n+5}} \right)^{\frac{n+5}{2r} \frac{n+5}{2} + r} \leq$$

$$b_2^n n^{(\delta-1)\frac{n}{2}} e^{\frac{(n+5)^2}{4r} + \frac{n+5}{2}}.$$

for some constants $b_1,\ b_2$.

Since $\delta \geq 1$ it follows that $\frac{(n+5)^2}{4r} + \frac{n+5}{2} = \Theta(n)$ and therefore there exists a constant b such that

$$\binom{\lceil \frac{n}{2} \rceil + r + 2}{r} \leq b^n n^{(\delta-1)\frac{n}{2}}.$$

Finally, we have that there exists a constant c such that

$$|\mathbb{S}_M(\mathcal{A}_{n,k},\mathbf{x},r)| \leq c^n n^{(1-\delta)\frac{n}{2}} n^{\frac{\epsilon n}{2}}.$$

□

We are ready to compute the capacity for the last case.

Theorem 7.25 *If* $1+\epsilon_1<\epsilon_2\leq 2$ *and* $0\leq\epsilon_1\leq 1$*, then*

$$C(\epsilon_1,\epsilon_2)=1-\frac{\epsilon_2}{2}.$$

Proof. Let $k=\lceil n^{\epsilon_1}\rceil$ and $d=\lceil n^{\epsilon_2}\rceil$. For $1+\epsilon_1\leq\epsilon_2<2$, it follows from Lemmas 7.21 and 7.24 that

$$\frac{\log E(n,k,d)}{\log n!}\geq\frac{\log|A_{n,k}|}{\log n!}-\frac{\log(c^n n^{(\epsilon_2-1+\epsilon_1)\frac{n}{2}})}{\log n!}.$$

Thus,

$$C(\epsilon_1,\epsilon_2)\geq\frac{1}{2}+\frac{\epsilon_1}{2}+\frac{1}{2}-\frac{\epsilon_2}{2}-\frac{\epsilon_1}{2}=1-\frac{\epsilon_2}{2}.$$

It follows from Lemmas 7.21 and 7.22 that

$$\frac{\log E(n,k,d)}{\log n!}\leq\frac{\log|\mathcal{A}_{n,k}|}{\log n!}-\frac{\log n^{(\epsilon_2-1+\epsilon_1)\frac{n}{2}}}{\log n!},$$

and therefore

$$C(\epsilon_1,\epsilon_2)\leq\frac{1}{2}+\frac{\epsilon_1}{2}-\frac{\epsilon_2+\epsilon_1-1}{2}=1-\frac{\epsilon_2}{2}.$$

We conclude that if $1+\epsilon_1\leq\epsilon_2\leq 2$ then $C(\epsilon_1,\epsilon_2)=1-\frac{\epsilon_2}{2}$.

□

For conclusion, Theorems 7.19, 7.23, and 7.25 are summarized in the following corollary.

Corollary 7.26 *Let* $0\leq\epsilon_1\leq 1$ *and* $0\leq\epsilon_2\leq 2$*. Then*

$$C(\epsilon_1,\epsilon_2)=\begin{cases}\frac{1}{2}+\frac{\epsilon_1}{2} & \text{if } 0\leq\epsilon_2\leq 1\\ \frac{3}{2}+\frac{\epsilon_1}{2}-\epsilon_2 & \text{if } 1<\epsilon_2\leq 1+\epsilon_1\\ 1-\frac{\epsilon_2}{2} & \text{if } 1+\epsilon_1<\epsilon_2\leq 2\end{cases}.$$

Let $\tilde{E}(n,k,d)$ be the maximum size of a code in $B_{n,k}$ (the set of all permutations in S_n that satisfy the asymmetric two neighbor k-constraint) with minimum inversion distance d. For $0\leq\epsilon_1\leq 1$, $0\leq\epsilon_2\leq 2$, $k=\lceil n^{\epsilon_1}\rceil$

and $d = \lceil n^{\epsilon_2} \rceil$, the capacity and asymmetric two neighbor constrained code with minimum inversion distance d is defined by

$$\tilde{C}(\epsilon_1, \epsilon_2) = \lim_{n\to\infty} \frac{\log \tilde{E}(n,k,d)}{\log n!}.$$

Let $E(n,d)$ be the maximum size of a code in S_n with minimum inversion distance d. For $0 \leq \delta \leq 2$, and $d = \lceil n^{\delta} \rceil$, the capacity of error-correcting codes in S_n with minimum inversion distance d by

$$C_{err}(\delta) = \lim_{n\to\infty} \frac{\log E(n,d)}{\log n!}.$$

Barg and Mazumdar [5] prove the following

Theorem 7.27 *Let $0 \leq \delta \leq 2$. Then*

$$C_{err}(\delta) = \begin{cases} 1 & \textit{if } 0 \leq \delta \leq 1 \\ 2-\delta & \textit{if } 1\delta \leq 2 \end{cases}.$$

Following the same technique used in [5] we have

Theorem 7.28 *Let $0 \leq \epsilon_1 \leq 1$ and $0 \leq \epsilon_2 =\leq 2$. Then*

$$\tilde{C}(\epsilon_1, \epsilon_2) = C_{err}(\epsilon_2)$$

Proof. Since every code in $B_{n,k}$ with minimum inversion distance d is also a code in S_n with minimum inversion distance d it follows that $\tilde{E}(n,k,d) \leq E(n,d)$ and therefore, $\tilde{C}(\epsilon_1, \epsilon_2) \leq C_{err}(\epsilon_2)$.

We have the following lower bound on $\tilde{E}(n,k,d)$, which is a Gilbert-Varshamov type of lower bound.

$$\tilde{E}(n,k,d) \geq \frac{|B_{n,k}|}{s_I(n,d-1)}.$$

Hence,

$$\tilde{C}(\epsilon_1, \epsilon_2) = \lim_{n\to\infty} \frac{\log \tilde{E}(n,k,d)}{\log n!}$$

$$\geq \lim_{n\to\infty} \frac{\log |B_{n,k}|}{\log n!} - \lim_{n\to\infty} \frac{\log s_I(n,d-1)}{\log n!} = \tilde{C}(\epsilon_1) - \lim_{n\to\infty} \frac{\log s_I(n,d-1)}{\log n!}$$

By Theorem 7.18 we have that if $0 \leq \epsilon_2 \leq 1$ then there exist some constant c_1 such that $s_I(n, d-1) \leq e^{c_1 n}$ and therefore,

$$\tilde{C}(\epsilon_1, \epsilon_2) \geq \tilde{C}(\epsilon_1) = 1 = C_{err}(\epsilon_2).$$

By Theorem 7.18 it also follows that if $1 < \epsilon_2 \leq 2$ then there exist some constant c_2 such that $s_I(n, d-1) \leq (c_2 n^{\epsilon_2 - 1})n$ and therefore,

$$\tilde{C}(\epsilon_1, \epsilon_2) \geq \tilde{C}(\epsilon_1) - (\epsilon_2 - 1) = 2 - \epsilon_2 = C_{err}(\epsilon_2).$$

We conclude that $\tilde{C}(\epsilon, \epsilon_2) = C_{err}(\epsilon_2)$ for all $0 \leq \epsilon_1 \leq 1$ and $0 \leq \epsilon_2 \leq 2$.

□

Appendix A

In Theorem 5.2 we proved that a perfect single-error-correcting code in S_n with the Kendall's τ-metric does not exist if $n > 4$ is a prime or if $n = 4$. The proof of Theorem 5.2 is based on a certain linear equations system, where the existence of a perfect single-error-correcting code in S_n implies the existence of a solution to the linear equations system over the integers, and thus, by showing the nonexistence of such solution we derive the nonexistence of a perfect single-error-correcting code. By using similar techniques we prove the nonexistence of perfect single-error-correcting codes in S_n for $n \in \{6, 8, 9, 10\}$. For each such n, let $\mathcal{C}$ be a perfect single-error-correcting code in S_n. We will describe the corresponding linear equations system and use a computer to show that this linear equations system does not have a solution over the integers.

$n = 6$: We denote by D_6 the set of all vectors of $\{1, 2, 3\}^6$ in which each of the elements 1,2,3 appears twice. For each $\mathbf{v} \in D_6$ we define $S_{\mathbf{v}}$ to be the set of eight permutations in S_6, such that the elements 1 and 2 appear in the two positions in which 1 appears in $\mathbf{v}$, the elements 3 and 4 appear in the two positions in which 2 appears in $\mathbf{v}$, and the elements 5 and 6 appear in the two positions in which 3 appears in $\mathbf{v}$. Let $x_{\mathbf{v}} = |\mathcal{C} \cap S_{\mathbf{v}}|$ and let $\mathbf{x} = (x_{\mathbf{v}_1}, x_{\mathbf{v}_2}, \ldots, x_{\mathbf{v}_m})$, where $m = |D_6| = \frac{6!}{2!2!2!}$. By considering how the elements of $S_{\mathbf{v}}$ are covered (similarly to the way it was done in the proof of Theorem 5.2), for each $\mathbf{v} \in D_6$, we obtain a linear equations system of the form $A\mathbf{x}^T = |S_{\mathbf{v}}| \cdot \mathbf{1} = 8 \cdot \mathbf{1}$, where A is a square matrix of order m. The kernel of A is an one-dimensional vector space which is spanned by a vector $\mathbf{y} \in \{0, -1, 1\}^9$, that has both negative and positive entries. Every solution for this system is of the form $\frac{8}{6} \cdot \mathbf{1} + \alpha \cdot \mathbf{y}$, $\alpha \in \mathbb{R}$, and therefore, the system does not have a solution in which all entries are integers.

$n = 8$: We denote by D_8 the set of all vectors $\mathbf{v} \in \{1, 2, 3, 4\}^8$ in which each of the elements 1 and 2 appears three times and each of the elements 3 and 4 appears once. For every $\mathbf{v} \in D_8$ we define $S_{\mathbf{v}}$ to be the set of 36 permutations in S_8, such that the elements $1, 2$, and 3 appear in the three positions in which 1 appears in $\mathbf{v}$, the elements $4, 5$, and 6 appear in the three positions in which 2 appears in $\mathbf{v}$, the element 7 appears in the position of 3 in $\mathbf{v}$, and the element 8 appears in the position of 4 in $\mathbf{v}$. Let $x_{\mathbf{v}} = |\mathcal{C} \cap S_{\mathbf{v}}|$ and let $\mathbf{x} = (x_{\mathbf{v}_1}, x_{\mathbf{v}_2}, \ldots, x_{\mathbf{v}_m})$, where $m = |D_8| = \frac{8!}{3!3!}$. By considering how elements of $S_{\mathbf{v}}$ are covered, for each $\mathbf{v} \in D_8$, we obtain a linear equations system of the form $A\mathbf{x}^T = 36 \cdot \mathbf{1}$, where A is a square matrix of order m. The system has a unique solution, $\mathbf{x}^T = \frac{36}{8} \cdot \mathbf{1}$, which has non-integer entries.

$n = 9$: We denote by D_9 the set of all vectors $\mathbf{v} \in \{1, 2, 3\}^9$ in which the element 1 appears five times and each of the elements 2 and 3 appears twice. For every $\mathbf{v} \in D_9$ we define $S_{\mathbf{v}}$ to be the set of 480 permutations in S_8, such that the elements $1, 2, 3, 4$, and 5 appear in the five positions in which 1 appears in $\mathbf{v}$, the elements 6 and 7 appear in the two positions in which 2 appears in $\mathbf{v}$, and the elements 8 and 9 appear in the two positions in which 3 appears in $\mathbf{v}$. Let $x_{\mathbf{v}} = |\mathcal{C} \cap S_{\mathbf{v}}|$ and let $\mathbf{x} = (x_{\mathbf{v}_1}, x_{\mathbf{v}_2}, \ldots, x_{\mathbf{v}_m})$, where $m = |D_9| = \frac{9!}{5!2!2!}$. By considering how elements of $S_{\mathbf{v}}$ are covered, for each $\mathbf{v} \in D_9$, we obtain a linear equations system of the form $A\mathbf{x}^T = 480 \cdot \mathbf{1}$, where A is a square matrix of order m. The system has a unique solution, $\mathbf{x}^T = \frac{480}{9} \cdot \mathbf{1}$, which has non-integer entries.

$n = 10$: We denote by D_{10} the set of all vectors $\mathbf{v} \in \{1, 2, 3\}^{10}$ in which each of the elements 1 and 2 appears four times and the element 3 appears twice. For every $\mathbf{v} \in D_{10}$ we define $S_{\mathbf{v}}$ to be the set of 1,152 permutations in S_{10}, such that the elements $1, 2, 3$, and 4 appear in the four positions in which 1 appears in $\mathbf{v}$, the elements $5, 6, 7$, and 8 appear in the four positions in which 2 appears in $\mathbf{v}$, and the elements 9 and 10 appear in the two positions in which 3 appears in $\mathbf{v}$. Let $x_{\mathbf{v}} = |\mathcal{C} \cap S_{\mathbf{v}}|$ and let $\mathbf{x} = (x_{\mathbf{v}_1}, x_{\mathbf{v}_2}, \ldots, x_{\mathbf{v}_m})$, where $m = |D_{10}| = \frac{10!}{4!4!2!}$. By considering how elements of $S_{\mathbf{v}}$ are covered, for each $\mathbf{v} \in D_{10}$, we obtain a linear equations system of the form $A\mathbf{x}^T = 1,152 \cdot \mathbf{1}$, where A is a square matrix of order m. The system has a unique solution, $\mathbf{x}^T = \frac{1{,}152}{10} \cdot \mathbf{1}$, which has non-integer entries.

Appendix B

In Section 5.3 an algorithm that calculate the cyclic Kendall's-τ-weight of a permutation $\sigma \in S_n$, $w_\kappa(\sigma)$, was presented. The running time of the algorithm is $O(n^2)$ and it consists of the following five steps.

1) For every $i \in [0, n-1]$, compute

$$dist_\sigma(i) \overset{\text{def}}{=} \min\{i - \sigma^{-1}(i) \pmod n, \sigma^{-1}(i) - i \pmod n\}$$

and

$$sign_\sigma(i) \overset{\text{def}}{=} \begin{cases} 0 & \text{if } \sigma(i) = i \\ + & \text{if } \sigma(i) \neq i \text{ and } dist_\sigma(i) = i - \sigma^{-1}(i)(\bmod n) \\ - & \text{otherwise} \end{cases} .$$

2) Compute

$$r_\sigma \overset{\text{def}}{=} \frac{\sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i)}{n}.$$

3) Choose a set $M \subset [0, n-1]$ of $|r_\sigma|$ elements such that for every $i \in M$, $sign_\sigma(i) r_\sigma \geq 0$ and for every $j \in [0, n-1] \setminus M$, for which $sign_\sigma(j) sign(r_\sigma) \geq 0$, we have that $dist_\sigma(j) \leq dist_\sigma(i)$.

4) For every $i \in [0, n-1]$ compute

$$d_{M,\sigma}(i) \overset{\text{def}}{=} \begin{cases} n - dist_\sigma(i) & \text{if } i \in M \\ dist_\sigma(i) & \text{otherwise} \end{cases}$$

and

$$s_{M,\sigma}(i) \overset{\text{def}}{=} \begin{cases} -sign_\sigma(i) & \text{if } i \in M \\ sign_\sigma(i) & \text{otherwise} \end{cases} .$$

5) For every $i, j \in [0, n-1]$ compute

$$f_{M,\sigma}(i,j) \overset{\text{def}}{=} \begin{cases} 1 & \text{if } s_{M,\sigma}(i) > 0,\ s_{M,\sigma}(j) \geq 0, \text{ and } [\sigma^{-1}(j), j] \subset [\sigma^{-1}(i), i] \\ 1 & \text{if } s_{M,\sigma}(i) < 0,\ s_{M,\sigma}(j) < 0, \text{ and } [j, \sigma^{-1}(j)] \subset [i, \sigma^{-1}(i)] \\ 0 & \text{otherwise} \end{cases} ,$$

where $[a, b]$ is the set of elements $\{a \pmod n, a+1 \pmod n, \ldots, b \pmod n\}$.

Finally, let

$$w_{M,\sigma} = \sum_{i \in [0,n-1] \text{ s.t. } s_{M,\sigma}(i) > 0} d_{M,\sigma}(i) + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\sigma}(i,j).$$

A set M that satisfies the requirements of step (3) is called a *balancing set* for σ. Note, that M is not necessarily unique. For example, if $\sigma =$

$[4,3,6,1,2,5,0]$ then

$$r_\sigma 7 = \sum_{i=0}^{6} sign_\sigma(i) dist_\sigma(i) = 1-2-2+2-3+0-3 = -7$$

and $r_\sigma = -1$. The set $M = \{6\}$ is a set of size one and for every $j \in [0,5]$ such that $sign_\sigma(j) = -$, $dist_\sigma(j) \leq dist_\sigma(6) = 3$. Hence, M is a balancing set for σ, $d_{M,\sigma}(6) = 4$, and $s_{M,\sigma}(6) = +$. $\hat{M} = \{4\}$ is another balancing set for σ. It will be proven in this appendix that $w_\kappa = w_{M,\sigma}$. The proof consists of three arguments. The first argument is that $w_{M,\sigma}$ does not depend on the choice of the balancing set for σ, M. The second argument is that for every $\sigma, \pi \in S_n$, if $d_K(\sigma,\pi) = 1$ then $w_{M,\sigma} = w_{M',\pi} \pm 1$, where M, M' are balancing sets for σ, π, respectively. The last argument is that for every $\sigma \in S_n \setminus \{\varepsilon\}$ there exists $\pi \in S_n$ such that $d_K(\sigma,\pi) = 1$ and $w_{M',\pi} = w_{M,\sigma} - 1$.

As mentioned in Section 5.3, it is more convenient to consider positions and elements of permutations in S_n as residues modulo n. Henceforth, throughout this appendix, both positions and elements of permutations in S_n are taken from the set $[0, n-1] = \{0, 1, \ldots, n-1\}$, and for every $\ell \in \mathbb{Z}$, $\sigma(\ell) = \sigma(\ell \ (\bmod n))$. Under this notations, $(n-1, n) \circ \sigma = (n-1, 0) \circ \sigma$ is the permutation obtained from σ by the exchange of the elements $\sigma(0)$ and $\sigma(n-1)$. By abuse of notation, the set $\{a(\bmod n), a+1(\bmod n), \ldots, b(\bmod n)\}$ is denoted by $[a, b]$.

Lemma B.1 *For every $\sigma \in S_n$,*

$$\sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i) \equiv 0(\ mod\ n).$$

Proof.

$$\sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i) = \sum_{\substack{i \in [0,n-1], \\ sign_\sigma(i) \in \{0,+\}}} dist_\sigma(i) - \sum_{\substack{i \in [0,n-1], \\ sign_\sigma(i) = -}} dist_\sigma(i)$$

$$= \sum_{\substack{i \in [0,n-1], \\ sign_\sigma(i) \in \{0,+\}}} i - \sigma^{-1}(i) - \sum_{\substack{i \in [0,n-1], \\ sign_\sigma(i) = -}} n - (i - \sigma^{-1}(i)$$

$$\equiv \sum_{i=0}^{n-1} i - \sigma^{-1}(i) \ (\bmod n) \equiv \sum_{i=0}^{n-1} i - \sum_{i=0}^{n-1} i \ (\bmod n) \equiv 0 \ (\bmod n).$$

□

Lemma B.1 implies that r_σ is an integer.

Lemma B.2 *For every $\sigma \in S_n$ such that $r_\sigma \neq 0$ there exist at least $|2r_\sigma|$ elements $i \in [0, n-1]$, for which $sign_\sigma(i) = sign(r_\sigma)$.*

Proof. Assume to the contrary that there exist at most $|2r_\sigma| - 1$ elements $i \in [0, n-1]$ for which $sign_\sigma(i) = sign(r_\sigma)$. If $sign(r_\sigma) = -$ then

$$\sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i) > (2r_\sigma + 1)\frac{n}{2} = r_\sigma n + \frac{n}{2} > r_\sigma n.$$

Similarly, if $sign(r_\sigma) = +$ then

$$\sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i) \leq (2r_\sigma - 1)\frac{n}{2} = r_\sigma n - \frac{n}{2} < r_\sigma n.$$

□

Lemma B.2 implies that there exists a balancing set for σ.

Lemma B.3

$$\sum_{i=0}^{n-1} s_{M,\sigma}(i) d_{M,\sigma}(i) = 0.$$

Proof.

$$\sum_{i=0}^{n-1} s_{M,\sigma}(i) d_{M,\sigma}(i) = \sum_{i \in [0,n-1] \setminus M} sign_\sigma(i) dist_\sigma(i) - \sum_{i \in M} sign_\sigma(i)(n - dist_\sigma(i)).$$

$$= -r_\sigma n + \sum_{i=0}^{n-1} sign_\sigma(i) dist_\sigma(i) = -rn + rn = 0.$$

□

Let $N_{M,\sigma,0}$, $N_{M,\sigma,+}$, and $N_{M,\sigma,-}$ be a partition of the elements in $[0, n-1]$ into three classes according to their sign, $s_{M,\sigma}$, i.e.

$$N_{M,\sigma,0} = \{i \ : \ s_{M,\sigma}(i) = 0\}, \qquad N_{M,\sigma,+} = \{i \ : \ s_{M,\sigma}(i) = +\},$$

and

$$N_{M,\sigma,-} = \{i \ : \ s_{M,\sigma}(i) = -\}.$$

Lemma B.4 *Let $i \in [0, n-1]$ and let*

$$I_1 = \{j \in N_{M,\sigma,+} \setminus \{i\} \ : \ i \in [\sigma^{-1}(j), j]\},$$

$$I_2 = \{j \in N_{M,\sigma,-} \setminus \{i\} \ : \ i \in [j, \sigma^{-1}(j)]\}.$$

Then, $|I_1| = |I_2|$.

Proof.
Assume w.l.o.g. that $s_{M,\sigma}(i) \neq -$. For every $j \in [0, n-1]$ define

$$\tilde{d}(j) = \begin{cases} n - d_{M,\sigma}(j), & j \in I_1 \cup I_2, \\ d_{M,\sigma}(j), & \text{otherwise} \end{cases}.$$

and

$$\tilde{s}(j) = \begin{cases} -s_{M,\sigma}(j), & j \in I_1 \cup I_2. \\ s_{M,\sigma}(j), & \text{otherwise.} \end{cases}.$$

Let $\pi = [\sigma(i+1), \sigma(i+2), \ldots, \sigma(n-1), \sigma(0), \sigma(1), \ldots, \sigma(i)]$, and let $\rho = [i+1, i+2, \ldots, n-1, 0, 1, \ldots, i]$. For every $j \in [0, n-1]$, $j \neq i$, $\tilde{d}(j) = \rho^{-1}(j) - \pi^{-1}(j)$ if $\tilde{s}(j) \in \{0, +\}$ and $\tilde{d}(j) = \pi^{-1}(j) - \rho^{-1}(j)$ if $\tilde{s}(j) = -$.

$$\sum_{j=0}^{n-1} \tilde{s}(j)\tilde{d}(j) = \sum_{j,\ \tilde{s}(j) \geq 0} \rho^{-1}(j) - \pi^{-1}(j) - \sum_{j,\ \tilde{s}(j) < 0} \pi^{-1}(j) - \rho^{-1}(j)$$

$$= \sum_{j=0}^{n-1} \rho^{-1}(j) - \sum_{j=0}^{n-1} \pi^{-1}(j) = 0.$$

On the other hand,

$$\sum_{j=0}^{n-1} \tilde{s}(j)\tilde{d}(j) = \sum_{j \in I_1} -(n - d_{M,\sigma}(j)) + \sum_{j \in I_2} n - d_{M,\sigma}(j) +$$

$$\sum_{j \in [0,n-1] \setminus (I_1 \cup I_2)} s_{M,\sigma}(j) d_{M,\sigma}(j) = n|I_2| - n|I_1| + \sum_{j=0}^{n-1} s_{M,\sigma}(j) d_{M,\sigma}(j).$$

By Lemma B.3 it follows that $\sum_{j=0}^{n-1} s_{M,\sigma}(j) d_{M,\sigma}(j) = 0$, and therefore, $n|I_2| - n|I_1| = 0$, i.e. $|I_1| = |I_2|$.

□

Lemma B.5 *Let* $\sigma \in S_n$ *such that* $r_\sigma \neq 0$. *Let* M, *be a balancing set for* σ, *and assume that there exist* $a \in M$ *and* $b \in [0, n-1] \setminus M$ *such that* $sign_\sigma(a) = sign_\sigma(b)$ *and* $dist_\sigma(a) = dist_\sigma(b)$. *Let* $\tilde{M} = (M \setminus \{a\}) \cup \{b\}$. *Then* $w_{M,\sigma} = w_{\tilde{M},\sigma}$.

Proof.

Note, first that $N_{\tilde{M},\sigma,-sign(r_\sigma)} = (N_{M,\sigma,-sign(r_\sigma)} \backslash \{a\}) \cup \{b\}$. By Lemma B.3 it follows that

$$\sum_{i \in N_{M,\sigma,+}} d_{M,\sigma}(i) = \sum_{i \in N_{M,\sigma,-sign(r_\sigma)}} d_{M,\sigma}(i).$$

Therefore,

$$w_{M,\sigma} = \sum_{i \in N_{M,\sigma,-sign(r_\sigma)}} d_{M,\sigma}(i) + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\sigma}(i,j),$$

and similarly,

$$w_{\tilde{M},\sigma} = \sum_{i \in N_{\tilde{M},\sigma,-sign(r_\sigma)}} d_{\tilde{M},\sigma}(i) + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(i,j).$$

Since $d_{M,\sigma}(i) = d_{\tilde{M},\sigma}(i)$ for every $i \in [0, n-1] \backslash \{a, b\}$ and since $d_{M,\sigma}(a) = d_{\tilde{M},\sigma}(b)$, it follows that

$$\sum_{i \in N_{M,\sigma,-sign(r_\sigma)}} d_{M,\sigma}(i) = \sum_{i \in N_{\tilde{M},\sigma,-sign(r_\sigma)}} d_{M,\sigma}(i).$$

Next, it is proved that

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\sigma}(i,j) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(i).$$

Clearly, for every $i, j \in [0, n-1] \setminus \{a, b\}$, $f_{M,\sigma}(i,j) = f_{\tilde{M},\sigma}(i,j)$. Moreover, $dist_\sigma(a) = dist_\sigma(b) \leq dist_\sigma(i)$, for all $i \in M \setminus \{a\}$, which implies that $d_{M,\sigma}(a) \geq d_{M,\sigma}(j)$, $d_{\tilde{M},\sigma}(b) \geq d_{\tilde{M},\sigma}(j)$, for all $j \in [0, n-1]$. It also implies that $d_{\tilde{M},\sigma}(a) \geq d_{\tilde{M},\sigma}(j)$, for all $j \in N_{\tilde{M},\sigma,sign(r_\sigma)}$, and $d_{M,\sigma}(b) \geq d_{M,\sigma}(j)$, for all $j \in N_{M,\sigma,sign(r_\sigma)}$. Therefore, $f_{M,\sigma}(j,a) = 0$, $f_{\tilde{M},\sigma}(j,b) = 0$, $f_{\tilde{M},\sigma}(j,a) = 0$, and $f_{M,\sigma}(j,b) = 0$, for all $j \in [0, n-1]$. Hence, it is enough to show that

$$\sum_{j=0}^{n-1} f_{M,\sigma}(a,j) + f_{M,\sigma}(b,j) = \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(a,j) + f_{\tilde{M},\sigma}(b,j),$$

or equivalently,

$$\sum_{j=0}^{n-1} f_{M,\sigma}(a,j) - f_{\tilde{M},\sigma}(a,j) = \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(b,j) - f_{M,\sigma}(b,j). \tag{B.1}$$

Let

$$I_1 = \{j \in N_{M,\sigma,+} \setminus \{a\} \ : \ a \in [\sigma^{-1}(j), j]\},$$

and

$$I_2 = \{j \in N_{M,\sigma,-} \setminus \{a\} \ : \ a \in [j, \sigma^{-1}(j)]\}.$$

By Lemma B.4, $|I_1| = |I_2|$. Since $d_{M,\sigma}(a)$ is maximal, it follows that there are three types of elements in $N_{M,\sigma,-sign(r_\sigma)} \setminus \{a\}$: The first type is j such that $f_{M,\sigma}(a,j) = 1$. If $sign(r_\sigma) = -$ then this j is such that $[\sigma^{-1}(j), j] \subset [\sigma^{-1}(a), a]$ and if $sign(r_\sigma) = +$ then this j is such that $[j, \sigma^{-1}(j)] \subset [a, \sigma^{-1}(a)]$. The second type is j, such that $\sigma^{-1}(j) \in [\sigma^{-1}(a), a]$ and $j \in [a, \sigma^{-1}(a)]$. If $sign(r_\sigma) = -$ then these are exactly the elements of I_1, otherwise, let x be the number of such elements. The third type is j such that $\sigma^{-1}(j) \in [a, \sigma^{-1}(a)]$ and $j \in [\sigma^{-1}(a), a]$. If $sign(r_\sigma) = +$ then these are exactly the elements of I_2, otherwise, let x be the number of such elements. Note, that since $d_{M,\sigma}(a)$ is maximal, if $sign(r_\sigma) = -$ then x counts the number of elements $j \in [0, n-1]$ such that $\sigma^{-1}(j) \in [a, \sigma^{-1}(a)]$, $s_{M,\sigma}(j) = +$, and $f_{M,\sigma}(a,j) = 0$. There are $|I_2| + \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(a,j)$ elements j such that $\sigma^{-1}(j) \in [a, \sigma^{-1}(a)]$ and $s_{M,\sigma}(j) = -$. Therefore,

$$x = n - d_{M,\sigma}(a) - \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(a,j) - |I_2|. \tag{B.2}$$

Similarly, if $sign(r_\sigma) = +$ then x counts the number of elements $j \in [0, n-1]$ such that $\sigma^{-1}(j) \in [\sigma^{-1}(a), a]$, $s_{M,\sigma}(j) = -$, and $f_{M,\sigma}(a,j) = 0$. There are $|I_1| + \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(a,j)$ elements j such that $\sigma^{-1}(j) \in [\sigma^{-1}(a), a]$ and $s_{M,\sigma}(j) = +$, and since $|I_1| = |I_2|$, it follows that in any case, x satisfies equation (B.2). Thus,

$$|N_{M,\sigma,-sign(r_\sigma)}| - 1 = \sum_{j=0}^{n-1} f_{M,\sigma}(a,j) + |I_1| + n - d_{M,\sigma}(a) - \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(a,j) - |I_2|.$$

$$= \sum_{j=0}^{n-1} f_{M,\sigma}(a,j) - \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(i_1,j) + n - d_{M,\sigma}(a).$$

It follows that,

$$\sum_{j=0}^{n-1} f_{M,\sigma}(a,j) - \sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(a,j) = |N_{M,\sigma,-sign(r_\sigma)}| - 1 - n + d_{M,\sigma}(a).$$

The same arguments are applied to derive that

$$\sum_{j=0}^{n-1} f_{\tilde{M},\sigma}(b,j) - \sum_{j=0}^{n-1} f_{M,\sigma}(b,j) = |N_{\tilde{M},\sigma,-sign(r_\sigma)}| - 1 - n + d_{\tilde{M},\sigma}(b).$$

Since $|N_{\tilde{M},\sigma,-sign(r_\sigma)}| = |N_{M,\sigma,-sign(r_\sigma)}|$ and $d_{M,\sigma}(a) = d_{\tilde{M},\sigma}(b)$, it follows that equation (B.1) holds, which completes the proof of the lemma.

□

Corollary B.6 *The value of $w_{M,\sigma}$ does not depend on the choice of the balancing set M.*

Proof. Let M and $\tilde{M}$ be two balancing sets for σ, i.e. $sign_\sigma(i) = sign(r_\sigma)$, for every $i \in M \cup \tilde{M}$, $dist_\sigma(j) \leq dist_\sigma(i)$ for every $i \in M$, $j \in [0, n-1] \setminus M$, and $dist_\sigma(j) \leq dist_\sigma(i)$,for every $i \in \tilde{M}$, $j \in [0, n-1] \setminus \tilde{M}$. In particular, for every $a \in M \setminus \tilde{M}$ and for every $b \in \tilde{M} \setminus M$, $dist_\sigma(a) \leq dist_\sigma(b)$ and $dist_\sigma(b) \leq dist_\sigma(a)$, hence, $dist_\sigma(a) = dist_\sigma(b)$. Moreover, since M and $\tilde{M}$ are both sets of size $|r_\sigma|$ it follows that $|M \setminus \tilde{M}| = |\tilde{M} \setminus M|$. Let $M \setminus \tilde{M} = \{a_1, a_2, \ldots, a_\ell\}$, $\tilde{M} \setminus M = \{b_1, b_2, \ldots, b_\ell\}$, and let $M_1 = (M \setminus \{a_1\}) \cup \{b_1\}$. For every $2 \leq t \leq \ell$, let $M_t = (M_{t-1} \setminus \{a_t\}) \cup \{b_t\}$. Note, that $M_\ell = \tilde{M}$. By Lemma B.5, it follows that $w_{M,\sigma} = w_{M_1,\sigma} = \ldots = w_{M_t,\sigma} = w_{\tilde{M},\sigma}$.

□

Corollary B.6 states that the value of $w_{M,\sigma}$ does not depend on the choice of the balancing set M. Each permutation $\sigma \in S_n$ is assigned with a non-negative integer w_σ, where $w_\sigma = w_{M,\sigma}$ for some balancing set for σ, M, and this assignment is well defined. In what follows, it will be proved that $w_\sigma = w_\kappa(\sigma)$. To this end, it is proved that for every $\sigma, \pi \in S_n$, $d_\kappa(\sigma, \pi) = 1$ then $w_\pi = w_\sigma \pm 1$. Let $\sigma, \pi \in S_n$ such that $d_\kappa(\sigma, \pi) = 1$, i.e. $\pi = (\ell, \ell+1) \circ \sigma$, where $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$. In order to show that $w_\pi = w_\sigma \pm 1$ we will show the existence of a balancing set for σ, M, and a balancing set for π, $\tilde{M}$, such that $s_{M,\sigma}(i) = s_{\tilde{M},\pi}(i)$, for every $i \in [0, n-1]$ (with exception for $i = a$ if $s_{M,\sigma}(a) = 0$ or $s_{\tilde{M},\pi}(i) = 0$ and for $i = b$ if $s_{M,\sigma}(b) = 0$ or $s_{\tilde{M},\pi}(b) = 0$). This will simplify the computation of $d_{\tilde{M},\pi}(i)$ and $f_{\tilde{M},\pi}(i,j)$, in terms of $d_{M,\sigma}(i)$ and $f_{M,\sigma}(i)$, respectively, for every $i \in [0, n-1]$. The balancing set for π, $\tilde{M}$, will depend on $sign_\sigma(a)$, $sign_\sigma(b)$, $dist_\sigma(a)$, $dist_\sigma(b)$, and whether or not $a, b \in M$. In order to find such balancing sets for σ and π, it is required to compute r_π in terms of r_σ. This is done by simply computing $dist_\pi(a)$, $dist_\pi(b)$, $sign_\pi(a)$, and $sign_\pi(b)$, in terms of $dist_\sigma(a)$, $dist_\sigma(b)$,

$sign_\sigma(a)$, and $sign_\sigma(b)$, respectively, and substitute these values in

$$r_\pi n = \sum_{i=0}^{n-1} sign_\pi(i) dist_\pi(i).$$

$$dist_\pi(a) = \begin{cases} dist_\sigma(a) - 1 & \text{if } sign_\sigma(a) = + \\ dist_\sigma(a) + 1 & \text{if } sign_\sigma(a) = 0 \\ dist_\sigma(a) + 1 & \begin{array}{c}\text{if } sign_\sigma(a) = - \text{ and} \\ dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor\end{array} \\ n - (dist_\sigma(a) + 1) & \begin{array}{c}\text{if } sign_\sigma(a) = - \text{ and} \\ dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor\end{array} \end{cases}. \qquad \text{(B.3)}$$

$$sign_\pi(a) = \begin{cases} + & \text{if } sign_\sigma(a) = + \text{ and } dist_\sigma(a) > 1 \\ 0 & \text{if } sign_\sigma(a) = + \text{ and } dist_\sigma(a) = 1 \\ - & \text{if } sign_\sigma(a) = 0 \\ - & \text{if } sign_\sigma(a) = - \text{ and } dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor \\ + & \text{if } sign_\sigma(a) = - \text{ and } dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor \end{cases}. \qquad \text{(B.4)}$$

$$dist_\pi(b) = \begin{cases} dist_\sigma(b) - 1 & \text{if } sign_\sigma(b) = - \\ dist_\sigma(b) + 1 & \text{if } sign_\sigma(b) = 0 \\ dist_\sigma(b) + 1 & \begin{array}{c}\text{if } sign_\sigma(b) = + \text{ and} \\ dist_\sigma(b) < \left\lfloor \frac{n}{2} \right\rfloor\end{array} \\ n - (dist_\sigma(b) + 1) & \begin{array}{c}\text{if } sign_\sigma(b) = + \text{ and} \\ dist_\sigma(b) = \left\lfloor \frac{n}{2} \right\rfloor\end{array} \end{cases}. \qquad \text{(B.5)}$$

$$sign_\pi(b) = \begin{cases} - & \text{if } sign_\sigma(b) = - \text{ and } dist_\sigma(b) > 1 \\ 0 & \text{if } sign_\sigma(b) = - \text{ and } dist_\sigma(b) = 1 \\ + & \text{if } sign_\sigma(b) = 0 \\ + & \text{if } sign_\sigma(b) = + \text{ and } dist_\sigma(b) < \left\lfloor \frac{n}{2} \right\rfloor \\ - & \text{if } sign_\sigma(b) = + \text{ and } dist_\sigma(b) = \left\lfloor \frac{n}{2} \right\rfloor \end{cases}. \qquad \text{(B.6)}$$

The values of r_π in terms of r_σ are summarized in Table 7.1.

$sign_\sigma(a)$ $sign_\sigma(b)$	$sign_\sigma(a) \in \{0,+\}$	$sign_\sigma(a) = -$ $dist_\sigma(a) < \lfloor\frac{n-1}{2}\rfloor$	$sign_\sigma(a) = -$ $dist_\sigma(a) = \lfloor\frac{n-1}{2}\rfloor$
$sign_b \in \{0,-\}$	r_σ	r_σ	$r_\sigma + 1$
$sign_\sigma(b) = +$ $dist_\sigma(b) < \lfloor\frac{n}{2}\rfloor$	r_σ	r_σ	$r_\sigma + 1$
$sign_\sigma(b) = +$ $dist_\sigma(b) = \lfloor\frac{n}{2}\rfloor$	$r_\sigma - 1$	$r_\sigma - 1$	r_σ

Table 7.1: Values of r_π in terms of r_σ

Lemma B.7 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$. Assume that $dist_\sigma(a) = 0$ and $dist_\sigma(b) = 0$, i.e. $\ell = a$ and $b \equiv \ell + 1 \ (\ mod\ n)$. Then $w_\pi = w_\sigma + 1$.*

Proof.

Let M be a balancing set for σ. As shown in Table 7.1, $r_\pi = r_\sigma$. Moreover, $dist_\pi(a) = 1$, $dist_\pi(b) = 1$, and for every $i \in M$, $dist_\pi(i) = dist_\sigma(i) \geq 1$. Therefore, M is also a balancing set for π. Since $a, b \notin M$ it follows that $d_{M,\pi}(a) = d_{M,\pi}(b) = 1$, $s_{M,\pi}(a) = -$, and $s_{M,\pi}(b) = +$. For every $i \in [0, n-1] \setminus \{a, b\}$ we have that $d_{M,\pi}(i) = d_{M,\sigma}(i)$ and $s_{M,\pi}(i) = s_{M,\sigma}(i)$. By definition,

$$w_\pi = \sum_{i \in N_{M,\pi,+}} d_{M,\pi}(i) + \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{M,\pi}(i,j),$$

and $f_{M,\pi}(i,j) = f_{M,\sigma}(i,j)$, for every $i \in [0, n-1]$, $j \in [0, n-1] \setminus \{a\}$. By Lemma B.4 it follows that

$$\sum_{j=0}^{n-1} f_{M,\sigma}(j,a) = |\{j \in N_{M,\sigma,-} \ : \ a \in [j, \sigma^{-1}(j)]\}| = \sum_{j=0}^{n-1} f_{M,\pi}(j,a).$$

Note, that $N_{M,\pi,+} = N_{M,\sigma,+} \cup \{b\}$. Therefore,

$$w_\pi = \sum_{i \in N_{M,\sigma,+}} d_{M,\sigma}(i) + \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{M,\sigma}(i,j) + d_{M,\pi}(b) = w_\sigma + 1.$$

□

Lemma B.8 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, and let M be a balancing set for σ. If $s_{M,\sigma}(a) = +$ and $dist_\sigma(b) = 0$, i.e. $b \equiv \ell + 1 \ (\ mod\ n)$, then $w_\pi = w_\sigma - 1$.*

Proof. We distinguish between two cases.

Case 1: $a \in M$. In that case $r_\sigma < 0$ and $sign_\sigma(a) = -$. If $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$ then $r_\pi = r_\sigma$. Since $dist_\pi(a) = dist_\sigma(a) + 1$, it follows that M is also a balancing set for π and that $d_{M,\pi}(a) = d_{M,\sigma}(a) - 1$, $d_{M,\pi}(b) = 1$, $s_{M,\pi}(a) = +$, and $s_{M,\pi}(b) = +$. For every $i \in [0, n-1] \setminus \{a, b\}$ we have that $d_{M,\pi}(i) = d_{M,\sigma}(i)$ and $s_{M,\pi}(i) = s_{M,\sigma}(i)$. By definition,

$$w_\pi = \sum_{i \in N_{M,\pi,+}} d_{M,\pi}(i) + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\pi}(i,j),$$

and $f_{M,\pi}(i,j) = f_{M,\sigma}(i,j)$, for every $i \in [0, n-1]$, $j \in [0, n-1]$, where $(i,j) \neq (a,b)$. Since $b \in [\sigma^{-1}(a), a]$ it follows that $f_{M,\sigma}(a,b) = 1$ and $f_{M,\pi}(a,b) = 0$. Note, that $N_{M,\pi,+} = N_{M,\sigma,+} \cup \{b\}$. Therefore,

$$w_\pi = \sum_{i \in N_{M,\sigma,+}} d_{M,\sigma}(i) - 1 + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\sigma}(i,j) - 1 + d_{M,\pi}(b) = w_\sigma - 1.$$

If $dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor$ then $r_\pi = r_\sigma + 1$ and $M \setminus \{a\}$ is a balancing set for π. The same arguments that were used to the case where $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$ show that $w_\pi = w_\sigma - 1$.

Case 2: $a \notin M$. In that case $sign_\sigma(a) \in \{0, +\}$, $r_\pi = r_\sigma$, and M is also a balancing set for π. The same arguments that were used to prove case 1 show that $w_\pi = w_\sigma - 1$.

□

Lemma B.9 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, and let M be a balancing set for σ. If $dist_\sigma(a) = 0$, i.e. $\ell = a$, and if $s_{M,\sigma}(b) = -$, then $w_\pi = w_\sigma - 1$.*

Proof. The case $dist_\sigma(a) = 0$ and $s_{M,\sigma}(b) = -$ is symmetric to the case $s_{M,\sigma}(a) = +$ and $dist_\sigma(b) = 0$ that was stated in Lemma B.8.

□

Lemma B.10 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, an let M be a balancing set for σ. If $s_{M,\sigma}(a) = +$ and $s_{M,\sigma}(b) = -$ then $w_\pi = w_\sigma - 1$.*

Proof. We distinguish between three cases.

Case 1: $a \in M$. In that case $r_\sigma < 0$ and $sign_\sigma(a) = -$. If $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$ then $r_\pi = r_\sigma$. Since $dist_\pi(a) = dist_\sigma(a) + 1$, it follows that M is also a balancing set for π and that $d_{M,\pi}(a) = d_{M,\sigma}(a) - 1$, $d_{M,\pi}(b) = d_{M,\sigma}(b) - 1$, $s_{M,\pi}(a) = +$, and $s_{M,\pi}(b) = -$. For every $i \in [0, n-1] \setminus \{a, b\}$ we have that $d_{M,\pi}(i) = d_{M,\sigma}(i)$ and $s_{M,\pi}(i) = s_{M,\sigma}(i)$. By definition,

$$w_\pi = \sum_{i \in N_{M,\pi,+}} d_{M,\pi}(i) + \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\pi}(i,j),$$

and $f_{M,\pi}(i,j) = f_{M,\sigma}(i,j)$, for every $i \in [0, n-1]$, $j \in [0, n-1] \setminus \{b\}$. If $dist_\sigma(b) > 1$ then $f_{M,\pi}(i,b) = f_{M,\sigma}(i,b)$. Otherwise, if $dist_\sigma(b) = 1$ then by Lemma B.4 it follows that

$$\sum_{j=0}^{n-1} f_{M,\pi}(j,b) = |\{j \in N_{M,\pi,-} \ : \ b \in [j, \pi^{-1}(j)]\}| = \sum_{j=0}^{n-1} f_{M,\sigma}(j,b).$$

In any of these cases it follows that

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\pi}(i,j) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{M,\sigma}(i,j).$$

Note, that $N_{M,\pi,+} = N_{M,\sigma,+}$ and therefore $w_\pi = w_\sigma - 1$. If $dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor$ then $r_\pi = r_\sigma + 1$ and $M \setminus \{a\}$ is a balancing set for π. The same arguments that were used to the case where $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$ show that $w_\pi = w_\sigma - 1$.

Case 2: $b \in M$. This case is symmetric to case 1.

Case 3: $a, b \notin M$. In that case $sign_\sigma(a) = +$, $sign_\sigma(b) = -$, $r_\pi = r_\sigma$, and M is also a balancing set for π. The same arguments that were used to prove case 1 show that $w_\pi = w_\sigma - 1$.

□

Lemma B.11 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, an let M be a balancing set for σ. If $s_{M,\sigma}(a) = +$ and $s_{M,\sigma}(b) = +$ then $w_\pi = w_\sigma \pm 1$.*

Proof. We distinguish between four cases:

Case 1: $b \in M$ and there exists a $c \in [0, n-1] \setminus M$, where $sign_\sigma(c) = sign_\sigma(b)$, such that $\tilde{M} = (M \setminus \{b\}) \cup \{c\}$ is a balancing set for σ. In this case

$w_\pi = w_\sigma - 1$. Indeed, since $b \in M$ it follows that $sign_\sigma(b) = -$. Note, that $c \neq a$ because otherwise, $a \notin M$ and $sign_\sigma(a) = + \neq sign_\sigma(b)$, and it follows that a does not belong to any balancing set for σ. Since $\tilde{M}$ is a balancing set for σ, $b \notin \tilde{M}$, $c \neq a$, it follows that $s_{\tilde{M},\sigma}(a) = s_{M,\sigma}(a) = +$ and $s_{\tilde{M},\sigma}(b) = -$. By Lemma B.10 it follows that $w_\pi = w_\sigma - 1$.

Case 2: Every balancing set for σ contains b. In this case $w_\pi = w_\sigma + 1$. Indeed, since every balancing set for σ contains b it follows that for every $i \notin M$, such that $sign_\sigma(i) = sign_\sigma(b) = -$, we have that $dist_\sigma(i) < dist_\sigma(b)$. If $a \notin M$ or $a \in M$ and $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$ then $r_\pi = r_\sigma$ and $\tilde{M} = M$ is a balancing set for π. If $a \in M$ and $dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor$ then $\tilde{M} = M \setminus \{a\}$ is a balancing set for π. Following the same arguments used in the proofs of the previous Lemmas to compute $d_{\tilde{M},\pi}(i)$ and $f_{\tilde{M},\pi}(i,j)$, for every $i, j \in [0, n-1]$, it can be readily verified that $w_\pi = w_\sigma + 1$.

Case 3: $b \notin M$ and there exists a $c \in M$ such that $\tilde{M} = (M \setminus \{c\}) \cup \{b\}$ is a balancing set for σ. In this case it is shown that $w_\pi = w_\sigma - 1$. Since $b \notin M$ it follows that $sign_\sigma(b) = +$. Note, that $c \neq a$ because otherwise, $a \in M$, $sign_\sigma(a) = - \neq sign_\sigma(b)$, and it follows that b does not belong to any balancing set for σ. Since $\tilde{M}$ is a balancing set for σ, $b \in \tilde{M}$, and $c \neq a$, it follows that $s_{\tilde{M},\sigma}(a) = s_{M,\sigma}(a) = +$ and $s_{\tilde{M},\sigma}(b) = -$. By Lemma B.10 it follows that $w_\pi = w_\sigma - 1$.

Case 4: Every balancing set for σ does not contain b. In that case it is shown that $w_\pi = w_\sigma + 1$. Since $b \notin M$ it follows that $sign_\sigma(b) = +$. Assume first that $dist_\sigma(b) < \left\lfloor \frac{n}{2} \right\rfloor$. If $a \notin M$ or $a \in M$ and $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$ then $r_\pi = r_\sigma$ and $\tilde{M} = M$ is a balancing set for π. If $a \in M$ and $dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor$ then $\tilde{M} = M \setminus \{a\}$ is a balancing set for π. For $dist_\sigma(b) = \left\lfloor \frac{n}{2} \right\rfloor$, we have that $\tilde{M} = M \cup \{b\}$ is a balancing set for π, unless $a \in M$ and $dist_\sigma(a) = \left\lfloor \frac{n-1}{2} \right\rfloor$, in that case $\tilde{M} = (M \setminus \{a\}) \cup \{b\}$ is a balancing set for π. Following the same arguments used in the proofs of the previous Lemmas to compute $d_{\tilde{M},\pi}(i)$ and $f_{\tilde{M},\pi}(i,j)$, for every $i, j \in [0, n-1]$, it can be readily verified that $w_\pi = w_\sigma + 1$.

□

Lemma B.12 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, and let M be a balancing set for σ. If $s_{M,\sigma}(a) = -$ and $s_{M,\sigma}(b) = -$ then $w_\pi = w_\sigma \pm 1$.*

Proof. The case $s_{M,\sigma}(a) = -$ and $s_{M,\sigma}(b) = -$ is symmetric to the case $s_{M,\sigma}(a) = +$ and $s_{M,\sigma}(b) = +$ that was stated in LemmaB.11.

□

The following Lemma is derived by a similar arguments to those that were used in the proofs of Lemmas B.8, B.10, and B.11.

Lemma B.13 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, an let M be a balancing set for σ. If $dist_\sigma(a) = 0$, i.e. $\ell = a$, and if $s_{M,\sigma}(b) = +$ then $w_\pi = w_\sigma \pm 1$.*

Lemma B.14 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, an let M be a balancing set for σ. If $s_{M,\sigma}(a) = -$ and $dist_\sigma(b) = 0$ i.e. $b \equiv \ell + 1 \ (\mod n)$, then $w_\pi = w_\sigma \pm 1$.*

Proof. The case $dist_\sigma(a) = -$ and $dist_\sigma(b) = 0$ is symmetric to the case $dist_\sigma(a) = 0$ and $s_\sigma(b) = +$ that was stated in LemmaB.13.

□

Lemma B.15 *Let $\sigma, \pi \in S_n$, where $\pi = (\ell, \ell+1) \circ \sigma$, $\sigma(\ell) = a$, and $\sigma(\ell+1) = b$, an let M be a balancing set for σ. If $s_{M,\sigma}(a) = -$ and $s_{M,\sigma}(b) = +$ then $w_\pi = w_\sigma \pm 1$.*

Proof.

If there exists a balancing set for σ, $\hat{M}$, such that $s_{\hat{M},\sigma}(a) = +$ or $s_{\hat{M},\sigma}(b) = -$ then from Lemmas B.10, B.11, and B.12 it follows that $w_\pi = w_\sigma \pm 1$. Otherwise, assume without loss of generality that $r_\sigma \leq 0$. This implies that every balancing set for σ does not contain a and therefore, $sign_\sigma(a) = -$ and $dist_\sigma(a) < \left\lfloor \frac{n-1}{2} \right\rfloor$. Then either every balancing set for σ contains b or every balancing set for σ does not contain b. Assume first that every balancing set for σ contains b. In that case $sign_\sigma(b) = -$ and for every $c \in [0, n-1] \setminus M$, where $sign_\sigma(c) = -$, we have that $dist_\sigma(c) < dist_\sigma(b)$. In particular, $1 \leq dist_\sigma(a) < dist_\sigma(b)$. It follows that $\tilde{M} = M$ is a balancing set for σ.

For the case where every balancing set for σ does not contain b, we have that $sign_\sigma(b) = +$. If $dist_\sigma(b) < \left\lfloor \frac{n}{2} \right\rfloor$ then $\tilde{M} = M$ is a balancing set for σ. Otherwise, if $dist_\sigma(b) = \left\lfloor \frac{n}{2} \right\rfloor$, then $\tilde{M} = M \cup \{b\}$ is balancing set for σ. Following the same arguments used in the previous Lemmas to compute $d_{\tilde{M},\pi}(i)$ and $f_{\tilde{M},\pi}(i,j)$ for every $i, j \in [0, n-1]$, it can be readily verified that $w_\pi = w_\sigma + 1$.

□

Corollary B.16 *For every $\sigma, \pi \in S_n$, $d_\kappa(\sigma, \pi) = 1$ then $w_\pi = w_\sigma \pm 1$.*

Proof. Follows from Lemmas B.7, B.8, B.9, B.10, B.11, B.13, B.14, B.12, and B.15.

□

Theorem B.17 *For every $\sigma \in S_n$, $w_\sigma = w_\kappa(\sigma)$.*

Proof. Let $\sigma \in S_n$ and let $w = w_\sigma$. The theorem is proved by induction on w. For the basis of the induction we have to show that $w = 0$ if and only if σ is the identity permutation of S_n, ε. Clearly, $w_\varepsilon = 0$. Moreover, $w_\sigma = 0$ implies that $dist_\sigma(i) = 0$, for every $i \in [0, n-1]$, and therefore $\sigma = \varepsilon$. The induction hypothesis states that for every $\pi \in S_n$, if $w_\pi < w$ then $w_\pi = w_\kappa(\pi)$. Assume that $w > 0$ and let M be a balancing set for σ. Since $w > 0$ it follows that $\sigma \neq \varepsilon$. Hence, there must exist $a, b \in [0, n-1]$ such that $s_{M,\sigma}(a) = +$ and $s_{M,\sigma}(b) = -$. In particular, there must exist $a \in [0, n-1]$ such that $s_{M\sigma}(a) = +$ and $s_{M,\sigma,b} \neq +$, where $b = \sigma(\sigma^{-1}(a) + 1)$. Then by Lemmas B.8 and B.10, it follows that for $\pi = (\ell, \ell+1) \circ \sigma$, $w_\pi = w - 1$. By the induction hypothesis $w_\pi = w_\kappa(\pi)$ and from $d_\kappa(\sigma, \pi) = 1$, we conclude that $w_\kappa(\sigma) \leq w$. By Corollary B.16 and since $w_\varepsilon = 0$, it follows that $w \leq w_\kappa(\sigma)$, and therefore $w_\sigma = w_\kappa(\sigma)$.

□

Bibliography

[1] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Designs, Codes Crypto.*, vol. 22, pp. 221–237, 2001.

[2] R. Ahlswede, H. Aydinian, and L. Khachatrian, "Unidirectional error control codes and related combinatorial problems", in Proc. *Eighth Int. Workshop Algebr. Combin. Coding Theory (ACCT-8)*, St. Petersburg, pp. 6–9, 2002.

[3] R. Ahlswede and V. Blinovsky, *Lectures on Advances in Combinatorics*, Springer-Verlag, 2008.

[4] C. Araujo, I. Dejter, P. Horak, "A generalization of Lee codes," *Des. Codes Cryptogr.,* vol. 70, pp. 77–90, 2014.

[5] A. Barg and A. Mazumdar, "Codes in permutations and error correction for rank modulation," *IEEE Trans. on Inform. Theory*, vol. 56, no. 7, pp. 3158–3165, July 2010.

[6] S. Buzaglo and E. Yaakobi, "Constrained codes for rank modulation," *Proc. IEEE International Symp. on Information Theory*, Honolulu, HI, June-July 2014.

[7] S. Buzaglo, E. Yaakobi, T. Etzion, and J. Bruck, "Error-correcting codes for multipermutations," *Proc. IEEE International Symp. on Information Theory*, pp. 724–728, Istanbul, Turkey, July 2013.

[8] P. J. Cameron *Permutation Groups,* London Mathematical Society Student Texts 45, Cambridge University Press, ISBN 978-0-521-65378-7

[9] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes multi-level flash memories: correcting asymmetric limited-magnitude errors", in Proc. *IEEE Inter. Symp. on Inform. Theory,* Nice, pp. 1176–1180, 2007.

[10] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with application to multilevel flash memories", *IEEE Trans. Inform. Theory*, vol. IT-56, pp. 1582–1595, 2010.

[11] Y. Cassuto and E. Yaakobi, "Short q-ary WOM codes with hot/cold write differentiation", in Proc. *IEEE Inter. Symp. on Inform. Theory,* Boston, pp. 1396–1400, 2012.

[12] P. Cappelletti and A. Modelli, "Flash memory reliability," in *Flash Memories*, P. Cappelletti, C. Golla, P. Olivo, and E. Zanoni, Eds. Amsterdam, The Netherlands: Kluwer, 1999, pp. 399–441.

[13] A. Cayley, "Desiderata and suggestions: No. 2. The Theory of groups: graphical representation," *Amer. J. Math.*, vol. 1, pp. 174–176, 1878.

[14] J. Charlebois, "Tiling by (k, n)-crosses," *Electronic Journal of Undergraduate Mathematics,* 7, pp. 1–11, 2001.

[15] L. Chihara, "On the zeros of the Askey-Wilson polynomials, with applications to coding theory," *SIAM J. Math. Anal.*, vol. 18, pp. 191–207, 1987.

[16] G. D. Cohen, P. Godlewski, F. Merkx, "Linear binary code for write-once memories", *IEEE Trans. Inform. Theory*, vol IT-32, pp. 697–700, 1986.

[17] T. M. Cover, "Enumerative source encoding," *IEEE Trans. on Information Theory*, vol. 19, pp. 73–77, January 1973.

[18] I. J. Dejter, personal communication, 2011.

[19] Ph. Delsarte, "An algebraic approach to association schemes of coding theory", *Philips J. Res.*, vol. 10, pp. 1–97, 1973.

[20] M. Deza and H. Huang, "Metrics on permutations, a survey," *J. Comb. Inf. Sys. Sci.*, vol. 23, pp. 173–185, 1998.

[21] P. Diaconis and R. L. Graham, "Spearman's foortule as a measue of disarray," *J. Roy. Statis. Soc. B*, vol. 39, no. 2, pp. 262–268, 1977.

[22] L. Dolecek, "Towards longer lifetime of emerging technologies using number theory", in Proc. *Workshop on the Application of*

Commun. Theory to Emerging Memory Technologies, Miami, pp. 1936–1940, 2010.

[23] N. Elarief and B. Bose, "Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude", *IEEE Trans. on Inform. Theory,* vol. IT-56, pp. 979–983, 2010.

[24] E. En Gad, A. Jiang, and J. Bruck, "Trade-offs between instantaneous and total capacity in multi-cell flash memories," *Proc. IEEE International Symp. on Information Theory*, pp. 990–994, Cambridge, MA, July 2012.

[25] E. En Gad, E. Yaakobi, A. Jiang, and J. Bruck, "Rank-modulation rewriting codes for flash memories," *Proc. IEEE Inter. Symp. on Information Theory*, pp. 704–708, Istanbul, Turkey, July 2013.

[26] T. Etzion, "On the nonexistence of perfect codes in the Johnson scheme," *SIAM Journal on Discrete Mathematics*, vol. 9, pp. 201–209, May 1996.

[27] T. Etzion, "Product constructions for perfect Lee codes," *IEEE Trans. on Inform. Theory*, vol. IT-57, pp. 7473–7481, November 2011.

[28] T. Etzion and M. Schwartz, "Perfect constant-weight codes," *IEEE Trans. on Inform. Theory,* IT-50, pp. 2156–2165, September 2004.

[29] T. Etzion and A. Vardy, "Perfect binary codes: constructions, properties, and enumeration," *IEEE Trans. on Inform. Theory*, vol. IT-40, pp. 754–763, May 1994.

[30] H. Everett and D. Hickerson, "Packing and covering by translates of certain nonconvex bodies," *Proc. Amer. Math. Soc.,* 75, pp. 87–91, 1979.

[31] X. Feng, B. Chitturi, and H. Sudborough, "Sorting circular permutations by bounded transpositions," *Advances in Computational Biology: Advances in Experimental Medicine and Biology*, vol. 680, pp. 725–736, 2010.

[32] A. Fiat and A. Shamir, "Generalized write-once memories", *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 470–480, 1984.

[33] F. Fu and H. J. Han Vinck, "On the capacity of generalized write once memory with state transitions described by an arbitrary directed acyclic graph", *IEEE Trans. Inform. Theory*, vol. IT-45, pp. 308–313, 1999.

[34] S. Gerschgorin, "Über die abgrenzung der eigenwerte einer matrix," *Izv. Akad. Nauk. USSR Otd. Fiz.-Mat. Nauk.*, vol. 7, pp. 749–754, 1931.

[35] S. W. Golomb, "A general formulation of error metrics," *IEEE Trans. on Information Theory,* 15, pp. 425–426, 1969.

[36] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyminoes," *SIAM J. Appl. Math.*, vol. 18, no. 2, pp. 302–317, January 1970.

[37] G. Haj*ó*s, "Uber einfache und mehrfache Bedeckung des n-dmensionalen Raumes mit einem Wrflegitter," *Math. Zeit.*, vol. 47,427–467, 1942.

[38] W. Hamakar and S. Stein, *Spliting groups by integers*, Proc. Amer. Math. Soc., 46 (1974), pp. 322–324.

[39] W. Hamakar and S. Stein, *Combinatorial packing of* $\mathbb{R}^3$ *by certain error spheres*, IEEE Trans. on Information Theory, 30 (1984), pp. 364–368.

[40] D. Hickerson, *Splitting of finite groups*, Pacific J. Math., vol. 107, pp. 141–171, 1983.

[41] P. Horak, "On perfect Lee codes," *Discrete Mathematics*, vol. 309, pp. 5551–5561, 2009.

[42] M. Jerrum, "The complexity of finding minimum-length generator sequences," *Theor. Comput. Sci.*, vol. 36, pp. 265–289,1985.

[43] A. Jiang, R. Mateescu, M. Schwartz, and J. Bruck, "Rank modulation for flash memories," *IEEE Trans. on Inform. Theory*, vol. 55, no. 6, pp. 2659–2673, June 2009.

[44] A. Jiang, M. Schwartz, and J. Bruck, "Correcting charge-constrained errors in the rank-modulation scheme," *IEEE Trans. on Inform. Theory*, vol. 56, no. 5, pp. 2112–2120, May 2010.

[45] F. Kárteszi, *Szemléletes geometria*, Gondolat, Budapest, 1966.

[46] M. Kendall and J. D. Gibbons, *Rank Correlation Methods*, New York: Oxford Univ. Press, 1990.

[47] T. Kløve, "Lower bounds on the size of spheres of permutations under the Chebychev distance," *Designs, Codes Cryptography,* vol. 59, no. 1-3, pp. 183–191, 2011.

[48] T. Kløve, B. Bose, and N. Elarief, "Systematic single limited magnitude asymmetric error correcting codes", *IEEE Trans. Inform. Theory*, vol. IT-57, pp. 4477–4487, 2011.

[49] T. Kløve, T.-T. Lin, D.-C. Tsai, and W.-G Tzeng, "Permutation arrays under the Chebychev distance," *IEEE Trans. on Inform. Theory*, vol. 56, no. 6, pp. 2611–2617, June 2010.

[50] T. Kløve, J. Luo, I. Naydenova, and S. Yari, "Some codes correcting asymmetric errors of limited magnitude", *IEEE Trans. Inform. Theory*, vol. IT-57, pp. 7459–7472, 2011.

[51] D. E. Knuth, *The Art of Computer Programming, Volume 3: Sorting and Searching*, Reading, MA: Addiaon-Wesley, 1998.

[52] M. Kolountzakis, "Lattice tilings by cubes: whole, notched and extended", *Electron. J. Combin.*, vol. 5, pp. 1–11, 1998.

[53] M. Kolountzakis and J. H. Schmerl, personal communication, 2011

[54] J.-D. Lee, S.-H. Hur, and J.-D. Choi, "Effects of floating-gate interference on NAND flash memory cell operation," *IEEE Electron Device Letters*, vol. 23, no. 5, pp. 264–266, May 2002.

[55] J.-Y. Lee and R. V. Moody, "Lattice substitution system and model sets", *Discrete and Computational Geometry*, vol. 25, pp. 173–201, 2001.

[56] G. Louchard and H. Prodinger, "The number of inversions in permutations: A saddle point approach," *J. Integer Seq.,* vol. 6, Article. 03.2.8 (electronic), 2003.

[57] P. Loomis, "The covering constant of a certain symmetric star body," *Sitzungsberichte der österreichischen Akadamie der Wissenschaften,* pp. 295–308, 1984.

[58] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[59] B. H. Margolius, “Permutations with inversions,” *J. Integer Seq.,* vol. 3, Article. 01.2.4 (electronic), 2001.

[60] W. J. Martin and X. J. Zhu, “Anticodes for the Grassmann and bilinear forms graphs,” *Designs, Codes, and Cryptography,* vol. 6, pp. 73–79, 1995.

[61] A. Mazumdar, A. Barg and G. Zémor, “Construction of rank modulation codes,” *IEEE Trans. on Information Theory*, vol. 59, pp. 1018–1029, February 2013.

[62] M. Mollard, “A generalized parity function and its use in the construction of perfect codes”, *SIAM J. Alg. Disc. Meth.*, vol. 7, pp. 113–115, 1986.

[63] K. O’Bryant, “A complete annotated bibliography of work related to Sidon sequences”, *The Elec. J. of Combin.*, DS11, pp. 1–39, July 2004.

[64] K. T. Phelps, “A combinatorial construction of perfect codes”, *SIAM J. Alg. Disc. Meth.*, vol. 4, pp. 398–403, 1983.

[65] K. T. Phelps, “A general product construction for error-correcting codes”, *SIAM J. Alg. Disc. Meth.*, vol. 5, pp. 224–228, 1984.

[66] K. T. Phelps, “A product construction for perfect codes over arbitrary alphabets”, *IEEE Trans. on Inform. Theory*, vol. IT-30, pp. 769–771, September 1984.

[67] K. A. Post, “Nonexistence theorems on perfect Lee codes over large alphavets,” *Information and Control*, vol. 29, pp. 302–317, 1975.

[68] T. R. N. Rao and E. Fujiwara, *Error-Control Coding for Computer Systems*, London, U.K.: Prentice-Hall, 1989.

[69] B.C. Rennie and A.J. Dobson, “On Striling numbers of the second kind,” *J. Combinatorial Theory*, vol. 7, pp. 116–121, 1969.

[70] R. L. Rivest and A. Shamir, “How to reuse a write-once memory”, *Information and Control*, vol. 55, pp. 1–19, 1982.

[71] C. Roos, “A note on the existence of perfect constant weight codes,” *Discrete Mathematics,* vol. 47, pp. 121–123, 1983.

[72] F. Sala and L. Dolecek, “Constrained permutations for rank modulation,” submitted to *IEEE Trans. on Information Theory*, 2013.

[73] F. Sala and L. Dolecek, “Constrained rank modulation schemes,” *Proc. IEEE Information Theory Workshop (ITW)*, pp. 479–483, Sevilla, Spain, September 2013.

[74] F. Sala, R. Gabrys, and L. Dolecek, “Dynamic threshold schemes for multi-level non-volatile memories,” *IEEE Trans. on Communications*, vol. 61, pp. 2624–2634, July 2012.

[75] J. H. Schmerl, “Tiling space with notched cubes,” *Discrete Mathematics*, vol. 133, pp. 225–235, 1994.

[76] M. Schwartz, “Quasi-cross lattice tilings with applications to flash memory,” *IEEE Trans. on Information Theory,* 58, 2397–2405,2012.

[77] M.-Z. Shieh and S.-C. Tsai, “Decoding frequency permutation arrays under Chebychev distance,” *IEEE Trans. on Inform. Theory*, vol. 56, no. 11, pp. 5730–5737, November 2010.

[78] M.-Z. Shieh and S.-C. Tsai, “Computing the ball size of frequency permutations under Chebychev distance,” *Proc. IEEE International Symposium on Inform. Theory*, pp. 2100–2104, St. Petersburg, Russia, August 2011.

[79] A. Shpilka, “New constructions of WOM codes using the Wozencraft ensemble,” *arxiv.org/abs/1110.6590.*

[80] D. Slepian, “Permutation modulation,” *Proc. of the IEEE*, vol. 53, no. 3, pp. 228–236, 1965.

[81] J. Spencer, “Maximal consistent families of triples,” *Journal of Combinatorial Theory.,* 5, pp. 1–8, 1986.

[82] S. Stein, “Factoring by subsets,” *Pacific J. Math.,* vol. 22, pp. 523–541, 1967.

[83] S. Stein, “A symmetric star body that tiles but not as a lattice,” *Proc. Amer. Math. Soc.,* 36, pp. 543-548, 1972.

[84] S. Stein, *Algebraic tiling*, Amer. Math. Mon., vol. 81, pp. 445–462, 1967.

[85] S. Stein, "Packing of $\mathbb{R}^n$ by certain error spheres," *IEEE Trans. on Information Theory,* vol. IT-30, pp. 356–363, 1984.

[86] S. Stein, "Tiling, packing, and covering by clusters", *Rocky Mountain J. Math.*, vol. 16. pp. 277–321, 1986.

[87] S. Stein, "The notched cube tiles $\mathbf{R}^n$", *Discrete Mathematics*, vol. 80. pp. 335–337, 1990.

[88] S. Stein and S. Szabó, *Algebra and Tiling*, The Mathematical Association of America, 1994.

[89] S. Szabó, "On mosaics consisting of multidimensional crosses," *Acta Math. Acad. Sci. Hung.,* 39, pp. 191–203, 1981.

[90] S. Szabó, *Rational tilings by n-dimensional crosses, I*, Proc. Amer. Math. Soc., 87 (1983), pp. 213–222.

[91] S. Szabó, "Rational tilings by n-dimensional crosses, II," *Proc. Amer. Math. Soc.,* 93, pp. 569–577, 1957.

[92] I. Tamo and M. Schwartz, "Correcting limited-magnitude errors in the rank-modulation scheme," *IEEE Trans. on Informa. Theory*, vol. 56, pp. 2551–2560, June 2010.

[93] I. Tamo and M. Schwartz, "Optimal permutation anticodes with the infinity norm via permanents of $(0, 1)$-marices," *J. Comb. Theory*, Ser. A, vol. 118, pp. 1761–1774, August 2011.

[94] I. Tamo and M. Schwartz, "On the labeling problem of permutation group codes under the infinity metric," *IEEE Trans. on Inform. Theory*, vol. 58, no. 10 pp. 6595–6604, October 2012.

[95] W. Ulrich, "Non-binary error correction codes," *The Bell System Technological Journal,* 36 , pp. 1341–1387, 1957.

[96] R. R. Varshamov,, "On some specifics error-correcting linear codes", *Rep. Acad. Sci. USSR*, vol. 157. pp. 546–548, 1964.

[97] R. R. Varshamov,, "On the theory of asymmetric codes", *Rep. Acad. Sci. USSR*, vol. 164. pp. 757–760, 1965.

[98] R. R. Varshamov and G. M. Tenengolts, “A code for correcting a single asymmetric error,” *Autom. Telemkh.*, vol. 26, pp. 288–292, 1965.

[99] L. Wang, M. Qin, E. Yaakobi, Y.-H. Kim, and P. H. Siegel, “WOM with retained messages”, in Proc. *IEEE Inter. Symp. on Inform. Theory,* Boston, pp. 1396–1400, 2012.

[100] P. M. Weichsel, “Dominating sets in n-cubes,” *J. of Graph Theory,* 18, pp. 479–489, 1994.

[101] J. K. Wolf, A. D. Wyner, J. Ziv, and J. Korner, “Coding for write-once memory”, *AT&T Bell Labs. tech. J.*, vol. 63, pp. 1089–1112, 1984.

[102] E. Yaakobi, personal communication, 2012.

[103] E. Yaakobi and A. Shpilka, “High sum-rate three-write and nonbinary WOM codes”, in Proc. *IEEE Inter. Symp. on Inform. Theory,* Boston, pp. 1391–1395, 2012.

[104] E. Yaakobi, P. H. Siegel, A. Vardy, and J. K. Wolf, “On codes that correct asymmetric errors with graded magnitude distribution”, in Proc. *IEEE Inter. Symp. on Inform. Theory,* Saint Petersburg, pp. 1021–1025, 2011.

[105] E. Yaakobi, P. H. Siegel, A. Vardy, and J. K. Wolf, “Multiple error-correcting WOM-codes”, *IEEE Trans. Inform. Theory*, vol IT-58, pp. 2220–2230, 2012.

[106] A. van Zuylen, J. Bieron, F. Schalekamp, and G. Yu, “An upper bound on the number of circular transpositions to sort a permutation,” *arXiv:1402.4867v1*, February 2014.

[107] Z. Zemor and G. D. Cohen, “Error-correcting WOM-codes”, *IEEE Trans. Inform. Theory*, vol IT-37, pp. 730–734, 1991.

[108] H. Zhou, A. Jiang, and J. Bruck, “Systematic error-correction codes for rank modulation,” *Proc. IEEE International Symposium on Information Theory*, pp. 2978–2982, Cambridge, MA, July 2012.

[109] H. Zhou, M. Schwartz, A. Jiang, and J. Bruck, “Systematic error-correction codes for rank modulation,” *arxiv.org/abs/1310.6817.*

בעיות אלגבריות וגאומטריות עם
יישומים עבור זכרון בלתי נדיף

שרית בוזגלו

בעיות אלגבריות וגאומטריות עם
יישומים עבור זכרון בלתי נדיף

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת התואר
דוקטור לפילוסופיה

שרית בוזגלו

הוגש לסנט הטכניון – מכון טכנולוגי לישראל
סיוון ה'תשע"ד חיפה יוני 20014

המחקר נעשה בהנחיית פרופסור טובי עציון ופרופסור איתן יעקובי בפקולטה למדעי המחשב.

ברצוני להודות למנחה שלי, פרופסור טובי עציון, על ההדרכה והתמיכה הרבה במשך תקופת השלמותי לתואר דוקטור. טובי לימד אותי כיצד לגשת לבעיה מחקרית מזוויות שונות ולמצות את מלוא הפוטנציאל של המחקר. עוד למדתי ממנו שהסבלנות משלתמת ולעולם לא להרים ידיים.

ברצוני להודות גם למנחה הנוסף שלי, פרופסור איתן יעקובי, שהדריך אותי במשך השנתיים האחרונות להשתלמותי לתואר דוקטור. איתן הציג בפניי בעיות ושיטות חדשות ותמיד היה מוכן לעשות מעל ומעבר על מנת לעזור לי בכל נושא אקדמי.

לסיום, אני רוצה להודות למשפחתי שתמיד האמינה בי ולהקדיש את עבודה מחקר זו לבני יהלי, האושר והגאווה בחיי, ולאבא שלי, שאני מקווה לגרום לו גאווה.

אני מודה לטכניון ולמשפחת ג'ייקובס על התמיכה הכספית הנדיבה בהשתלמותי.

תקציר

זכרון פלאש הוא אחד הזכרונות הבלתי נדיפים הנפוצים ביותר בימינו. חשיבות המחקר בנושא זכרון פלאש גברה בשנים האחרונות עקב ריבוי הישומים של זכרונות אלה. זכרון פלאש מורכב מקבוצות גדולות של תאים הנקראות בלוקים. כתיבת מידע לזכרון פלאש נעשית על ידי הזרקת מטען חשמלי לתוך תא, כאשר כמות המטען החשמלי בתא מתאימה לאחד מ q מצבים המייצגים $\log_2 q$ סיביות. מחיקה של מידע מתא בודד היא פעולה מסובכת הדורשת את מחיקת כל הבלוק אליו התא שייך ותכנות מחדש של הבלוק. כיוון שפעולה זו יקרה בזמן ובאנרגיה, היא נעשית באופן מרוכז, עבור מספר רב של תאים בבלוק, ואינה נעשית עבור תא אחד בודד. על מנת למנוע מצב של תכנות עודף הגורם לשגיאות, תכנות התאים נעשה באופן זהיר במספר שלבים, כאשר בכל שלב מתבצעת מדידת הזרם החשמלי בתאים והזרקה נוספת של כמות מטען חשמלי מזערית, במידת הצורך. מכאן, שתכנות התאים בזכרון פלאש היא פעולה איטית יחסית למערכות אחסון אחרות. חוסר הסימטריה בין פעולת הכתיבה לבין פעולת המחיקה של תאים בזכרון פלאש גורמת למקורות שגיאות מרכזיים לשנות את מצב התא בכיוון אחד עיקרי. בנוסף, רוב השגיאות הן בעלות עוצמה קטנה, כלומר, גורמות לשינוי קטן במצב התא.

עבודת מחקר זו עוסקת בשתי סכימות קידוד לזכרונות פלאש: קידוד לשגיאות אסימטריות בעוצמה מוגבלת (asymmetric limited magnitude error model) וסכימת אפנון הדרגה (rank modulation scheme).

מודל השגיאה האסימטרית בעוצמה מוגבלת פונה לאסימריה המובנית בשגיאות נפוצות בזכרון פלאש בעל תא רב מצבי (multi level cell flash memory). שגיאות במודל זה הן בכיוון אחד ועוצמתן מוגבלת על ידי חסם כלשהו. משמעות הדבר היא שתא במצב i יכול לעלות כתוצאה משגיאה למצב j, כך ש $i < j \le q-1$ וגם $j - i \le \ell \le q-1$, כאשר ℓ הוא החסם על עוצמת השגיאה. צופנים לתיקון שגיאות במודל זה הוצגו ב [2] ונעשה בהם שימוש לראשונה עבור זכרונות בלתי נדיפים ב [9, 10] . מספר מאמרים נוספים התייחסו לצופנים אלו, למשל, [22, 23, 48, 104].

סכימת אפנון השגיאה נועדה לשיפור יעילות הכתיבה לזכרון פלאש [43]. צופנים במודל זה הם תתי קבוצות של S_n, קבוצת כל התמורות על n איברים, כאשר כל תמורה מייצגת דירוג של n תאים בזכרון לפי הסדר העולה של מצביהם. צופני תמורות נלמדו בהקשר זה בעיקר תוך שימוש במטריקת האינסוף ובמטריקת ה τ של קנדל (Kendall's τ-metric).

מרחק ה τ של קנדל בין שתי תמורות $\sigma, \pi \in S_n$ הוא המספר הקטן ביותר של חילופי מקומות בין שני איברים סמוכים בתמורה, הנדרשים כדי לשנות את σ ל π [46]. צופני תמורות עם מרחק מינימלי d במטריקה זו יכולים לתקן עד כ $\left\lfloor \frac{d-1}{2} \right\rfloor$ שגיאות הנגרמות מדליפת מטען ושגיאות הנגרמות על ידי קריאה מהזכרון. צופני תמורות לתיקון שגיאות במטריקה זו נלמדו ב [5, 61, 44]. ב [108, 109] הוצג המושג של צופנים סיסטמים עבור תמורות וב [73] נלמדו צופני תמורות תחת אילוצים.

עבודת תזה זו מורכבת משני חלקים. החלק הראשון עוסק בריצוף המרחב האוקלידי ה n־מימדי עם צורה מסוימת. ריצופים אלו נלמדים עבור שתי צורות, הקרוס ה n־מימדי עם אורך זרוע 0.5 ($(0.5, n)$-cross) והכסא ה n־מימדי (n-dimensional chair). ריצופים עם הכסא ה n־מימדי משרים צופנים לתיקון שגיאות אסימטריות בעוצמה מוגבלת. החלק השני מוקדש כולו לחקר צופני תמורות לתיקון שגיאות במטריקת ה τ של קנדל.

צופנים לתיקון שגיאות ואריזה וריצוף של המרחב האוקלידי ה n מימדי עם צורה מסוימת הם נושאים קשורים ומשום כך, אריזה וריצוף הם שני נושאים שהיוו מוקד עניין רב בקרב חוקרים בתורת הצפינה. ריצוף של המרחב האוקלידי ה n מימדי עם צורה מסוימת, $\mathcal{S}$, הוא חלוקה של המרחב לעותקים מוזזים של $\mathcal{S}$. הגדרות בסיסיות עבור המושגים אריזה וריצוף ודיון על הקשר בין מושגים אלה לבין צופנים לתיקון שגיאות ניתנים בפרק 1. שתי הצורות הנלמדות ביותר בהקשר של צופנים לתיקון שגיאות הן הסמיקרוס (semicross) והקרוס (cross). אריזה וריצוף עם הסמיקרוס והקרוס הוא נושא שנלמד רבות (ראה [86, 88] ואת רשימת המקורות במאמרים אלה). הסיבה לעניין הרב באריזה וריצוף עם צורות אלו היא שהם משרים צופנים לתיקון שגיאות במטריקה של המינג (Hamming), המהווים צופנים לתיקון שגיאות סימטריות [58] .

פרק 2 עוסק בריצופים עם ה $(0.5, n)$־קרוס. ה $(0.5, n)$־קרוס מורכב מקוביית יחידה n־מימדית, כאשר אל כל אחת מפאותיה ה $n-1$־מימדיות מחוברת חצי קוביית יחידה n מימדית. כיוון שנוח יותר לעבוד עם צורות המורכבות מקוביות יחידה n־מימדיות, מתבצע שינוי קנה המידה פי שניים לקבלת צורה חדשה המורכבת כולה מקוביות יחידה n־מימדיות. צורה זו מסומנת ב Υ_n. דוגמאות ל $(0.5, 3)$־קרוס ול Υ_3 מוצגות באיור 2.1. התוצאה המרכזית בפרק 2 היא שקיים ריצוף בשלמים של המרחב האוקלידי ה n מימדי עם Υ_n אם ורק אם $n = 2^t - 1$ או $n = 3^t - 1$, כאשר t הוא שלם חיובי.

בפרק 3 נלמדים ריצופים עם הכסא ה n־מימדי. כסא n־מימדי הוא תיבה n־מימדית אשר הוסרה מאחת מפינותיה תיבה n־ מימדית קטנה יותר (ראה איור 3.1). ריצופים עם הכסא ה n מימדי משרים צופנים היכולים לתקן עד $n-1$ שגיאות אסימטריות עם עוצמה מוגבלת. פרק זה דן בשקילות בין ריצופי שריג (lattice) לבין סדרות מפצלות מוכללות (generalized splitting sequences), מושג המכליל את הסדרות המפצלות שהוגדרו ב [82] ואת סדרות ה $B_h[\ell]$, שהוגדרו לצורך בנית צופנים לתיקון שגיאות אסימטריות מוגבלות בעוצמה ב [48]. בנוסף, הפרק כולל בניות של ריצופים עם הכסא ה n־מימדי, הן על ידי סדרות מפצלות מוכללות והן על ידי שריג, והוכחת אי קיום

ריצופים עבור פרמטרים מסוימים.

החלק השני של תזה זו מוקדש לצופני תמורות עם מטריקת ה τ של קנדל. בפרק 5 נלמדים המושגים צופנים מושלמים וצופנים מושלמים לפי קוטר עבור תמורות. צופנים מושלמים בתמורות עם מטריקת ה τ של קנדל הוזכרו בקצרה ב [108], שם הוכח שלא קיימים צופנים מושלמים לתיקון שגיאה אחת ב S_4. בפרק זה מוכח כי לא קיימים צופנים מושלמים לתיקון שגיאה אחת ב S_n, כאשר $n \geq 4$ הוא ראשוני או $4 \leq n \leq 10$. בנוסף, פרק זה דן במושג של צופנים מושלמים לפי קוטר ובוריאציות של מטריקת ה τ של קנדל.

פרק 6 עוסק בצופנים סיסטמטים לתיקון שגיאות בתמורות. כאמור, מושג זה הוצא ב [108, 109]. צופן סיסטמטי ב S_n הוא צופן המכיל $k!$ מילות צופן, כך שכל תמורה ב S_k היא תת תמורה (תת סדרה) של בדיוק מילת צופן אחת. בניה של צופנים סיסטמטים לתיקון שגיאות ניתנת בפרק זה. בניה זו משתמשת בפחות אותיות יתירות ביחס לבניות קודמות.

פרק 7 עוסק בצופני תמורות תחת אילוצים. ב [73, 72] נלמד אילוץ מסוים הנובע מתופעה בזכרון פלאש שבה תא במצב נמוך, הלכוד בין שני תאים במצבים גבוהים, עשוי לעבור למצב גבוה יותר עקב השפעת התאים השכנים שלו. בפרק זה נלמדים שני אילוצים נוספים, חלשים יותר, שנועדו למנוע תופעה זו. תחת האילוץ הראשון, מילת צופן $\sigma \in S_n$ מקיימת שלכל $1 \leq i \leq n-1$, $|\sigma(i) - \sigma(i+1)|$ חסום על ידי קבוע k. האילוץ השני הוא חלש יותר ודורש שלכל $2 \leq i \leq n-1$, $\sigma(i) - \sigma(i-1) < k$ או $\sigma(i+1) - \sigma(i) < k$. אילוץ זה תואם יותר לתופעה בפלאש אותה מעונינים למנוע. התוצאות בפרק זה כוללות חישוב קיבולת לצופנים עבור שני האילוצים ובנוסף חישוב קיבולת עבור צופנים מסוג זה אשר משלבים גם יכולת לתיקון שגיאות במטריקת הקנדל של τ.