HAMMING GEOMETRY

by

Douglas H. Wiedemann

Ph.D. Thesis

Mathematics

University of Waterloo

Waterloo, Ontario

1986

Re-typeset July, 2006

ABSTRACT

This thesis deals with the geometry of the n-th Cartesian powers of the complete graphs K(b). Emphasis is placed on the n-th power of K(2), the graph of the n-cube. We investigate sets of vertices which behave like the convex sets of Euclidean geometry. A geometric characterization is given for the solution sets of 2SAT problems (systems of Boolean disjunctions of two literals). As a result, an algorithm is obtained for solving 2SAT problems with a limited number of additional parity constraints. Furthermore, an algorithm is obtained for computing the fixed points of any contraction mapping of the graph of the n-cube to itself. The next chapter considers sets related to convexity in a more loose sense. For example, any convex set in real n-space meets some collection of closed orthants. Many properties are derived for the sets of vertices of the n-cube which represent these collections of orthants. The final chapter looks at decomposition and covering problems of the n-cube. For example, it is shown that the vertices of the n-cube cannot be partitioned into smaller cubes, no two of which are parallel. Furthermore, an algorithm is obtained for solving linear equations over GF(2) together with a single polynomial equation of higher degree. Finally, we discuss the problem of covering a Hamming sphere by affine subspaces.

HAMMING GEOMETRY

1. Introduction

1.1. What is Hamming Geometry?

There is a remarkable distance function which can be applied to any set of n-dimensional vectors. This is the *Hamming distance*, which is the number of coordinates in which the two vectors differ. If $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are any two vectors, the Hamming distance is $d(\mathbf{x}, \mathbf{y}) = |\{ i \mid x_i \neq y_i \}|$, where for a set S, we use $|S|$ to denote the cardinality of S.

The vectors involved might come from anywhere. There is no requirement that different coordinates use the same sets. In other words, the first coordinate of these vectors could contain apples and the second could contain oranges. To compute the Hamming distance, it is not necessary to compare apples to oranges, only to detect if two apples or two oranges are the same.

In most applications, this level of generality is not required. Usually, the vectors are taken from the Cartesian power of some finite set. If there are b, $1 < b < \infty$, elements in this set, we can relabel them as $\{0, 1, \ldots, b-1\} = K_b$. The Hamming distance on the set of vectors in K_b^n is exactly the same as the graphical distance between corresponding vertices in the n^{th} Cartesian power of the ‘‘complete’’ graph on b vertices. Therefore, K_b^n can also be thought of as a graph.

Hamming geometry arose in a paper by R.W. Hamming [1], [2], which described his famous error correcting codes. The use of Hamming distance in coding theory, for the case $b = 2$, is widely accepted. For signaling alphabets with more than two signals, the Hamming distance remains one of the most commonly studied distance functions, but there are other competitors. This is a reason why most of the interest in Hamming geometry is concerned with the case $b = 2$. The graph K_2^n is studied in its own right in graph theory, where it is usually referred to as the n-cube or $Q(n)$.

Although this thesis observes that occasionally theorems about K_2^n extend to K_b^n, $b \geq 3$, most questions about general K_b^n are left open. Given a result about K_2^n, there does not yet exist any easy way to determine the extension of the result to K_b^n. Most significant is that K_2^n is bipartite while K_b^n, $b \geq 3$, is not. Furthermore, any thorough understanding of Hamming geometry requires an understanding of K_2^n, because the ‘‘intervals’’ in K_b^m are isometric to K_2^n, for some n. In any set X with distance function d, we can make the following definition.

Definition. For $\mathbf{x}, \mathbf{y} \in X$, the *interval* from $\mathbf{x}$ to $\mathbf{y}$ is

$$I(\mathbf{x}, \mathbf{y}) = \{ \mathbf{z} \in X \mid d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y}) = d(\mathbf{x}, \mathbf{y}) \} .$$

In K_b^m,

$$I(\mathbf{x}, \mathbf{y}) = (\{x_1\} \cup \{y_1\}) \times \cdots \times (\{x_m\} \cup \{y_m\}) ,$$

which is essentially the same as $K_2^{d(\mathbf{x}, \mathbf{y})}$, since when $x_i = y_i$, the corresponding term in the Cartesian product is a singleton.

Hamming geometry got started with its application to error correcting codes, but this thesis will venture into other subjects. In many other areas of combinatorics, the set $\{0,1\}^n$ arises. Some of these are the theories of partial orders, designs, finite sets, switching functions and combinatorial optimization. Perhaps this thesis is most related to switching theory, since in the 1950’s investigators began to study various families of subsets of $\{0,1\}^n$, because the characteristic function of any subset of $\{0,1\}^n$ can be identified with a Boolean function. This thesis extends those ideas in several ways. In particular, Corollaries 2.3.7 and 4.5.3 show that fast algorithms exist for determining the consistency of certain systems of Boolean equations. Furthermore, Proposition 2.7.7 would possibly be of use in some optimization problems.

Chapter 2 is an investigation of an operation on K_2^n which involves ‘‘voting’’ on three points to produce another point. This is an extremely important operation having nontrivial connections between several concepts.

Chapter 3 investigates a peculiar nested sequence of families of subsets of K_2^n. This chapter is motivated by pure theory, but there are some strong connections to linear programming. In particular, in sections 3.4 and 3.5 the problem is raised of determining which collections of closed orthants of $\mathbf{R}^n$ can be intersected by the solution set of a system of linear inequalities.

Chapter 4 is not concerned with families of sets, but instead looks at some decomposition and covering problems in K_b^n. In particular, section 4.6 contains an idea which may be of use in algebraic coding theory.

Besides assuming some familiarity with finite fields and linear programming ideas, the reader is assumed to be familiar with some graph theory definitions and ideas, which can be found in the book by Bondy and Murty [3], for example. There are occasions where we place upper bounds on the computational complexity of algorithms. Our model for measuring computational work is the random access machine with "limited" word size [4,p.3]. At present, this is the most commonly used model for stating complexity results.

1.2. Properties of the Distance Function and Cylinders

The Hamming distance is a *metric* in that for all points $\mathbf{x}, \mathbf{y}, \mathbf{z}$,

i) $d(\mathbf{x}, \mathbf{y}) \geq 0$ with equality precisely when $\mathbf{x} = \mathbf{y}$.
ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.
iii) $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Hamming geometry, like Euclidean geometry, arises from a "norm" on a vector space. In the case of K_2^n, we may identify the points of K_2^n with the members of an n-dimensional vector space over $GF(2)$. To add two vectors in this vector space, we use the operation $\oplus$, coordinatewise addition modulo two. The *norm* or *weight* of a vector $\mathbf{x} \in K_2^n$ is the number of 1's it contains, denoted $|\mathbf{x}|$. The distance function derived from this norm is

$$d(\mathbf{x}, \mathbf{y}) = |\mathbf{x} \oplus \mathbf{y}| ,$$

the Hamming distance. For $b \geq 3$, the norm can again be taken to be the number of nonzero coordinates. The vectors can be considered to be a module over an arbitrary ring with b elements, and the derived distance, $d(\mathbf{x}, \mathbf{y}) = |\mathbf{x} - \mathbf{y}|$, is again the Hamming distance.

Given a set of vertices in a graph the *induced subgraph* is the graph with this set of vertices together with all adjacencies that appear between them in the original graph. The following sets are those subsets of K_b^n which induce graphs isomorphic to K_b^m, for some m.

Definition. A *cylinder* of K_b^n is any set of its points such that the set is a Cartesian product which is a member of $\{\{0\}, \{1\}, \ldots, \{b-1\}, *\}^n$, where $*$ denotes $\{0, 1, \ldots, b-1\}$. Also, the empty set is considered a cylinder.

To denote a nonempty cylinder, we use a vector (or word) in $\{0, 1, \ldots, b-1, *\}^n$. Thus, in K_2^4, $0{*}1{*}$ denotes a cylinder consisting of the four points 0010, 0011, 0110 and 0111. The *dimension* of the cylinder is the number of $*$'s. The *co-dimension* is n minus the dimension. The coordinate positions in which the $*$ appears will be called the *directions* of the cylinder.

Given any nonempty cylinder $C \subseteq K_b^n$, there is a *projection* map $\pi_C\colon K_b^n \to C$. For any point $\mathbf{x}$, $\pi_C(\mathbf{x})$ is the unique point in C which is closest to $\mathbf{x}$. In the example above, the projection of the point 1110 to the cylinder $0{*}1{*}$ is 0110. In general, every coordinate of the point which is not a direction of the cylinder is replaced by the corresponding coordinate of the cylinder.

In a sense, the distance function decomposes into distances within the cylinder and distance to the cylinder. More explicitly, the projection map satisfies the following equation,

$$d(\mathbf{a}, \mathbf{x}) = d(\mathbf{a}, \pi_C(\mathbf{x})) + d(\pi_C(\mathbf{x}), \mathbf{x}) ,$$

for any point $\mathbf{a}$ of C.

Two nonempty cylinders, C and D, are said to be *parallel* if the projection maps possess both the property that $\pi_C \pi_D = \pi_C$ and that $\pi_D \pi_C = \pi_D$, where compositions are performed right to left. More pragmatically, C and D are parallel if and only if they have the same dimension and the $*$'s appear in the same positions.

It is easy to verify that parallelism is an equivalence relation and that the cylinders parallel to a given nonempty cylinder partition the points of K_b^n.

The intersection of any two cylinders is a cylinder. To have this property is the main reason for including the empty set as a cylinder. Given any set of points the cylinder *generated* by these points is the intersection of all cylinders containing the set.

The definition of cylinders has an obvious weaker version.

Definition. A set $S \subseteq K_b^n$ is a *partial cylinder* if it can be written in the form

$$S = S^{(1)} \times S^{(2)} \times \cdots \times S^{(n)}$$

where each $S^{(i)}$ is some subset of K_b.

Trivially, cylinders and partial cylinders can be looked at as the solution sets of certain systems of constraints. The set of all $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ satisfying a system where each constraint is of the form $x_i \in C$, where i and $C \subseteq K_b$ are parameters of the constraint, forms a partial cylinder. The collection of cylinders is obtained by using constraints of the form $x_i = c$, where i and $c \in K_b$ are parameters of the constraint.

1.3. Isometries

An *isometry* of K_b^n, as with any other geometry, is a bijection of K_b^n to itself which preserves the distance function. The group of isometries of K_b^n is easy to describe. To perform an arbitrary isometry, first select a permutation on n objects and permute the coordinates of all points accordingly. Next, for each coordinate position, select a permutation on b objects and for all points apply this permutation to the value appearing in position i. There are $n!(b!)^n$ isometries obtained in this way, and these are all the isometries.

In the case $b = 2$ the isometry group is called the hyper-octahedral group. There has been much interest in classifying subsets of K_2^n, partly because the characteristic function of such a set corresponds to a unique n-variable Boolean function. Burnside-Polya techniques have been used to enumerate equivalence classes of Boolean functions under the hyper-octahedral symmetries [5], [6].

The symmetry group of K_2^n has some important subgroups. The collection of isometries with trivial coordinate permutation forms a subgroup of size 2^n, called the *translation* subgroup. For such an isometry we may form an n-vector $\mathbf{t}$ whose i^{th} coordinate is 1 if the isometry changes the value of that coordinate, and is 0 otherwise. The isometry takes a point $\mathbf{x}$ to $\mathbf{x} \oplus \mathbf{t}$. This subgroup of isometries is therefore isomorphic with the additive group of an n-dimensional vector space over $GF(2)$. The name "translation" is perhaps justified because the isometry acts by vector addition, only the trivial element has fixed points, and every element is moved a constant Hamming distance.

The isometries which only permute the n coordinates among themselves form a subgroup isomorphic with the symmetric group on n elements. This "permutation" group is not as special as the translation group because it is not normal in the group of all isometries (for $n > 1$). In fact, the translation group consists of all fixed point free isometries of order two, together with the identity map. The group of permutations cannot be identified in such a coordinate free fashion, but it is the set of isometries which fix the vector $\mathbf{0}$. The hyper-octahedral group is the semidirect product of the translation group by the permutation group.

The hyper-octahedral group has a nontrivial element which commutes with all other elements. This is the translation which changes all coordinates. This will be called the *antipodal* map. For each $\mathbf{x}$, it produces the antipodal point $\bar{\mathbf{x}} = \mathbf{x} \oplus (1, 1, \ldots, 1)$. The point $\bar{\mathbf{x}}$ is the unique point at greatest distance from $\mathbf{x}$. Also, $I(\mathbf{x}, \bar{\mathbf{x}}) = K_2^n$.

Permutations and translations are both $GF(2)$-affine maps from K_2^n to itself. That is, if Φ is an isometry, it has the property that $\Phi(\mathbf{x} \oplus \mathbf{y} \oplus \mathbf{z}) = \Phi(\mathbf{x}) \oplus \Phi(\mathbf{y}) \oplus \Phi(\mathbf{z})$, for all $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$. Thus, the isometry group fits inside the group of all affine bijections from K_2^n to itself. The affine group has been useful in design and coding theory, but the isometry group will be the most important one for this thesis.

In a sense popularized by Felix Klein, geometry is the study of those features of a metric space which are invariant under isometries. This includes the problem of determining when two sets in the space are equivalent under isometry. Suppose we have two finite sets $X = \{\mathbf{x}^1, \ldots, \mathbf{x}^m\}$ and $Y = \{\mathbf{y}^1, \ldots, \mathbf{y}^m\}$, and that $d(\mathbf{x}^i, \mathbf{x}^j) = d(\mathbf{y}^i, \mathbf{y}^j)$ for all $1 \le i \le j \le m$. Is it necessarily true that there is an isometry Φ such that $\Phi(\mathbf{x}^i) = \mathbf{y}^i$, for all i? In Euclidean space of any dimension the answer is "Yes" (W.J. Gilbert has provided the author with a proof, of this based on Gram-Schmidt.), but in every Hamming geometry of sufficiently large dimension the answer is "No". In K_2^4 let $\mathbf{x}^1 = 0000$, $\mathbf{x}^2 = 0011$, $\mathbf{x}^3 = 0110$ and $\mathbf{x}^4 = 0101$. Also, let $\mathbf{y}^1 = \mathbf{x}^1$, $\mathbf{y}^2 = \mathbf{x}^2$ and $\mathbf{y}^3 = \mathbf{x}^3$, but let $\mathbf{y}^4 = 1010$. Note $d(\mathbf{x}^i, \mathbf{x}^j) = d(\mathbf{y}^i, \mathbf{y}^j)$, for all i and j. Suppose Φ is an isometry taking each $\mathbf{x}^i$ to $\mathbf{y}^i$. Since Φ fixes 0000, Φ must be a coordinate permutation. Since Φ fixes 0011, the coordinate permutation fixes the index sets $\{1, 2\}$ and $\{3, 4\}$. Since Φ fixes 0110, the permutation fixes $\{1, 4\}$ and $\{2, 3\}$. The only possibility consistent with all these constraints is the identity permutation, but $\Phi(\mathbf{x}^4) \ne \mathbf{y}^4$, so Φ cannot exist!

Definition. $S \subseteq K_b^n$ is *rigid* if whenever there is $T \subseteq K_b^n$ and bijection $\Theta: S \to T$ such that $d(\mathbf{s}^1, \mathbf{s}^2) = d(\Theta(\mathbf{s}^1), \Theta(\mathbf{s}^2))$, for all $\mathbf{s}^1, \mathbf{s}^2 \in S$, then Θ is the restriction to S of some isometry of K_b^n.

We have not been able to determine which subsets of K_b^n are rigid, but the next theorem gives a large collection of such sets. A complete classification of rigid sets might allow a faster version of the algorithm in section 2.7, but it is also of theoretical interest.

A set $S \subseteq K_b^n$ is called *connected* if the subgraph it induces in K_b^n is connected, i.e., has at most one connected component.

Theorem 1.3.1. Connected subsets of K_b^n are rigid.

Proof. Our methods are similar to those mentioned in a paper by Graham [7]. The following proof is rather intricate, so the reader may want to temporarily bypass it.

Let $\{\mathbf{u}, \mathbf{v}\}$ and $\{\mathbf{x}, \mathbf{y}\}$ determine two arbitrary edges of K_b^n. Associated with these sets is the 4-tuple of distances, $(d(\mathbf{u}, \mathbf{x}), d(\mathbf{u}, \mathbf{y}), d(\mathbf{v}, \mathbf{x}), d(\mathbf{v}, \mathbf{y}))$. If necessary, interchange $\mathbf{u}$ with $\mathbf{v}$ and possibly $\mathbf{x}$ with $\mathbf{y}$, so that $d(\mathbf{u}, \mathbf{x})$ is the minimal element of the 4-tuple. We will now list all possible cases for this 4-tuple. Let i be the single coordinate position such that $u_i \ne v_i$, and let j be the position such that $x_j \ne y_j$. The important relationships are the equalities amongst the values u_i, v_i, x_i, y_i and the equalities amongst the values u_j, v_j, x_j, y_j. If $i = j$, then $u_i \ne v_i$, $x_i \ne y_i$, and if any of the values u_i, v_i, x_i, y_i are equal, $u_i = x_i$, and in addition $v_i = y_i$ may or may not hold. If $i \ne j$, we have $u_i \ne v_i$, $x_i = y_i$ and $u_j = v_j$, $x_j \ne y_j$. If there is any additional equality amongst the i^{th} coordinates, it must be that $u_i = x_i$, and if there are any additional equalities amongst the j^{th} coordinates, it must be that $u_j = x_j$. The form of the 4-tuple is listed below, for all cases.

Case 1)	$i = j$	$u_i \ne x_i$	(d, d, d, d)
Case 2)	$i = j$	$u_i = x_i, v_i \ne y_i$	$(d, d+1, d+1, d+1)$
Case 3)	$i = j$	$u_i = x_i, v_i = y_i$	$(d, d+1, d+1, d)$
Case 4)	$i \ne j$	$u_i \ne x_i, u_j \ne x_j$	(d, d, d, d)
Case 5)	$i \ne j$	$u_i \ne x_i, u_j = x_j$	$(d, d+1, d, d+1)$
Case 6)	$i \ne j$	$u_i = x_i, u_j \ne x_j$	$(d, d, d+1, d+1)$
Case 7)	$i \ne j$	$u_i = x_i, u_j = x_j$	$(d, d+1, d+1, d+2)$

Unfortunately, case 4) is indistinguishable from case 1), so it cannot always be determined whether $i = j$ from the Hamming distances between $\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}$.

However, let $S \subseteq K_b^n$ be connected, so there is a walk, $\mathbf{s}^1, \mathbf{s}^2, \ldots, \mathbf{s}^m$ in S, covering all points of S, possibly with repetition. We will show how assign coordinates $\Phi(\mathbf{s}^k)$ to the $\mathbf{s}^k$ by a procedure that depends only on $d(\mathbf{s}^p, \mathbf{s}^q)$, $1 \le p < q \le m$, and such that Φ is the restriction of an isometry of K_b^n.

Begin by setting $\Phi(\mathbf{s}^1) = \mathbf{0}$. Suppose $\Phi(\mathbf{s}^1), \ldots, \Phi(\mathbf{s}^l)$ have been determined, but that $\Phi(\mathbf{s}^{l+1})$ has not yet been determined. Let the *direction* of an edge of K_b^n be the coordinate position where the two endpoints are different. The first step in determining $\Phi(\mathbf{s}^{l+1})$ is to find out if the direction of the edge $\{\mathbf{s}^l, \mathbf{s}^{l+1}\}$ equals the direction of some $\{\mathbf{s}^k, \mathbf{s}^{k+1}\}$, $k < l$. If this is the case, choose k, $k < l$, maximal with this property. Then if i is the direction of $\{\mathbf{s}^l, \mathbf{s}^{l+1}\}$, $s_i^{k+1} = s_i^l$, because there are no changes in coordinate i between $\mathbf{s}^{k+1}$ and $\mathbf{s}^l$. Looking at the distances between the points $\mathbf{s}^k, \mathbf{s}^{k+1}, \mathbf{s}^l, \mathbf{s}^{l+1}$ in the above table, cases 2) and 3) are the only possibilities and the 4-tuple of distances in these cases do not appear anywhere else in the table. Thus, whether $\{\mathbf{s}^l, \mathbf{s}^{l+1}\}$ is a new direction can be determined from the distances $d(\mathbf{s}^p, \mathbf{s}^q)$ alone.

Assume it has been determined that $\{\mathbf{s}^l, \mathbf{s}^{l+1}\}$ is a new direction. If $\{\mathbf{s}^l, \mathbf{s}^{l+1}\}$ is the r^{th} new direction, form $\Phi(\mathbf{s}^{l+1})$ from $\Phi(\mathbf{s}^l)$ by putting a 1 in position r. The r^{th} coordinate of $\Phi(\mathbf{s}^p)$, $1 \le p \le l$, is 0, because no previous changes have been made in this direction.

Assume that it has been determined that $\{\mathbf{s}^l, \mathbf{s}^{l+1}\}$ is a direction that has previously occurred. It must now be determined if s_i^{l+1} is a new value for coordinate i. If $s_i^q = s_i^{l+1}$, for some $1 \le q < l$, then $d(\mathbf{s}^q, \mathbf{s}^{l+1}) < d(\mathbf{s}^q, \mathbf{s}^l)$, otherwise, $d(\mathbf{s}^q, \mathbf{s}^{l+1}) \ge d(\mathbf{s}^q, \mathbf{s}^l)$. Thus, from the distances alone, it can be determined if $\mathbf{s}_i^{l+1}$ is a value which has previously occurred in coordinate i. Let r be such that $\Phi(\mathbf{s}^k)_r \ne \Phi(\mathbf{s}^{k+1})_r$. Assume the value is new, and suppose a distinct values have appeared in $\Phi(\mathbf{s}^1)_r, \ldots, \Phi(\mathbf{s}^l)_r$. Then, form $\Phi(\mathbf{s}^{l+1})$ from $\Phi(\mathbf{s}^l)$ by changing the value of coordinate r to a. On the other hand, if the value is not new, form $\Phi(\mathbf{s}^{l+1})$ from $\Phi(\mathbf{s}^l)$ by changing the value of coordinate r to $\Phi(\mathbf{s}^q)_r$, where q is the value found above.

If this process is run until $\Phi(\mathbf{s}^m)$ is determined, Φ has permuted coordinate positions to be in order of use, and the values in each coordinate position have been renamed to be in order of appearance. Hence, Φ is the restriction of an isometry to S. Now, if $\mathbf{t}^1, \ldots, \mathbf{t}^m$ is a walk through another set $T \subseteq K_b^n$, and $d(\mathbf{t}^p, \mathbf{t}^q) = d(\mathbf{s}^p, \mathbf{s}^q)$, for all $1 \le p \le q \le m$, the procedure applied to the $\mathbf{t}$-sequence produces $\Psi(\mathbf{t}^1), \ldots, \Psi(\mathbf{t}^m)$. Since the result of the procedure only depends on the distances, $\Phi(\mathbf{s}^k) = \Psi(\mathbf{t}^k)$, for all k. Thus, $\Theta = \Psi^{-1}\Phi$ is an isometry taking each $\mathbf{s}^k$ to $\mathbf{t}^k$, as required. ∷

Note: the procedure in the proof can be used to test a given square matrix of positive integers $[d_{p,q}]$, to determine if there exist points $\mathbf{s}^k \in K_b^n$, such that $d(\mathbf{s}^p, \mathbf{s}^q) = d_{p,q}$, providing that if all entries not equal to 1 are set to 0, the adjacency matrix of a connected graph results.

The action of isometries gives us the opportunity to define another type of subset of K_b^n. These are the sets which can be realized as the set of fixed points of some subgroup of isometries. Call these fixed-sets. Since we have a description of what a general isometry looks like, it is straightforward to work out the fixed point set for a single isometry. The fixed-sets are those sets that arise as intersections of fixed point sets of individual isometries.

In the case of K_2^n the fixed-sets are not quite the collection we desire. In K_2^n, if $\mathbf{x}$ is in a fixed-set then so is $\bar{\mathbf{x}}$. We therefore expand the family of fixed-sets to a family defined below.

Definition. A *combinatorial* set is a subset of K_b^n which is either the empty set or the solution set of a system of any number of constraints, each of which is in one of the following two forms.
i) $x_i = \alpha(x_j)$, α any permutation on K_b.
ii) $x_i \in K'$, K' any subset of K_b.

The indices i and j, along with α and K' are parameters of the constraint. The system of constraints can be empty, in which case the solution set is all of K_b^n. Allowing equations of only type i) gives the fixed-sets. Allowing constraints of only type ii) we obtain a the partial cylinders. The only connected combinatorial sets are those which are also partial cylinders. Basically, this is because any essential constraint of type i) prevents changing only x_i inside the solution set. Furthermore, every connected component of a combinatorial set is a partial cylinder.

1.4. Convexity

Much of this thesis will deal with sets in K_2^n which share some properties with convex subsets of $\mathbf{R}^n$. There are many properties of convex sets $\mathbf{R}^n$, leading to many different versions of convexity in other geometries. Perhaps twenty properties relating to convexity were explored in work on this thesis. Occasionally two of these versions of convexity coincide in K_2^n, leading to identical families of sets. Aside from this, in several other cases, one version includes another. The entire chapter on hereditary families explores a chain of increasingly restrictive properties relating to convexity.

Probably every researcher who has thought about abstract convexity has arrived at a definition equivalent to the following, which may be applied in any geometry.

Definition. A set S is *strongly convex* if for every $\mathbf{x}, \mathbf{y} \in S$, the interval $I(\mathbf{x}, \mathbf{y})$ is a subset of S.

It is clear from the definition that the intersection of strongly convex sets is strongly convex.

Proposition 1.4.1. The strongly convex sets of K_b^n are the partial cylinders.

Proof. Note that

$$I(\mathbf{x}, \mathbf{y}) = (\{x_1\} \cup \{y_1\}) \times \cdots \times (\{x_n\} \cup \{y_n\})$$

is a partial cylinder and in fact, is the intersection of all partial cylinders containing $\mathbf{x}$ and $\mathbf{y}$. It follows that any partial cylinder is strongly convex.

Suppose S is strongly convex, and let $S_i \subseteq K_b$ be the set of values which appear in the i^{th} coordinate position in the elements of S. Let $P = S_1 \times \cdots \times S_n$, a partial cylinder. It is clear that $S \subseteq P$. Suppose $\mathbf{z} \in P \backslash S$. Let $\mathbf{x}$ be a point in S such that $d(\mathbf{x}, \mathbf{z})$ is minimal. There must be an i such that $x_i \neq z_i$. By construction of P, there is an element $\mathbf{y}$ of S such that $y_i = z_i$. Now $I(\mathbf{x}, \mathbf{y})$ contains the point $\hat{\mathbf{x}} = (x_1, \ldots, x_{i-1}, z_i, x_{i+1}, \ldots, x_n)$ and $d(\hat{\mathbf{x}}, \mathbf{z}) < d(\mathbf{x}, \mathbf{z})$, a contradiction because $I(\mathbf{x}, \mathbf{y}) \subseteq S$. ∎

Note that since intervals are partial cylinders, Hamming geometry has the nice feature that intervals are strongly convex. In K_2^n, cylinders, partial cylinders, intervals and strongly convex sets are all the same thing, except the empty set is not considered to be an interval. In K_2^n these sets, including the empty set, will be called *cubes*. A cube which is a subset of some set under discussion will be referred to as a *subcube* of that set.

Even though strongly convex sets in K_b^n may seem trivial to recognize, it is useful to have a criterion which only looks at the set locally. Consider the following condition.

No3) If $\mathbf{u}, \mathbf{v} \in S$ and $d(\mathbf{u}, \mathbf{v}) = 2$, then $|S \cap I(\mathbf{u}, \mathbf{v})| \neq 3$.

If S is connected and satisfies No3), then S is strongly convex. We will prove this only for the case $b = 2$, because that is our main area of interest, however, it is true for all values of b.

Lemma 1.4.2. If $S \subseteq K_2^n$, satisfies No3), $I(\mathbf{x}, \mathbf{y}) \subseteq S$, $\mathbf{z} \in S$ and $d(\mathbf{y}, \mathbf{z}) = 1$, then $I(\mathbf{x}, \mathbf{z}) \subseteq S$.

Proof. Since intervals are strongly convex, the conclusion is automatic if $\mathbf{z} \in I(\mathbf{x}, \mathbf{y})$, so we can assume $\mathbf{z} \notin I(\mathbf{x}, \mathbf{y})$.

Now we use mathematical induction on $d(\mathbf{x}, \mathbf{y})$. If $d(\mathbf{x}, \mathbf{y}) = 0$, then under the hypotheses of the lemma, $I(\mathbf{x}, \mathbf{z}) = \{\mathbf{x}, \mathbf{z}\} \subseteq S$, so the lemma holds when $d(\mathbf{x}, \mathbf{y}) = 0$.

Assume for some $k \geq 1$, the lemma is true whenever $d(\mathbf{x}, \mathbf{y}) < k$. Let S be a set containing $I(\mathbf{x}, \mathbf{y})$ and $\mathbf{z}$, $d(\mathbf{x}, \mathbf{y}) = k$, $d(\mathbf{y}, \mathbf{z}) = 1$, $\mathbf{z} \notin I(\mathbf{x}, \mathbf{y})$ and assume S satisfies No3). Since all these conditions are invariant under isometries of K_2^n, we assume $\mathbf{x} = \mathbf{0}$, $\mathbf{y} = \mathbf{e}^1 \oplus \cdots \oplus \mathbf{e}^k$ and $\mathbf{z} = \mathbf{y} \oplus \mathbf{e}^{k+1}$, where $\mathbf{e}^i$ is the unit vector with a single 1 in position i.

Note $I(\mathbf{e}^i, \mathbf{y}) \subseteq I(\mathbf{0}, \mathbf{y})$, for $1 \leq i \leq k$. The inductive hypothesis applies to give that $I(\mathbf{e}^i, \mathbf{z}) \subseteq S$. The only points of $I(\mathbf{0}, \mathbf{z})$ not in any of these intervals are $\mathbf{0}$ and $\mathbf{e}^{k+1}$. But, $\mathbf{0} = \mathbf{x} \in S$, and

$$I(\mathbf{0}, \mathbf{e}^1 \oplus \mathbf{e}^{k+1}) = \{\mathbf{0}, \mathbf{e}^1, \mathbf{e}^{k+1}, \mathbf{e}^1 \oplus \mathbf{e}^{k+1}\}$$

meets S in $\mathbf{0}$, $\mathbf{e}^1$ and $\mathbf{e}^1 \oplus \mathbf{e}^{k+1}$, so by No3), S must also contain $\mathbf{e}^{k+1}$. Thus, all of $I(\mathbf{0}, \mathbf{z})$ is in S. ∎

Proposition 1.4.3. If $S \subseteq K_2^n$ is connected and satisfies No3), then S is strongly convex.

Proof. It must be shown that for each $\mathbf{x}, \mathbf{y} \in S$, $I(\mathbf{x}, \mathbf{y}) \subseteq S$. Since S is connected there is a path

$\mathbf{x}^0 = \mathbf{z}^0, \mathbf{z}^1, \ldots, \mathbf{z}^t = \mathbf{y}$, with $d(\mathbf{z}^i, \mathbf{z}^{i+1}) = 1$ and $\mathbf{z}^i \in S$, for all $0 \le i < t$. Now clearly $I(\mathbf{z}^0, \mathbf{z}^0) \subseteq S$ and by the lemma $I(\mathbf{z}^0, \mathbf{z}^1) \subseteq S$. Repeating the application of the lemma, $I(\mathbf{z}^0, \mathbf{z}^2) \subseteq S$, and, eventually, $I(\mathbf{z}^0, \mathbf{z}^t) \subseteq S$. ∎

Of course, in Euclidean n-space the strongly convex sets are the usual convex sets. The following is another definition which gives the same sets when applied to Euclidean space.

Definition. A set S is *weakly convex* if its intersection with every strongly convex set is connected.

Since the intersection of two strongly convex sets is strongly convex and strongly convex sets are connected (at least in any reasonable geometry), strongly convex sets are weakly convex. Another consequence of the fact that two strongly convex sets have a strongly convex intersection is that the intersection of a strongly convex set with a weakly convex set is weakly convex. Furthermore, weakly convex sets are connected, because the set of all points is strongly convex. It is by no means true in K_b^n that the intersection of two weakly convex sets is weakly convex.

Yet another definition of convexity which gives convex sets in Euclidean space when applied to topologically closed sets is the following.

Definition. A set S is *isometric* if it is connected and the induced distances in S are identical to those in the entire space.

In other words, a set S is isometric if for every $\mathbf{x}, \mathbf{y} \in S$ at least one of the shortest paths from $\mathbf{x}$ to $\mathbf{y}$ has all its vertices in S.

Proposition 1.4.4. $S \subseteq K_b^n$ is isometric if and only if it is weakly convex.

Proof. Let $S \subseteq K_b^n$ be isometric. Let P be any strongly convex set and $\mathbf{x}$ and $\mathbf{y}$ two points in $S \cap P$. There is a path of length $d(\mathbf{x}, \mathbf{y})$ in S from $\mathbf{x}$ to $\mathbf{y}$. This path lies in $I(\mathbf{x}, \mathbf{y})$ since the interval contains all shortest paths. By strong convexity $I(\mathbf{x}, \mathbf{y}) \subseteq P$. Thus, the path is in $S \cap P$, so $\mathbf{x}$ and $\mathbf{y}$ are always in the same component of $S \cap P$, so $S \cap P$ is connected. Hence, S is weakly convex.

Now let $S \subseteq K_b^n$ be any weakly convex set. For any $\mathbf{x}$ and $\mathbf{y}$ in S, we show by induction on $d(\mathbf{x}, \mathbf{y})$ that $\mathbf{x}$ and $\mathbf{y}$ are connected in S by a path of length $d(\mathbf{x}, \mathbf{y})$. This is clearly true when $d(\mathbf{x}, \mathbf{y}) \le 1$. Now assume this is true whenever $d(\mathbf{x}, \mathbf{y}) < k$ for some $k \ge 2$ and suppose $\mathbf{x}, \mathbf{y} \in S$ and $d(\mathbf{x}, \mathbf{y}) = k$. Since $S \cap I(\mathbf{x}, \mathbf{y})$ is connected, there is a point $\mathbf{z} \in S \cap I(\mathbf{x}, \mathbf{y})$ which is adjacent to $\mathbf{x}$. By definition of intervals, $d(\mathbf{z}, \mathbf{y}) = k - 1$. By the induction hypothesis, there is a path of length $k - 1$ from $\mathbf{z}$ to $\mathbf{y}$ in S. By attaching $\mathbf{x}$ at the beginning of this path, we have the required path of length k from $\mathbf{x}$ to $\mathbf{y}$ in S. ∎

Proposition 1.4.5. For any fixed b, there is a test requiring $O(nm^2)$ operations which determines if a nonempty m-element subset of K_b^n is isometric.

Proof. Let $S \subseteq K_b^n$ be an m-element set given explicitly as a list of m vectors, $m \ge 1$, each with n components. To be isometric it must be true that for each $\mathbf{x}, \mathbf{y} \in S$ with $d(\mathbf{x}, \mathbf{y}) \ge 2$, there is a point in $S \cap I(\mathbf{x}, \mathbf{y})$ at unit distance from $\mathbf{x}$. Furthermore, if this is true for all $\mathbf{x}$ and $\mathbf{y}$ it is easy to show that S is isometric, as in the last half of the proof of Proposition 4.

For each of the m points construct a list of its neighbors. The collection of lists can be constructed in $O(nm^2)$ operations by comparing all n coordinates of all $O(m^2)$ pairs of points. The list of neighbors of a point $\mathbf{x}$ should be stored as a 0-1 array of dimensions $n \times b$, such that the (i, z) entry is 1 in those cases where $\mathbf{x}$ has a neighbor with a z in coordinate i, $z \ne x_i$.

Now, for all ordered pairs of points $\mathbf{x}, \mathbf{y} \in S$ with $d(\mathbf{x}, \mathbf{y}) \ge 2$ make an $n \times b$ 0-1 array with positive entries at (i, y_i) such that $x_i \ne y_i$. Check that this array and the list of neighbors of $\mathbf{x}$ have a 1 in some common position. If this ever fails, S is not isometric. Otherwise, S is isometric. The total number of operations is $O(nm^2)$. ∎

Note: It appears that a more complex algorithm for testing isometric sets has $O(nm^2)$ operations uniformly for all $b \le nm$, but we will not go into this here.

In Euclidean space, projecting a convex set to an affine space results in a convex set. Similarly, in Hamming geometry, projecting a strongly convex set to a nonempty cylinder results in a strongly convex set. The original strongly convex set, $P = P_1 \times \cdots \times P_n$, can be assumed to be nonempty and the cylinder C is represented as an element $\mathbf{c}$ of $(K_b \cup \{*\})^n$. The projection of P to this cylinder is found by replacing P_i by $\{c_i\}$ whenever $c_i \neq *$. A similar argument shows that $\pi_C^{-1}(P)$ is strongly convex. This is a result that will be useful in the following proposition.

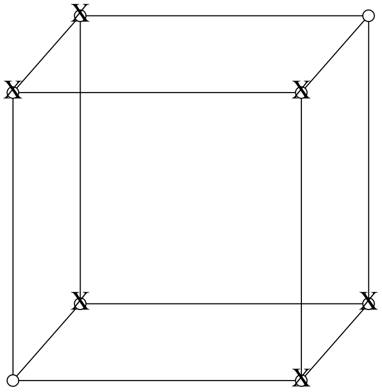
Proposition 1.4.6. In K_b^n, the projection of a weakly convex set to a nonempty cylinder is weakly convex.

Proof. Let S be a weakly convex set and let C be a nonempty cylinder. We must show that the intersection of $\pi_C(S)$ with any strongly convex set P is connected. Let $\hat{P} = \pi_C^{-1}(P)$, so $\pi_C(S) \cap P = \pi_C(S \cap \hat{P})$. Since S is weakly convex, $S \cap \hat{P}$ is connected. Note that if $d(\mathbf{u}, \mathbf{v}) = 1$, $d(\pi_C(\mathbf{u}), \pi_C(\mathbf{v})) \leq 1$. Thus, the projection of a connected set is connected because any sequence of points connecting $\mathbf{x}$ to $\mathbf{y}$ will project to a sequence of points connecting $\pi_C(\mathbf{x})$ to $\pi_C(\mathbf{y})$. Therefore, $\pi_C(S \cap \hat{P})$ is connected. ∎

Although we have kept this discussion general, the real interest has been for the case K_2^n, the n-cube. Various families in K_2^n related to convexity are discussed in this thesis, and the diagram at the end of section 3.5 summarizes these. Almost all the families lie between strong and weak convexity.

An important result of Djoković [8] gives an easy method to determine if a given graph is isomorphic to the induced subgraph of an isometric set in the n-cube. Isometric sets can be viewed as a type of bipartite graph - being identified with the graphs they induce in K_2^n. It appears that the larger problems of characterizing all subgraphs [9] or all induced subgraphs of n-cubes are still unsolved.

There are many interesting examples of isometric subsets of the n-cube, but of course they are not as numerous as rigid sets. The one pictured below is an isometric embedding of the 6-cycle. The points of the set are marked with an "X". This seems to serve as a good instructive example of such sets. If any one point is removed from this set, the resulting set will still be connected and therefore rigid, but it will not be isometric.



1.5. Spheres and Balls

The following definitions are standard in any geometry.

Definition. The *sphere* of defined radius r about the point $\mathbf{x}$ is the set of all points $\mathbf{y}$ such that $d(\mathbf{x}, \mathbf{y}) = r$.

Definition. The *ball* of defined radius r about the point $\mathbf{x}$ is the set of all points $\mathbf{y}$ such that $d(\mathbf{x}, \mathbf{y}) \leq r$.

We may take r to be negative, so the empty set is both a ball and a sphere. An important fact is that in K_2^n the complement of a ball is also a ball. In fact, the complement of the ball about $\mathbf{x}$ with defined radius r is the ball about $\bar{\mathbf{x}}$ with defined radius $n - r - 1$, when r is an integer.

Proposition 1.5.1. The intersection of two spheres in K_2^n is the Cartesian product of two spheres.

Proof. By isometry, we can assume the first sphere is centered at $\mathbf{0}$ and the second at a point $\mathbf{c}$, which written as a word is $0^j 1^{n-j}$, for some integer j. Now, any point $\mathbf{y}$ can be viewed as the concatenation of a j-vector $\dot{\mathbf{y}}$ with an $(n-j)$-vector $\ddot{\mathbf{y}}$. Let r and s be the defined radii of the first and second spheres, respectively. Then $\mathbf{y}$ is in the first sphere if and only if $|\dot{\mathbf{y}}| + |\ddot{\mathbf{y}}| = r$. It is in the second sphere whenever $|\dot{\mathbf{y}}| + (n-j) - |\ddot{\mathbf{y}}| = s$. A system equivalent to these two equations is,

$$|\dot{\mathbf{y}}| = \tfrac{1}{2}(r+s+j-n) \quad \text{and} \quad |\ddot{\mathbf{y}}| = \tfrac{1}{2}(r+n-s-j)\,.$$

Thus, the intersection of the two spheres is the Cartesian product of the sphere of radius $\frac{1}{2}(r+s+j-n)$ about $\mathbf{0}$ in K_2^j with the sphere of radius $\frac{1}{2}(r+n-s-j)$ about $\mathbf{0}$ in K_2^{n-j}. ∎

In Euclidean geometry, the intersection of two spheres can always be written as the intersection of a sphere with an affine space. In Euclidean geometry, consider the problem of determining if a collection of balls has nonempty intersection. There is a way to reformulate this problem as finding the minimum of a convex function. This may be accomplished to any degree of precision, using the ellipsoid algorithm, for example. In K_2^n, there is reason to believe that the problem might be more difficult.

Theorem 1.5.2. The problem of determining if a set of balls in K_2^n has nonempty intersection is NP complete.

Proof. We assume that the balls are specified as a list of vectors $\mathbf{c}^1, \ldots, \mathbf{c}^l$ and radii $r_1, \ldots, r_l$, which can be assumed to be integers. Of course, the problem is in NP because it is easy to verify that a point is in all l balls.

We show any instance of the NP complete problem 3SAT [10] with k variables can be transformed into an instance of the ball intersection problem with $n = 2k$. Several balls will depend only on k and not on the specific 3SAT problem. First, include the balls of radius k about $\mathbf{0}$ and about $\mathbf{1} = (1, \ldots, 1)$. The only points in both these balls are those having weight exactly k. Next, include the balls of radius k about each of the k points $(1,1,0,0,\ldots,0,0)$, $(0,0,1,1,0,0,\ldots,0,0)$,... and $(0,0,\ldots,0,0,1,1)$. The only points of weight k in all these balls are the points of the form

$$\mathbf{y} = (x_1, \bar{x}_1, x_2, \bar{x}_2, \ldots, x_k, \bar{x}_k)\,. \tag{*}$$

So far we have intersected $k+2$ balls. For each clause of the 3SAT system there will be one additional ball. For example, if $x_1 \vee \bar{x}_2 \vee x_3$ is one of the clauses, then include the ball of radius $k+1$ about the point $\mathbf{c} = (1,0,0,1,1,0,0,0,\ldots,0,0)$. Any point $\mathbf{y}$ in the form (*) will have $k-3$ 1's in the final $2(k-3)$ coordinates. To have at most 4 differences with the first 6 coordinates of $\mathbf{c}$, $\mathbf{y}$ must have $x_1 = 1$, $x_2 = 0$ or $x_3 = 1$, i.e., the clause must be satisfied. Likewise, there is a ball for every clause and (*) gives a correspondence between points in the intersection of all the balls and solutions $(x_1, \ldots, x_k)$ to the 3SAT problem. ∎

Our definition of weak convexity in the previous section was that the intersection with a cube always gave a connected set. The next proposition shows that in a sense the cubes can be replaced with balls.

Proposition 1.5.3. $S \subseteq K_2^n$ is isometric if and only if for each $\mathbf{s} \in S$, the intersection of S with each ball about $\mathbf{s}$ is connected.

Proof. Let S be isometric and let $\mathbf{s} \in S$ and let B be a ball about $\mathbf{s}$. Let $t \in S \cap B$, so B has defined radius at least $d(\mathbf{t}, \mathbf{s})$. Since S is isometric there is a path of length $d(\mathbf{t}, \mathbf{s})$ connecting $\mathbf{t}$ to $\mathbf{s}$ in S. Clearly, each point in this path must also lie in B. Thus, $\mathbf{t}$ and $\mathbf{s}$ are in the same component of $S \cap B$. Since this is true for every $\mathbf{t} \in S \cap B$, $S \cap B$ is connected.

Now assume $S \cap B$ is connected whenever B is a ball about a point of S. Let $\mathbf{s}, \mathbf{t}$ be arbitrary elements of S. It will be shown by induction on $d(\mathbf{s}, \mathbf{t})$ that there is a path of length $d(\mathbf{s}, \mathbf{t})$ connecting $\mathbf{s}$ to $\mathbf{t}$ in S. For $d(\mathbf{s}, \mathbf{t}) \le 1$, there is nothing to prove. Let $d(\mathbf{s}, \mathbf{t}) = k \ge 2$. Let B be the ball of radius k about $\mathbf{s}$. Since $S \cap B$ is connected there is a point $\mathbf{u} \in S \cap B$ adjacent to $\mathbf{t}$. Note $d(\mathbf{s}, \mathbf{u}) \ne k$, because $d(\mathbf{s}, \mathbf{t}) = k$ and $\mathbf{u}$ and $\mathbf{t}$ are in different parts of the bipartite graph K_2^n. Thus, $d(\mathbf{s}, \mathbf{u}) = k-1$, so by the induction hypothesis, there is a path of length $k-1$ from $\mathbf{s}$ to $\mathbf{u}$ in S. Adjoining $\mathbf{t}$ to the end of this, a path of length k from $\mathbf{s}$ to $\mathbf{t}$ is obtained.

This completes this inductive proof and the proof that S is isometric. ∎

Note that in the above proof K_2^n can be replaced by any connected bipartite graph. Also, it is true that if *every* ball intersects $S \subseteq K_2^n$ in a connected set, then S is a cube. This is easily established by appealing to the No3) condition of the previous section.

The balls of Euclidean space have the property that for a given volume they have the boundary of smallest measure. Consider the following related extremal problem of Hamming geometry.

Problem. What subset of m points of K_2^n has smallest closed neighborhood?

The *closed neighborhood* of a set S is S, together with all points for which there is an adjacent point in S. A large number of papers have been published concerning this problem. It is known that when m is the size of some ball in K_2^n then this ball is a solution to the problem. However, not all values of m are the size of some ball; points can be added onto a ball so that a solution is obtained for the other values of m. A paper by Ahlswede and Katona [11] discusses this and related extremal problems in K_2^n.

1.6. Quasicubes

Consider the following extremal problem.

Problem. What subset of m points of K_2^n has the largest number of edges in the subgraph it induces?

The solution [12, [13, [14] introduces a new type of set.

Definition. A *quasicube* is any subset of K_2^n obtained by applying an isometry of K_2^n to the set of 0-1 vectors consisting of the binary representations of the m integers from 0 to $m-1$, for some m.

Quasicubes generalize cubes because any k-cube is a quasicube with 2^k points. The references given above establish that these and only these sets solve the extremal problem. In these papers, alternative ways of describing quasicubes have been found. The empty set is a quasicube and if R is a quasicube contained in a cube Q, then $Q \cup (R \oplus \mathbf{t})$ is a quasicube for any vector $\mathbf{t}$ of weight 1. All quasicubes can be recursively constructed in this manner.

By interchanging 0 and 1 the first binary expansions of the first m nonnegative integers become the binary expansions of the *final* m integers in the range $[0, 2^n - 1]$. Thus, the complement of a quasicube is also a quasicube. Furthermore, it follows from the recursive definition of quasicubes, that if $F \subseteq K_2^n$ is any cube and $R \subseteq K_2^n$ is any quasicube then $F \cap R$ is a quasicube. In fact, the quasicubes of K_2^n are the smallest of family of its subsets which satisfy the following conditions.
i) The family contains the empty set.
ii) The intersection of any cube with any member of the family is again in the family.
iii) The complement of any member of the family is a member of the family.

Quasicubes apparently first arose in the attempt to label the vertices of the n-cube with the integers from 1 to 2^n so that the absolute value of the difference of the values of two adjacent vertices, averaged over all edges of the n-cube, is minimized. The solutions are the orders defined below.

Definition. A *Harper order* of the vertices of the n-cube is a bijection $F: \{0, 1, \ldots, 2^n - 1\} \to K_2^n$ with the property that the image of $\{0, 1, \ldots, i\}$ under F is a quasicube, for each $i < 2^n$.

By the definition of quasicubes, the map taking each integer to its representation in binary is one example of these orders. This order will be called the *lexicographic* order. The total number of such orders was found by Harper [12]. Since the complement of a quasicube is a quasicube, if $F(j)$ is a Harper order, so is the reversed order, $F(2^n - 1 - j)$.

I am indebted to David I. Lieberman for suggesting that the reflected Gray code [15] is another Harper order. The reflected Gray code order competes with the lexicographic order for being the most ‘‘natural’’ order of the n-cube. To find the j^{th} vector in the reflected Gray code order, first write the binary representation of j as a 0-1 vector $(\beta_{n-1}, \ldots, \beta_0)$, with lower order digits on the right and padding extra zeroes on the left to produce a vector of length n. The j^{th} vector of the reflected Gray code is

$$G(j) = (\beta_{n-1}, \beta_{n-1} \oplus \beta_{n-2}, \ldots, \beta_1 \oplus \beta_0) .$$

One of the many properties of this order is that $G(j)$ is adjacent to $G(j+1)$ for all $j < 2^n$ and $G(2^n - 1)$ is adjacent to $G(0)$. Thus, the order forms a Hamiltonian circuit of K_2^n, $n > 1$. Using the recursive definition of quasicubes, it can be shown that $\{G(0), \ldots, G(m-1)\}$ is a quasicube for each m. Since all quasicubes of order m are isometric, this shows that the induced subgraph of any quasicube has a Hamiltonian path. Furthermore, if $m \geq 4$ and m is even, a quasicube of order m is isometric to $K_2 \times$ (a quasicube of order $m/2$). Thus, such quasicubes have a Hamiltonian circuit which covers one half and then returns by covering the second half in reverse order.

Another interpretation of the problem stated at the beginning of this section is to maximize the number of 1-cubes in a set of order m. This problem has the obvious extension of asking for the sets of order m having the largest total number of subcubes of all dimensions. As an application of Theorem 4.2 in [11], the solutions to this problem are the same as the original problem, as might have been expected.

Instead of counting the total number of subcubes in a set, the most interesting problems have concentrated on the *maximal* subcubes of a set. Many papers have been written about the problem of covering a given set with the smallest possible number of its (maximal) subcubes. The general problem is NP hard, it being equivalent to the Minimum Disjunctive Normal Form problem of [10]. There has been great interest in this problem due to the application to efficiently implementing switching functions. For subsets of an n-cube, there exist methods which work well for reasonable values of n. The most well known of these is Quine-McCluskey [16]. The more theoretical problem of how many maximal subcubes a set of order m may have is explored in [17].

1.7. Ellipsoids

Balls and quasicubes belong to a more generalized family of subsets of K_2^n, defined below.

Definition. An *ellipsoid* is a set $S \subseteq K_2^n$ of the form $S = \{\mathbf{s} \in K_2^n \mid (\mathbf{s}, \mathbf{a}) \geq b\}$ where $\mathbf{a}$ is an arbitrary real vector and b is an arbitrary real number. Here $(\mathbf{s}, \mathbf{a})$ denotes the real-valued inner product.

The elements of K_2 may be taken to be $\{0, 1\}$, $\{1, -1\}$ or any two real numbers, and the family of ellipsoids will be the same. Imagine the vertices of the n-cube as the vertices of a regular polytope in $\mathbf{R}^n$. The ellipsoids are those sets of vertices which can be separated from the others by a hyperplane in $\mathbf{R}^n$. The name "ellipsoid" is used in this thesis because some constructions which give ellipsoids in Euclidean geometry yield these sets when applied to Hamming geometry. In the literature the characteristic functions of these sets are well known as the family of *threshold functions* [18], [19], [20], [21], [22].

Standard facts about ellipsoids are that application of an isometry of K_2^n to an ellipsoid gives an ellipsoid. Also, the complement of an ellipsoid is an ellipsoid, as is true of the families of balls and quasicubes. A result which probably deserves to be called "the fundamental theorem of ellipsoids" is that an ellipsoid is determined by the cardinalities of its intersections with cubes of co-dimension 1. One application of this theorem is to show that there are not a huge number of distinct ellipsoids. The number of subsets of K_2^n is 2^{2^n}, but it can be determined from the fundamental theorem that the number of ellipsoids is $2^{O(n^2)}$.

We will now discuss an extremal problem whose solution is an ellipsoid, but the specific ellipsoids which solve the problem are not known. Given $S \subseteq K_2^n$, let $v(S)$ be the sum of all Hamming distances between unordered pairs of points from S. Thus, $v(S)$ is a "potential energy" measure of S.

Theorem 1.7.1. If $S \subseteq K_2^n$, minimizes $v(S)$ subject to the constraint that $|S| = m$, then S is an ellipsoid.

Proof. Let $K_2^n = \{+1, -1\}^n$. Since every single point is an ellipsoid, we may assume $m \geq 2$. Let S be a set of m points with minimum value of v. Let $\mathbf{a} = \sum_{\mathbf{s} \in S} \mathbf{s}$. It will be shown that there exists a b such that the ellipsoid defined by $(\mathbf{a}, \mathbf{s}) \geq b$ is S. To the contrary, suppose that $(\mathbf{a}, \mathbf{s}) \leq (\mathbf{a}, \mathbf{t})$ for some $\mathbf{s} \in S$ and $\mathbf{t} \notin S$.

Let $T = (S \backslash \{\mathbf{s}\}) \cup \{\mathbf{t}\}$. It will be shown that $v(T) < v(S)$. Note that

$$v(T) - v(S) = \sum_{\mathbf{u} \in S \backslash \{\mathbf{s}\}} (d(\mathbf{u}, \mathbf{t}) - d(\mathbf{u}, \mathbf{s})) .$$

Also, for any points $\mathbf{x}$ and $\mathbf{y}$, $2d(\mathbf{x},\mathbf{y}) = n - (\mathbf{x},\mathbf{y})$. Thus, $2(d(\mathbf{u},\mathbf{t}) - d(\mathbf{u},\mathbf{s})) = (\mathbf{u},\mathbf{s}) - (\mathbf{u},\mathbf{t})$, so

$$2\nu(T) - 2\nu(S) = (\mathbf{a}-\mathbf{s},\mathbf{s}) - (\mathbf{a}-\mathbf{s},\mathbf{t})$$

$$= ((\mathbf{a},\mathbf{s}) - (\mathbf{a},\mathbf{t})) + ((\mathbf{s},\mathbf{t}) - (\mathbf{s},\mathbf{s}))\ .$$

Note that

$$(\mathbf{a},\mathbf{s}) - (\mathbf{a},\mathbf{t}) \le 0$$

by assumption and that $(\mathbf{s},\mathbf{t}) < (\mathbf{s},\mathbf{s})$. Thus, $\nu(T) < \nu(S)$, a contradiction. ∎

1.8. Stars

We may further generalize the ellipsoids. The following definition is standard in any geometry.

Definition. A set S is a *star* if there is a point $\mathbf{c}$ such that for every $\mathbf{x} \in S$, $I(\mathbf{c},\mathbf{x}) \subseteq S$. The point $\mathbf{c}$ is called a *center* of S.

Note that the empty set is a star and that for nonempty stars any center must lie in the star. If two stars have center $\mathbf{c}$, then both their intersection and union is a star with center $\mathbf{c}$. A fact which is true for any K_b^n is that the set of centers of any star is strongly convex. Also, in Euclidean geometry, the set of centers of a star is convex. If $C \subseteq K_b^n$ is a nonempty cylinder, then for any star S with center $\mathbf{c}$, both $S \cap C$ and $\pi_C(S)$ are stars with center $\pi_C(\mathbf{c})$.

If we restrict ourselves to K_2^n, then for every star with center $\mathbf{c}$, the complement, S^c, is a star with center $\bar{\mathbf{c}}$. Since the cylinders of K_2^n are its cubes, the intersection of any cube with a star is a star. Since stars are connected sets, this implies that stars in K_2^n are isometric.

To show that any ellipsoid is a star, consider some nonempty ellipsoid defined by $\mathbf{a}$ and b. It is convenient to take $K_2 = \{1,-1\}$. Let $\mathbf{c} \in K_2^n$ be such that $a_i c_i \ge 0$, for $i = 1,2,\ldots,n$. Since $\mathbf{x} = \mathbf{c}$ maximizes $(\mathbf{a},\mathbf{x})$ for all $\mathbf{x} \in K_2^n$, $\mathbf{c}$ is in the ellipsoid. Furthermore, if $\mathbf{y}$ is any other point in the ellipsoid, moving from $\mathbf{y}$ towards $\mathbf{c}$ can only increase the inner product with $\mathbf{a}$. Thus, $I(\mathbf{c},\mathbf{y})$ is contained in the ellipsoid. Therefore, the ellipsoid is a star with center $\mathbf{c}$.

In general, it is not true that the closed neighborhood of a quasicube is a quasicube or that the closed neighborhood of an ellipsoid is an ellipsoid. In the geometry of any graph, the closed neighborhood of a ball is a ball. For Hamming geometry, this property is also true of stars.

Proposition 1.8.1. The closed neighborhood of any star in K_b^n is a star.

Proof. Let $S \subseteq K_b^n$ be a star with center $\mathbf{c}$ and containing a point $\mathbf{x}$. Let $\mathbf{y}$ be any point at unit distance from $\mathbf{x}$. It will be shown that $I(\mathbf{c},\mathbf{y}) \subseteq N(S)$, where $N(S)$ is the closed neighborhood of S. Thus, $\mathbf{c}$ is a center for $N(S)$.

By isometry, we can assume $\mathbf{c} = 0^n$, writing vectors as words. Also, $\mathbf{x}$ can be taken to be $0^{n-j}1^j$, for some j. We can assume that $\mathbf{y} \notin I(\mathbf{c},\mathbf{x})$, since otherwise, $I(\mathbf{c},\mathbf{y}) \subseteq S \subseteq N(S)$ and we are done. Using the remaining freedom in the isometry, $\mathbf{y}$ can be assumed to be one of two words.

Case 1) $\mathbf{y} = 0^{n-j-1}1^{j+1}$.
Then $I(\mathbf{c},\mathbf{y})$ is a $(j+1)$-cube containing the j-cube $I(\mathbf{c},\mathbf{x})$. It follows that each point of $I(\mathbf{c},\mathbf{y})$ lies at distance at most 1 from some point of $I(\mathbf{c},\mathbf{x})$. Thus, $I(\mathbf{c},\mathbf{y}) \subseteq N(I(\mathbf{c},\mathbf{x})) \subseteq N(S)$. If $b = 2$ this completes the proof, otherwise there is the remaining case.

Case 2) $\mathbf{y} = 0^{n-j}1^{j-1}2$.
Then for each point of $I(\mathbf{c},\mathbf{y})$, if the rightmost symbol is replaced with a 0, the result is in $I(\mathbf{c},\mathbf{x})$. Thus, $I(\mathbf{c},\mathbf{y}) \subseteq N(I(\mathbf{c},\mathbf{x})) \subseteq N(S)$. ∎

The characteristic functions of stars in K_2^n form a class of Boolean functions called "unate". In the theory of unate functions there is an important subclass known as the "completely monotone" functions.

The corresponding family of sets, to which we apply the same name, is defined below.

Definition. $S \subseteq K_2^n$ is *completely monotone* if and only if for every two parallel cubes Q and R, either $\pi_Q(S \cap R) \subseteq S \cap Q$ or $\pi_R(S \cap Q) \subseteq S \cap R$.

Recall that parallel cubes must have the same dimension. If the definition above is modified to restrict Q and R to have dimension $n-1$, the family of stars is obtained. Thus, completely monotone sets are stars.

Another class of Boolean functions are the 2-asummable functions, and we again apply the same name to the associated family of sets.

Definition. $S \subseteq K_2^n$ is 2-*asummable* if and only if $S+S$ and S^c+S^c are disjoint.

In this definition + denotes addition of sets of real vectors. Ellipsoids are sets S such that a hyperplane of $\mathbf{R}^n$ separates S from S^c. This is equivalent to saying that the convex hull of S is disjoint from the convex hull of S^c. Thus, the midpoint of no two points of S is never equal to the midpoint of two elements of S^c. In other words, $\frac{1}{2}(S+S)$ is disjoint from $\frac{1}{2}(S^c+S^c)$, so ellipsoids are 2-asummable.

It was known early that 2-asummable implies completely monotone. Thus, there is the following relation among the families.

$$\text{Ellipsoids} \subseteq 2-\text{Asummable} \subseteq \text{Completely Monotone} \subseteq \text{Stars}\,.$$

It took some time to discover that 2-asummable is actually the same as completely monotone. Also, there is an example in the 9-cube of a 2-asummable set which is not an ellipsoid. Both of these facts can be found in Muroga's book [20,ch.7].

2. Retracts

2.1. Doubly Symmetric Operations

Given any metric space $\mathbf{X}$ consider mappings $F\colon \mathbf{X}^a \to \mathbf{X}$ which have the following two sets of symmetries.
1) $F(\mathbf{x}^{\sigma(1)}, \ldots, \mathbf{x}^{\sigma(a)}) = F(\mathbf{x}^1, \ldots, \mathbf{x}^a)$ for any a points $\mathbf{x}^1, \ldots, \mathbf{x}^a$ of $\mathbf{X}$ and any permutation σ of $\{1, 2, \ldots, a\}$.
2) $F(\eta(\mathbf{x}^1), \ldots, \eta(\mathbf{x}^a)) = \eta(F(\mathbf{x}^1, \ldots, \mathbf{x}^a))$ for any a points $\mathbf{x}^1, \ldots, \mathbf{x}^a$ of $\mathbf{X}$ and any isometry η of $\mathbf{X}$.

Any such F will be called an *a-ary doubly symmetric* operation on $\mathbf{X}$. Each $\mathbf{x}^i$ is an argument and $\mathbf{x}^1, \ldots, \mathbf{x}^a$ will be called the argument list. The motivating example is the operation of taking the midpoint of two points in Euclidean space. It is easily verified that this is a 2-ary doubly symmetric operation. It will soon be shown that if $\mathbf{X} = K_2^n$, no such 2-ary operations exist. However, there is an interesting 3-ary doubly symmetric operation. The 3-ary threshold operation, T_3, is performed by taking a majority vote in each coordinate of the three vectors. This is illustrated below for three five-dimensional vectors.

$$\begin{array}{c} 0\,0\,0\,1\,0 \\ 1\,0\,0\,1\,1 \\ \underline{1\,0\,1\,1\,0} \\ 1\,0\,0\,1\,0 \end{array}$$

The symmetries of the T_3 operation are best seen by using a purely geometric definition. Given any three points $\mathbf{x}, \mathbf{y}, \mathbf{z} \in K_2^n$, the point $\mathbf{w} = T_3(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is the unique point minimizing the following function of $\mathbf{w}$, $d(\mathbf{w}, \mathbf{x}) + d(\mathbf{w}, \mathbf{y}) + d(\mathbf{w}, \mathbf{z})$. This minimization problem can be solved for each coordinate of $\mathbf{w}$ separately, showing it is in fact the operation given above. The geometric definition immediately implies the operation commutes with any isometry, establishing the set 2) of symmetries. Another interesting property of the point $\mathbf{w} = T_3(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is that $\{\mathbf{w}\} = I(\mathbf{x}, \mathbf{y}) \cap I(\mathbf{y}, \mathbf{z}) \cap I(\mathbf{z}, \mathbf{x})$.

The other important 3-ary operation in K_2^n, which will be called A_3, is affine combination modulo 2. For this operation the columns are totaled modulo 2, as illustrated below.

$$\begin{array}{c} 0\,0\,0\,1\,0 \\ 1\,0\,0\,1\,1 \\ \underline{1\,0\,1\,1\,0} \\ 0\,0\,1\,1\,1 \end{array}$$

This operation can also be defined purely geometrically. For any three points $\mathbf{x}, \mathbf{y}, \mathbf{z}$, the point $\mathbf{v} = A_3(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is the unique point $\mathbf{v}$ minimizing $d(\mathbf{v}, \mathbf{x}) + d(\mathbf{v}, \mathbf{y}) + d(\mathbf{v}, \mathbf{z}) - 2d(\mathbf{v}, T_3(\mathbf{x}, \mathbf{y}, \mathbf{z}))$. Again, this can be shown for each coordinate of $\mathbf{v}$ independently.

In the notation of modulo 2 addition,

$$\mathbf{v} = A_3(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathbf{x} \oplus \mathbf{y} \oplus \mathbf{z}$$

$$d(\mathbf{v}, \mathbf{z}) = |\mathbf{v} \oplus \mathbf{z}| = |\mathbf{x} \oplus \mathbf{y}| = d(\mathbf{x}, \mathbf{y})\,.$$

Similarly, $d(\mathbf{v}, \mathbf{x}) = d(\mathbf{y}, \mathbf{z})$ and $d(\mathbf{v}, \mathbf{y}) = d(\mathbf{x}, \mathbf{z})$. Unfortunately, equality of these three pairs of distances does *not* in general uniquely determine the point $\mathbf{v}$.

In keeping with the above two examples, a method for constructing a-ary doubly symmetric operations, F, on K_b^n is to find an a-ary doubly symmetric operation, f, on K_b and apply it to each of the n coordinates.

$$F(\mathbf{x}^1, \ldots, \mathbf{x}^a)_i = f(x_i^1, \ldots, x_i^a) \quad \text{for } i = 1, \ldots, a\,.$$

It is this class of "elementary" doubly symmetric operations on K_b^n which is of most concern. They have additional properties, not the least of which is the Lipshitz property,

$$d(F(\mathbf{x}^1, \ldots, \mathbf{x}^a), F(\mathbf{y}^1, \ldots, \mathbf{y}^a)) \le d(\mathbf{x}^1, \mathbf{y}^1) + \cdots + d(\mathbf{x}^a, \mathbf{y}^a)\,.$$

Again, this has an easy coordinatewise proof.

The rest of this section is devoted to the problem of finding the a-ary doubly symmetric operators on K_b. The name doubly symmetric is particularly appropriate here because the isometries of K_b form the symmetric group on b symbols. The identity operation is always a doubly symmetric unary operation. For $b = 2$ the function taking 0 to 1 and 1 to 0 is another unary doubly symmetric operation. These are the *only* examples of unary doubly symmetric operations on K_b. It is clear that there are no more examples for $b = 2$. Suppose we have a unary doubly symmetric operation f on K_b with $b > 2$. If f is not the identity, $f(i) = j$, for some $i \neq j$. Without loss of generality, assume $i = 0$ and $j = 1$. Let η be a permutation of $\{0, 1, \ldots, b-1\}$ which fixes 0 but takes 1 to 2. Then $\eta(f(0)) = 2 \neq 0 = f(\eta(0))$, contradicting the second condition in the definition of doubly symmetric operations.

Theorem 2.1.1. Doubly symmetric operations on K_b with more than one argument only exist for $b \in \{2, 3, 4, 6\}$. For each of these values, doubly symmetric operations exist precisely when the number of arguments is,

for $b = 2$, any odd number,

for $b = 3$, any number not divisible by 3,

for $b = 4$, any odd number,

for $b = 6$, any odd number not divisible by 3.

Proof.

Let $b = 2$**.** If the number of arguments is $2n$ consider the value of a doubly symmetric f applied to the argument list of n 0's followed by n 1's, which we may denote $f(0^n 1^n)$. If η interchanges 0 and 1, by both symmetry conditions we have

$$\eta(f(0^n 1^n)) = f(1^n 0^n) = f(0^n 1^n) .$$

This is clearly a contradiction, because η has no fixed points. For an odd number of arguments, say $2n+1$, many types of doubly symmetric operations can be constructed. For example, the sum modulo 2 of all arguments can be taken. This will be denoted A_{2n+1}, extending the definition of A_3. The definition of T_3 can also be extended by taking a majority vote across any odd number of arguments, yielding the doubly symmetric operation T_{2n+1}.

A permutation σ on $\{1, 2, \ldots, a\}$, dependent on the values of the arguments, can be used to reorder the argument list of f so that all 0's appear to the left of all 1's, all 1's appear to the left of all 2's, and so on. Thus, the argument list can be brought into the form $0^{n_0} 1^{n_1} \cdots (b-1)^{n_{b-1}}$. A permutation η on K_b can be used to make 0 the most frequent value in the argument list, 1 the next most frequent, and so on. Thus, f is determined by its values on argument lists of the form

$$0^{n_0} 1^{n_1} \cdots (b-1)^{n_{b-1}} \qquad n_0 \geq n_1 \geq \cdots \geq n_{b-1} \qquad n_0 + n_1 + \cdots + n_{b-1} = a .$$

Let S be the set of argument lists in this "normalized" form.

It has just been shown that f is determined from its values on S. Let $g: S \rightarrow K_b$ be an arbitrary function. If g is the restriction to S of some doubly symmetric operation f then to evaluate $f(y)$, find a σ and η taking y to $x \in S$ and then it follows that $f(y) = \eta^{-1}(g(x))$. If this procedure can yield two distinct values for $f(y)$ then no doubly symmetric operation f restricts to g. Suppose that the action of η followed by σ takes $x \in S$ to itself and $\eta(g(x)) \neq g(x)$, i.e., g does not extend to a doubly symmetric operation. Then let $i = g(x)$ and let $j = \eta(i)$, so i and j are distinct integers such that $n_i = n_j$. Conversely, let $i = g(x)$ and suppose $n_i = n_j$ for some $j \neq i$. Pick η to be the transposition interchanging i and j and there will be a σ such that σ and η take x to itself and $\eta(g(x)) \neq g(x)$. Therefore, a necessary and sufficient condition that g extend to a doubly symmetric f is that for no $x \in S$ does a $j \in K_b$ exist such that $j \neq g(x)$ and j appears in x the same number of times as $g(x)$ appears in x.

If a solution, in nonnegative integers, to the equation $n_0 + \cdots + n_{b-1} = a$ can be found such that no n_i is unique then no doubly symmetric a-ary operation on K_b exists. Suppose, on the contrary, each solution always has some value uniquely appearing. Let $s(n_0, \ldots, n_{b-1})$ be the smallest value of i for which the value n_i appears precisely once in $n_0, \ldots, n_{b-1}$. Then the function $g(0^{n_0} \cdots (b-1)^{n_{b-1}}) = s(n_0, \ldots, n_{b-1})$ extends to a doubly symmetric operation. This operation will be denoted T_a (or just T) because in the case $b = 2$ it is the operation already given that name.

Let $b = 3$**.** If $a = 3n$ then the partition $n_0 = n_1 = n_2 = n$ has no unique part so there is no doubly symmetric operation. If $n_0 + n_1 + n_2 = a$ and a is not a multiple of 3, then some n_i is not equal to either of the others, so a doubly symmetric operation exists.

Let $b = 4$**.** If $a = 2n$ then $n + n + 0 + 0 = a$ is a partition with no distinct parts so no doubly symmetric operation exists. On the other hand if a is odd and $n_0 + n_1 + n_2 + n_3 = a$, all four parts obviously can't be equal. If there are no distinct parts we may assume $n_0 = n_1$ and $n_2 = n_3$, but this still contradicts that a is odd, so a doubly symmetric operation exists.

Let $b = 5$**.** For any $a \geq 2$ there is a partition $n_0 + n_1 + n_2 + n_3 + n_4 = a$, $n_0 \geq n_1 \geq n_2 \geq n_3 \geq n_4 \geq 0$, with no distinct parts. If a is even let $n_0 = n_1$ and $n_2 = n_3 = n_4 = 0$. If $a \geq 5$ is odd let $n_0 = n_1$ and $n_2 = n_3 = n_4 = 1$. Finally, for $a = 3$, we have $1 + 1 + 1 + 0 + 0 = 3$. Hence, no doubly symmetric operations exist with more than 1 argument.

Let $b = 6$**.** If $a = 2n$, $n + n + 0 + 0 + 0 + 0 = a$, and if $a = 3n$, $n + n + n + 0 + 0 + 0 = a$, so there are no doubly symmetric operations in these cases. Given an ordered partition with no distinct parts either $n_0 = n_1$, $n_2 = n_3$ and $n_4 = n_5$, or else $n_0 = n_1 = n_2$ and $n_3 = n_4 = n_5$. If neither 2 or 3 divides a no such partition exists, so there is a doubly symmetric operation.

Let $b \geq 7$**.** It was shown under the case $b = 5$ that for any $a \geq 2$ there is a partition $n_0 + n_1 + n_2 + n_3 + n_4 = a$ with no distinct parts. By setting $n_5 = n_6 = \cdots = n_{b-1} = 0$ we have a partition of a into b parts with no parts distinct, so there are no doubly symmetric operations. ∎

Corollary 2.1.2. Doubly symmetric operations with more than one argument don't exist on K_b^n for any $n \geq 1$ and $b \notin \{2, 3, 4, 6\}$.

Proof. Let η be the isometry on K_b^n which performs a left circular shift of the coordinates by one position. Thus, $\eta((x_1, \ldots, x_n)) = (x_2, \ldots, x_n, x_1)$. The set of fixed points of η is $\{\mathbf{x} | x_1 = x_2 = \cdots = x_n\}$. If F is a doubly symmetric operation on K_b^n and each of its arguments is fixed by η, the result of F must also be fixed by η. Thus, the equation

$$F((x^1, \ldots, x^1), \ldots, (x^a, \ldots, x^a)) = (y, \ldots, y)$$

defines a doubly symmetric operation f on K_b such that $f(x^1, \ldots, x^a) = y$. If $a > 1$, Theorem 1 showed that $b \in \{2, 3, 4, 6\}$. ∎

2.2. T_3 Closed Sets

A subset S of K_2^n will be said to be "T_3 closed" if application of T_3 to any three not necessarily distinct members of S is again a member of S. An interesting fact concerning such sets is that they can be identified with the solution sets of certain systems of equations in 0-1 valued variables. Given any such system in the variables $x_1, \ldots, x_n$, the *solution set* is a subset of K_2^n, such that whenever $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ is a solution, $(\alpha_1, \ldots, \alpha_n)$ is a member of the solution set.

A linear system of equations modulo 2 has solution set closed under the A_3 operation and any A_3 closed set is the solution set of some such system. T_3 closed sets correspond to solution sets of $2SAT$ systems.

Definition. A 2SAT system is a system of equations in 0-1 variables $x_1, \ldots, x_n$, $n \geq 1$, where each equation is of the form $y \vee z = 1$ where y and z are *literals*. The operation $\vee$ denotes logical OR. A literal is an expression of the form x_i or $\bar{x}_i$ for some variable x_i.

Each equation in a 2SAT system is called a clause. If the two literals involve distinct variables it will be called a 2-clause. A clause of the form $y \vee y = 1$ is equivalent to $y = 1$ and will be called a 1-clause.

It may be assumed that a 2SAT system contains no redundant clauses, in which case there are at most $4\binom{n}{2}$ 2-clauses and $2n$ 1-clauses. It is well known to complexity theorists that a linear time algorithm exists which determines consistency of a 2SAT system and produces a solution if one exists [23], [24].

Theorem 2.2.1. $S \subseteq K_2^n$, $n \geq 1$, is T_3 closed if and only if S is the solution set of a 2SAT system.

Proof. First, we show that any 2SAT solution set, S, is T_3 closed. Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in S$ and $y \vee z = 1$ be a clause of the system. Note that either $y = 1$ is true for at least two of the vectors or $z = 1$ is true for at least two of the vectors. Without loss of generality say $y(\mathbf{u}) = y(\mathbf{v}) = 1$. Then $y(T_3(\mathbf{u}, \mathbf{v}, \mathbf{w})) = 1$ and $T_3(\mathbf{u}, \mathbf{v}, \mathbf{w})$ satisfies the clause. Since $T_3(\mathbf{u}, \mathbf{v}, \mathbf{w})$ will satisfy all clauses, S is T_3 closed.

Now let S be any T_3 closed set. If $n = 1$, it is clear that S is the solution set of a 2SAT system, so it can be assumed that $n > 1$. For all 2- and 1-clauses involving the n variables determine which are true for all members of S. Form a 2SAT system from all these clauses. Let $\hat{S}$ be the solution set of this 2SAT system. Clearly $S \subseteq \hat{S}$. Let $\mathbf{u} \in \hat{S}$. There must be a vector, $\mathbf{v} \in S$, such that $v_1 = u_1$ and $v_2 = u_2$, since otherwise there would be a 2-clause involving the first two coordinates, $(x_1 \neq u_1) \vee (x_2 \neq u_2) = 1$, which is true everywhere on S, but not true on $\mathbf{u}$, a contradiction. Similarly, for any $1 \leq i < j \leq n$, there is a $v \in S$ with $v_i = u_i$ and $v_j = u_j$.

By induction it can be proved that for any collection of k coordinates, $2 \leq k \leq n$, there is an element of S which agrees with $\mathbf{u}$ in these positions. The preceding paragraph showed this for $k = 2$. Assume it is true for some particular value of $k < n$. Without loss of generality, the first $k+1$ coordinates are selected. By the induction hypothesis, there exist three vectors in S whose first $k+1$ coordinates are $(a, u_2, u_3, u_4, \ldots, u_{k+1})$, $(u_1, b, u_3, u_4, \ldots, u_{k+1})$ and $(u_1, u_2, c, u_4, \ldots, u_{k+1})$, for some a, b, c. The T_3 combination of these three vectors has its initial $k+1$ coordinates the same as $\mathbf{u}$, as required for the induction step. Now, apply this with $k = n$ to obtain $\mathbf{u} \in S$. Thus, $\hat{S} \subseteq S$, so $S = \hat{S}$. ⁑

Notes: The above theorem can be derived from the Baker-Pixley theorem in universal algebra [25]. Also, the method of proof was to take three vectors, each of which is correct in k positions, and produce a vector correct in $k+1$ positions. This can be made much more "efficient", in that we can use essentially the same method to take three vectors, each correct in $2k$ positions, and produce a vector correct in $3k$ positions. Thus, for whatever it is worth, the number of correct positions can be made to increase exponentially.

Proposition 2.2.2. For $n \geq 1$, the combinatorial spaces are those subsets of K_2^n which are closed under both T_3 and A_3.

Proof. It is easily verified that combinatorial spaces are both T_3 and A_3 closed. In fact, if equations of the form $x_i = 0$, $x_i = 1$, $x_i = x_j$, or $x_i = \bar{x}_j$ are true on all three argument vectors, they are true for the result of T_3 or A_3 applied to these vectors.

Now let $S \subseteq K_2^n$ be both T_3 and A_3 closed. If $n \leq 2$, S is a combinatorial space, by inspection. Assuming $n \geq 3$, pick $1 \leq i < j \leq n$ and let $U_{i,j} = \{(x_i, x_j) \mid \mathbf{x} \in S\}$. Note $U_{i,j} \subseteq K_2^2$ and $U_{i,j}$ is both T_3 and A_3 closed. We know by Theorem 1 that $U_{i,j}$ is a solution set of a 2SAT system in x_i and x_j. Since $U_{i,j}$ is a combinatorial space, it is also the solution set (see section 1.3) of a system where each equation either declares a variable to be a constant, declares two variables to be equal or declares one variable to equal the complement of the another.

By Theorem 1, the conjunction of the 2SAT systems for all the $U_{i,j}$ is a 2SAT system whose solution set is S. But, we have seen that the 2SAT system for each $U_{i,j}$ is equivalent to a "combinatorial system". The conjunction of all these is a combinatorial system whose solution set is also S. ⁑

Let t_3: $K_2^3 \to K_2$ be the 3-ary Boolean function equal to the operation T_3 on vectors of length 1. Consider the problem of determining which Boolean functions $f(x^1, \ldots, x^a)$ can be obtained from iterated compositions of the arguments and t_3. The function f can be represented by its truth table, a vector of length 2^a, and the argument functions $x^1, \ldots, x^a$ can also be represented as vectors of length 2^a. Since composition of three functions with t_3 results in a function whose truth table is a T_3 combination of the truth tables of each of the three functions, f is obtainable if and only if its truth table is in the T_3 closure of the truth tables of the argument functions. By Theorem 1, f is obtainable if and only if its truth table satisfies all 1- or 2-clauses satisfied by the truth tables of the argument functions. The set of clauses can be simplified to a smaller set by using elementary logical operations, to obtain the following well known result in switching theory.

Proposition 2.2.3. A function $f: K_2^a \to K_2$, $a \geq 1$, can be obtained from its arguments by iterated composition with t_3 if and only if the following statements always hold.
1) $f(0, \ldots, 0) = 0$,
2) $f(\bar{x}^1, \ldots, \bar{x}^a) = \bar{f}(x^1, \ldots, x^a)$
3) if $x^i \leq y^i$ for $i = 1, \ldots, a$ then $f(x^1, \ldots, x^a) \leq f(y^1, \ldots, y^a)$.

Let t_{2k+1} be the Boolean function corresponding to T_{2k+1}, $k \geq 1$. By the proposition above, each t_{2k+1} can be obtained from t_3. (It is also true that t_3 can be obtained from each t_{2k+1}, but this fact will not be needed). This means the T_{2k+1} combination of 0-1 vectors can be obtained by combining them three at a time using T_3.

Theorem 2.2.4. For any $S \subseteq K_2^n$ and $\mathbf{x} \in K_2^n$, let $v(\mathbf{x}, S) = \sum_{\mathbf{s} \in S} d(\mathbf{x}, \mathbf{s})$. The set of points $\mathbf{x} \in K_2^n$ minimizing $v(\mathbf{x}, S)$ is a cube, Q. If $|S|$ is odd then $|Q| = 1$. If S is T_3 closed and nonempty, then $Q \cap S$ is a nonempty combinatorial space, and Q is the smallest cube containing $Q \cap S$.

Proof. The problem of minimizing $v(\mathbf{x}, S)$ is easy, because it can be solved independently for each coordinate of $\mathbf{x}$. To find x_i, count how many times $s_i = 0$ and how many times $s_i = 1$, for all $\mathbf{s} \in S$. The value of x_i must be selected to agree with the value giving the larger count. If the two counts are equal, x_i can be arbitrarily set to 0 or 1. The set of all $\mathbf{x}$ obtained in this way is a cube, which will be called Q. In particular, if S is empty, then Q is all of K_2^n.

Call i a balanced coordinate if the count for $s_i = 0$ equals that for $s_i = 1$. The directions of Q are the balanced coordinates. Let $|S| = m$. If m is odd, there are no balanced coordinates, so $|Q| = 1$. In fact, the single element of Q is $T_m(\mathbf{s}^1, \ldots, \mathbf{s}^m)$, where $S = \{\mathbf{s}^1, \ldots, \mathbf{s}^m\}$.

Now let S be T_3 closed. If m is odd, by the discussion after Proposition 3, the single point of Q is in S.

Assume now that m is even and greater than 0. For any $\mathbf{s}^i \in S$, define $\mathbf{g}(\mathbf{s}^i)$ to be $T_{m-1}(\mathbf{s}^1, \ldots, \mathbf{s}^{i-1}, \mathbf{s}^{i+1}, \ldots, \mathbf{s}^m)$. Any coordinate which is unbalanced for S will have the majority value appearing at least two more times than the minority value, because $|S|$ is even. Thus, the coordinate will have the same majority value in $S \backslash \{\mathbf{s}^i\}$. Thus, $\mathbf{g}(\mathbf{s}^i) \in Q$.

By the discussion after Proposition 3, $\mathbf{g}(\mathbf{s}^i) \in S$. Let $\mathbf{c}$ be the vector which is zero at unbalanced coordinates of S and one at balanced coordinates of S. We claim that if $\mathbf{z} \in Q \cap S$, then $\mathbf{g}(\mathbf{z}) = \mathbf{z} \oplus \mathbf{c}$. This is because for each balanced coordinate, i, of S, the majority value in the i^{th} coordinate of $S \backslash \{\mathbf{z}\}$ is $\bar{z}_i$.

We have now shown that $Q \cap S$ is nonempty, and for $\mathbf{z} \in Q \cap S$, $\mathbf{z} \oplus \mathbf{c} \in Q \cap S$. This shows that Q is the smallest cube containing $Q \cap S$, because $Q \cap S$ contains both $\mathbf{z}$ and $\mathbf{z} \oplus \mathbf{c}$ and $d(\mathbf{z}, \mathbf{z} \oplus \mathbf{c}) = \dim(Q)$. Finally, $Q \cap S$ is the intersection of two 2SAT solution sets and is therefore a 2SAT solution set. If i is an unbalanced coordinate of S, q_i is constant for all $\mathbf{q} \in Q$. If $a \vee b = 1$ is a valid clause for $Q \cap S$, and involves the balanced coordinates of S, then $\bar{a} \vee \bar{b} = 1$ is also a valid clause, because translation by $\mathbf{c}$ preserves $Q \cap S$. But, these two clauses are logically equivalent to the single equation $a = \bar{b}$. Thus, the 2SAT system for $Q \cap S$ can be replaced by an equivalent combinatorial system. ∎

Definition. For $S \subseteq K_2^n$, the set of points $\mathbf{x} \in K_2^n$ minimizing $v(\mathbf{x}, S)$ is the *central cube* of S.

Apparently there are no known efficient methods for determining if the number of solutions to a 2SAT problem is odd, and whether a given point is in the central cube of the solution set. The problem of finding the number of solutions to a 2SAT problem is #P-complete, even in special cases, however [26].

Since T_3 closed spaces are not connected in general, it is difficult to think of them as generalizations of Euclidean convex sets. These sets do arise, though, in the following problem related to convexity. For $x \in \mathbf{R}$ let *sign*(x) be +1 if $x > 0$, –1 if $x < 0$, and undefined if $x = 0$. Given a real n-vector $\mathbf{x}$ with no zero coordinates, $\mathbf{sign}(\mathbf{x})$ is formed by taking *sign* of each coordinate.

Problem. Which sets $S \subseteq \{-1, +1\}^n$ have the property that for all integers $m > 0$, positive real numbers

$a_1, \ldots, a_m$, and $\mathbf{x}^1, \ldots, \mathbf{x}^m$ members of S, if $\mathbf{y} = a_1\mathbf{x}^1 + \cdots + a_m\mathbf{x}^m$ has no zero coordinates then $\mathbf{sign}(\mathbf{y}) \in S$?

For the moment say any set satisfying these conditions is a set with "property C". By a series of reductions we will show that the subsets of $\{-1, +1\}^n$ with property C are the T_3 closed sets. First, since no coordinate of $\mathbf{y}$ is exactly zero, each a_i can be replaced by an approximating positive rational number without changing $\mathbf{sign}(\mathbf{y})$. Next, multiply through by a common denominator to make each a_i a positive integer. Suppose the sum of the a_i's is even. In this case add one to a_1. This will change each coordinate of $\mathbf{y}$ by ±1, and since each coordinate was originally even, $\mathbf{sign}(\mathbf{y})$ is unchanged. Hence, it can be assumed that $a_1 + \cdots + a_m$ is odd.

Now, it can be assumed that each $a_i = 1$ because vector $\mathbf{x}^i$ occurring with coefficient a_i can be replaced with a_i copies of $\mathbf{x}^i$, each with coefficient one. This may increase m but it will not change the sum of the coefficients. Thus, it can be assumed that $\mathbf{y} = \mathbf{x}^1 + \cdots + \mathbf{x}^m$, and that m is odd. Note that $\mathbf{sign}(\mathbf{y}) = T_m(x^1, \ldots, x^m)$. Here T_m is applied to vectors whose elements are $-1, +1$-valued rather than $0, 1$-valued, but this is insignificant. Thus, S has property C if and only if it is T_m closed for *each* odd m. We have seen that each T_m combination can be obtained from T_3 combinations, so the sets with property C are simply the T_3 closed sets.

The following problem is probably a fruitful area for further research.

Unsolved Problem. What are the "lattice theoretic characteristics" of the lattice of T_3 closed subsets of K_2^n?

2.3. Basic Properties of Retracts

This section introduces an important subfamily of T_3 closed sets. In the following the subscript 3 will be omitted from this operation.

Definition. A *retract* is a T closed set of K_2^n which is connected.

The significance of the name "retract" will be explained in the section on contraction maps. Our main reference for retracts is a paper by Bandelt [27]. Our definition of retracts is very slightly different from the one in that paper, because we include the empty set and singletons as retracts. A few of our theorems correspond to previously known results.

Theorem 2.3.1. Any connected component of a T closed set is a retract.

Proof. Suppose Q is a component of a T closed set, S. Let $R = \{T(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mid \mathbf{x}, \mathbf{y}, \mathbf{z} \in Q\}$. Since $\mathbf{x} = T(\mathbf{x}, \mathbf{x}, \mathbf{x})$, $Q \subseteq R \subseteq S$. Call a sequence of points a *slow walk* if consecutive points have distance *at most* one. Let $\mathbf{x}^1, \ldots, \mathbf{x}^i$ $\mathbf{y}^1, \ldots, \mathbf{y}^j$ and $\mathbf{z}^1, \ldots, \mathbf{z}^k$ be any three slow walks in Q. Then,

$$T(\mathbf{x}^1, \mathbf{y}^1, \mathbf{z}^1), T(\mathbf{x}^2, \mathbf{y}^1, \mathbf{z}^1), \ldots, T(\mathbf{x}^i, \mathbf{y}^1, \mathbf{z}^1), T(\mathbf{x}^i, \mathbf{y}^2, \mathbf{z}^1), T(\mathbf{x}^i, \mathbf{y}^3, \mathbf{z}^1), \ldots$$

$$\ldots, T(\mathbf{x}^i, \mathbf{y}^j, \mathbf{z}^1), T(\mathbf{x}^i, \mathbf{y}^j, \mathbf{z}^2), T(\mathbf{x}^i, \mathbf{y}^j, \mathbf{z}^3), \ldots, T(\mathbf{x}^i, \mathbf{y}^j, \mathbf{z}^k)$$

is a slow walk in R. By picking i, j, k sufficiently large, the endpoints can be any three pairs of points in Q. Thus, two arbitrary points of R, $T(\mathbf{x}^1, \mathbf{y}^1, \mathbf{z}^1)$ and $T(\mathbf{x}^i, \mathbf{y}^j, \mathbf{z}^k)$ are connected by a slow walk in R. Thus, $Q = R$ and Q is therefore T closed. ⁝

Theorem 2.3.2. The intersection of a subcube of K_2^n and a retract is a retract.

Proof. It need only be shown that the intersection of a retract with any subcube of co-dimension one is a retract, because any proper subcube is the intersection of co-dimension one subcubes. Without loss of generality, assume the subcube is the set of points with first coordinate zero. Let R be a retract and let R_0 be the set of points of R with first coordinate zero. Note R_0 is T closed.

Let $\mathbf{x}, \mathbf{y} \in R_0$. There is a slow walk $\mathbf{x} = \mathbf{z}^1, \mathbf{z}^2, \ldots, \mathbf{z}^k = \mathbf{y}$ from $\mathbf{x}$ to $\mathbf{y}$ in R, as in the proof of the preceding theorem. Then,

$$\mathbf{x} = T(\mathbf{x}, \mathbf{y}, \mathbf{z}^1), T(\mathbf{x}, \mathbf{y}, \mathbf{z}^2), \ldots, T(\mathbf{x}, \mathbf{y}, \mathbf{z}^k) = \mathbf{y}$$

is a slow walk from $\mathbf{x}$ to $\mathbf{y}$ in R_0. Thus, R_0 is connected and T closed. ⁚

Corollary 2.3.3. Any nonempty retract contains its central cube.

Proof. Let R be a nonempty retract and Q its central cube. By Theorem 2.2.4, $R \cap Q$ is a nonempty combinatorial space. By Theorem 2, $R \cap Q$ is connected, because it is a retract. The only combinatorial spaces which are connected are cubes, so $R \cap Q$ is a cube. But, Theorem 2.2.4 asserts that Q is the smallest cube containing $R \cap Q$, so $Q = R \cap Q$. ⁚

Because all retracts are connected, Theorem 2 implies retracts are isometric. The *projection* of a retract to any nonempty subcube of K_2^n is also a retract because the projection of a T closed set to a subcube of K_2^n is a T closed and the projection of a connected set is connected. A related fact is that if R is a retract and $R \oplus \mathbf{t}$ is a translate of R by a unit vector, then $R \cup (R \oplus \mathbf{t})$ is a retract. The next proposition shows that $\cup$ can be replaced by $\cap$.

Proposition 2.3.4. If R is a retract and $|\mathbf{t}| = 1$, $R \cap (R \oplus \mathbf{t})$ is a retract.

Proof. Since both R and $R \oplus \mathbf{t}$ are T closed, and the intersection of T closed sets is T closed, $R \cap (R \oplus \mathbf{t})$ is T closed, so it only needs to be shown that $R \cap (R \oplus \mathbf{t})$ is connected. Assume $\mathbf{u}$ and $\mathbf{v}$ are both in $R \cap (R \oplus \mathbf{t})$. This is equivalent to saying $\mathbf{u}$, $\mathbf{v}$, $\mathbf{u} \oplus \mathbf{t}$ and $\mathbf{v} \oplus \mathbf{t}$ are all in R. Without loss of generality, assume $\mathbf{t}$ has its 1 in the first coordinate. If $\mathbf{u}$ has a 1 in the first coordinate, substitute $\mathbf{u} \oplus \mathbf{t}$ for $\mathbf{u}$. We can do the same for $\mathbf{v}$, so both $\mathbf{u}$ and $\mathbf{v}$ have first coordinate 0.

Since R is connected, let $\mathbf{u} = \mathbf{z}^1, \mathbf{z}^2, \ldots, \mathbf{z}^k = \mathbf{v}$ be a slow walk from $\mathbf{u}$ to $\mathbf{v}$ in R. Then $T(\mathbf{u}, \mathbf{v}, \mathbf{z}^i)$, $i = 1, 2, \ldots, k$ is a slow walk from $\mathbf{u}$ to $\mathbf{v}$ in R, with first coordinates all 0. Also, $T(\mathbf{u} \oplus \mathbf{t}, \mathbf{v} \oplus \mathbf{t}, \mathbf{z}^i)$ is a slow walk from $\mathbf{u} \oplus \mathbf{t}$ to $\mathbf{v} \oplus \mathbf{t}$ in R, with first coordinates all 1. Furthermore, $T(\mathbf{u} \oplus \mathbf{t}, \mathbf{v} \oplus \mathbf{t}, \mathbf{z}^i) = T(\mathbf{u}, \mathbf{v}, \mathbf{z}^i) \oplus \mathbf{t}$, so the points $T(\mathbf{u}, \mathbf{v}, \mathbf{z}^i)$ are in $R \oplus \mathbf{t}$. Thus, these points form a slow walk from $\mathbf{u}$ to $\mathbf{v}$ in $R \cap (R \oplus \mathbf{t})$. ⁚

The following theorem is counter-intuitive, because it implies that projection cannot increase the size of the largest subcube contained in a retract.

Theorem 2.3.5. If $R, Q \subseteq K_2^n$ with R a retract and Q a nonempty subcube of K_2^n and if the projection of R to Q is all of Q, then R contains a subcube parallel to Q.

Proof. (Induction on n). The claim is obvious for $n \leq 1$. Assume that the claim is true in K_2^m whenever $m < n$. Take $R \subseteq K_2^n$ to be a retract and suppose its projection to the cube Q is all of Q. If $\dim(Q) = n$, R is all of K_2^n, so it contains a cube parallel to Q. Suppose $\dim(Q) \leq n - 2$. Let H be an $(n-1)$-dimensional cube containing Q. Since $Q = \pi_Q(R) = \pi_Q(\pi_H(R))$, the retract $\pi_H(R)$ projects to cover all of Q. Then, by the induction hypothesis $\pi_H(R)$ contains a subcube, Q_1, parallel to Q. Now let $\hat{Q} = \pi_H^{-1}(Q_1)$. By Theorem 2, $\hat{R} = R \cap \hat{Q}$ is a retract. Since $\dim(\hat{Q}) \leq n - 1$, we may again use the induction hypothesis to say $\hat{R}$ contains a subcube parallel to Q_1. Thus, R will contain a subcube parallel to Q.

We now must prove the statement of the theorem when $\dim(Q) = n - 1$. Without loss of generality, assume Q is the subset of K_2^n having first coordinate 0. Let U be the set of points of R^c having first coordinate 0 and V be the set of points of R^c having first coordinate 1. We would like to show that either U or V is empty. Assume the contrary and let $\mathbf{u} \in U$, $\mathbf{v} \in V$ with $d(\mathbf{u}, \mathbf{v})$ minimal. All points in $I(\mathbf{u}, \mathbf{v})$, except $\mathbf{u}$ and $\mathbf{v}$, must be in R since anything else would contradict minimality of $d(\mathbf{u}, \mathbf{v})$.

Case i) $d(\mathbf{u}, \mathbf{v}) = 1$. This would imply $u_i = v_i$ for $i > 1$. Then, $\pi_Q(R)$ does not contain $\mathbf{u}$, a contradiction because $\mathbf{u} \in Q$.

Case ii) $d(\mathbf{u}, \mathbf{v}) = 2$. Then, $I(\mathbf{u}, \mathbf{v})$ is a 2-cube meeting R in two nonadjacent points, contradicting Theorem 2.

Case iii) $d(\mathbf{u}, \mathbf{v}) \geq 3$. Then, $\mathbf{u}$ has at least three neighbors $\mathbf{z}^1$, $\mathbf{z}^2$, $\mathbf{z}^3$ in $I(\mathbf{u}, \mathbf{v})$. These three points are therefore in R, but then $T(\mathbf{z}^1, \mathbf{z}^2, \mathbf{z}^3) = \mathbf{u}$ must also be in R, a contradiction.

In all cases a contradiction is obtained, so U or V is empty, and R therefore contains a subcube parallel to Q. ■

The above result can be expressed more concretely with the following example, where $\dim(Q) = 2$. Writing vectors as words, suppose $00\mathbf{a}$, $01\mathbf{b}$, $10\mathbf{c}$ and $11\mathbf{d}$ are all vectors in some retract. By the theorem there is a $\mathbf{z}$ such that $00\mathbf{z}$, $01\mathbf{z}$, $10\mathbf{z}$ and $11\mathbf{z}$ are all vectors in the retract.

We have seen from Theorem 1 that the solution set of a 2SAT problem in general produces many retracts - its connected components. Now it will be shown that by eliminating "equivalent coordinates" there is a way to derive a single retract from a T closed set. The retract will only be unique up to isometries, however.

Definition. Given $S \subseteq K_2^n$, a coordinate i is said to be *degenerate* if s_i is the same for each $\mathbf{s} \in S$. Two coordinates i and j are said to be *equivalent* if either $s_i = s_j$ for each $\mathbf{s} \in S$ *or* $s_i \neq s_j$ for each $\mathbf{s} \in S$.

Note that any two degenerate coordinates are equivalent and that any coordinate equivalent to a degenerate coordinate is itself degenerate. Equivalence of coordinates is an equivalence relation. Given any T closed set we may "eliminate" the degenerate coordinates, by restriction to a cube whose directions are the nondegenerate coordinates. If two nondegenerate coordinates are equivalent the second one can be eliminated by projection to a cube of co-dimension 1. All equivalent pairs can be eliminated in this way, resulting in a new T closed set which preserves the "essential" information about the original set. For example, the resulting set and the original set have the same cardinality. The next theorem shows that the resulting set is a retract.

Theorem 2.3.6. A T closed set is a retract if and only if it does not have two distinct nondegenerate coordinates which are equivalent.

Proof. Let S be T closed. Suppose the first and second coordinates are equivalent and nondegenerate. There are points of the form $(0, 0, \mathbf{a})$ and $(1, 1, \mathbf{b})$ in S *or* there are points of the form $(0, 1, \mathbf{c})$ and $(1, 0, \mathbf{d})$. The first of these cases holds when s_1 always equals s_2 and the second case holds when they are always unequal. In either case the projection of S to any subcube generated by the first two coordinates is disconnected, so that S is disconnected and therefore not a retract.

To prove the second half, assume S is T closed with no two equivalent distinct, nondegenerate coordinates. Suppose S is not connected. Select $\mathbf{x}$ and $\mathbf{y}$ from S such that $d(\mathbf{x}, \mathbf{y})$ is minimized, subject to $\mathbf{x}$ and $\mathbf{y}$ being in different components of S. By application of isometry it can be assumed that $\mathbf{x} = \mathbf{0}$ and $y_1 = y_2 = 1$. The second assumption holds because $d(\mathbf{x}, \mathbf{y}) \geq 2$. Since coordinates 1 and 2 are not degenerate and not equivalent to each other, there exists $\mathbf{z} \in S$ such that $z_1 \neq z_2$. Let $\mathbf{u} = T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathbf{y} \wedge \mathbf{z}$ (we use $\wedge$ to denote coordinatewise conjunction of 0-1 vectors), so

$$d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x}, \mathbf{u}) + d(\mathbf{u}, \mathbf{y}) \quad . \qquad (*)$$

Since $u_1 = z_1$ and $u_2 = z_2$, $\mathbf{u}$ is not equal to either $\mathbf{x}$ or $\mathbf{y}$. Hence $d(\mathbf{x}, \mathbf{u}) \geq 1$ and $d(\mathbf{u}, \mathbf{y}) \geq 1$. Either $\mathbf{x}$ or $\mathbf{y}$ is in a different component than $\mathbf{u}$. By (*), $d(\mathbf{x}, \mathbf{u})$ and $d(\mathbf{y}, \mathbf{u})$ are each less than $d(\mathbf{x}, \mathbf{y})$. Note $\mathbf{u}$ can't be in both $\mathbf{x}$'s and $\mathbf{y}$'s component of S. Thus, one of the pairs $\mathbf{x}$, $\mathbf{u}$ or $\mathbf{y}$, $\mathbf{u}$ contradicts the minimality assumption. ■

Corollary 2.3.7. For every k, there is a polynomial time algorithm to determine if the conjunction of a 2SAT system and k $GF(2)$-linear equations is consistent and if so provides a solution.

Proof. (Induction on k). First, it is clear that if $k = 0$, the 2SAT system can be solved in polynomial time. For $k > 1$, first check to see that the 2SAT part is consistent, and if so produce a solution $\mathbf{x}$. If $\mathbf{x}$ should happen to satisfy all $GF(2)$-linear equations, we can stop; otherwise assume $\mathbf{x}$ does not satisfy all equations.

Now, determine all pairs of equivalent coordinates, for the solution set of the 2SAT problem. A straightforward way to tell if i and j are equivalent is to look for solutions to the 2SAT problem with the additional constraints $x_i = \alpha$ and $x_j = \beta$. From the set of α, β pairs which produce consistent systems, it can be determined if the coordinates are equivalent. If $i < j$ and i and j are equivalent, eliminate x_j from the 2SAT and $GF(2)$-linear equations, by replacing each occurrence of x_j with x_i or $\bar{x}_i$, depending on the type of equivalence. Do this for all equivalent pairs. By Theorem 6, the solution set to the 2SAT part can now be described as a retract, say R.

The point $\mathbf{x}$ corresponds to some point in R, and we will also call this point $\mathbf{x}$. Suppose that in R there is a point $\mathbf{y}$ which does solve all the $GF(2)$-linear equations. Since retracts are connected, there is a path from $\mathbf{x}$ to $\mathbf{y}$ in R. At some point $\mathbf{z}$ on this path not all $GF(2)$-linear equations are satisfied, but the next point $\mathbf{z}\oplus\mathbf{t}$, does satisfy all of them. Since $|\mathbf{t}| = 1$, there are at most n possible vectors $\mathbf{t}$, so we will proceed by trying all possible $\mathbf{t}$'s.

Let $\mathbf{t} = (1, 0, \ldots, 0)$, since all other cases are similar. Perform a Gaussian elimination on the $GF(2)$-linear system so that only the first equation involves x_1. This can be done as long as one of the original equations uses x_1. If no equations use x_1, it is not possible for $\mathbf{z}$ to violate some equation that $\mathbf{z}\oplus\mathbf{t}$ solves, so we can move on to the next value of $\mathbf{t}$. Assume, now that the first $GF(2)$-linear equation depends on x_1 and it is the only such equation.

By Proposition 4, $R\cap(R\oplus\mathbf{t})$ is a retract. A 2SAT system for this set is easily produced from the 2SAT system describing R, by converting all 2-clauses involving x_1 (or $\bar{x}_1$) to 1-clauses not involving x_1. For example, $x_1 \vee \bar{x}_3 = 1$ is replaced by $\bar{x}_3 = 1$. Now look for a member of $R\cap(R\oplus\mathbf{t})$ which solves the final $k-1$ $GF(2)$-linear equations. If $\mathbf{z}$ is such a solution, either $\mathbf{z}$ or $\mathbf{z}\oplus\mathbf{t}$ must also solve the first $GF(2)$-linear equation, giving a solution to the original problem. If no solution is found, we move on to the next value of $\mathbf{t}$.

The bound for the work grows by a factor of n each time k increases by 1. Thus, even though it is bounded by a polynomial for any fixed k, this method may be impractical for large k. ∎

2.4. Retracts Intersected with Balls

It was seen that by Theorem 2.3.2, every subcube intersects a retract in a connected set, so retracts are isometric sets. Let R be a retract, $\mathbf{x} \in R$ and $B(\mathbf{x}, s)$ be a ball of radius s about $\mathbf{x}$. By Proposition 1.5.3, since R is isometric, $R\cap B(\mathbf{x}, s)$ is connected, but in fact, $R\cap B(\mathbf{x}, s)$ is also isometric itself. To see this, assume $\mathbf{x} = \mathbf{0}$ (without loss of generality) and let $\mathbf{y}, \mathbf{z} \in R\cap B(\mathbf{0}, s)$. Then $T(\mathbf{0}, \mathbf{y}, \mathbf{z}) = \mathbf{y}\wedge\mathbf{z}$ is in R. Since R is isometric and $\mathbf{y}\wedge\mathbf{z} \le \mathbf{y}$ (we use $\le$ for vectors in the coordinatewise sense), there is a path in R from $\mathbf{y}$ to $\mathbf{y}\wedge\mathbf{z}$, along which the Hamming weight is strictly decreasing. Similarly, there is a path in R from $\mathbf{z}$ to $\mathbf{y}\wedge\mathbf{z}$. Joining the first path to the reverse of the second, we obtain a path in R from $\mathbf{y}$ to $\mathbf{z}$ of length $d(\mathbf{y}, \mathbf{y}\wedge\mathbf{z}) + d(\mathbf{z}, \mathbf{y}\wedge\mathbf{z}) = d(\mathbf{y}, \mathbf{z})$. Furthermore, every point on this path is in $B(\mathbf{0}, s)$.

Theorem 2.4.1. A set R is a retract if and only if for each integer $s \ge 0$ and $\mathbf{x} \in R$, $R\cap B(\mathbf{x}, s)$ is isometric.

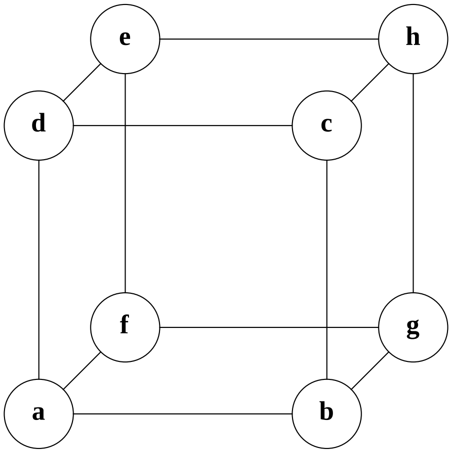
Proof. The "only if" part was proved in the discussion above. Assume the hypothesis of the "if" part. By taking s very large, we find R itself is isometric and therefore connected. It must only be shown that if $\mathbf{x}, \mathbf{y}, \mathbf{z} \in R$ then so is $T(\mathbf{x}, \mathbf{y}, \mathbf{z})$. Since everything so far has been invariant under isometry, it may be assumed that $\mathbf{x} = \mathbf{0}$. Suppose $T(\mathbf{0}, \mathbf{y}, \mathbf{z}) = \mathbf{y}\wedge\mathbf{z}$ is not always in R for $\mathbf{y}, \mathbf{z}$ in R. Select such a $\mathbf{y}$ and $\mathbf{z}$ with $|\mathbf{y}| + |\mathbf{z}|$ minimal. Interchange $\mathbf{y}$ and $\mathbf{z}$ if necessary so that $|\mathbf{y}| \le |\mathbf{z}|$. By hypothesis, $R\cap B(\mathbf{0}, |\mathbf{z}|)$ is isometric. Let $\mathbf{z}'$ be the first step in $R\cap B(\mathbf{0}, |\mathbf{z}|)$ on a shortest path from $\mathbf{z}$ to $\mathbf{y}$. Moving one step changes the Hamming norm by one, and because $\mathbf{z}'$ stays in the ball, $|\mathbf{z}'| = |\mathbf{z}| - 1$. Thus, $\mathbf{y}\wedge\mathbf{z}' = \mathbf{y}\wedge\mathbf{z}$. This contradicts the minimality of $|\mathbf{y}| + |\mathbf{z}|$, because $\mathbf{z}'$ can be used instead of $\mathbf{z}$. ∎

This theorem leads naturally to the following definition.

Definition. A set S is 0 *ball-isometric* if and only if it is connected. For integers $k \ge 1$, a set S is k *ball-isometric* if and only if $\mathbf{x} \in S$ implies that the intersection of S with any ball about $\mathbf{x}$ is $(k-1)$ ball-isometric.

We see immediately that k ball-isometric implies $(k-1)$ ball-isometric, and in K_2^n, 1 ball-isometric is the same as isometric and the 2 ball-isometric sets are the retracts. The question we now answer is: "Which retracts are 3 ball-isometric?"

The first observation to make is that any set containing a 3-cube is *not* 3 ball-isometric. Suppose there was a 3 ball-isometric $S \subseteq K_2^n$ which contains the 3-cube Q pictured below. By definition, $S\cap B(\mathbf{a}, 2)$ is a retract. Since the intersection of a cube with a retract is also a retract, $S\cap B(\mathbf{a}, 2)\cap Q$ is a retract. But, this is $Q\backslash\{\mathbf{h}\}$, which is not T closed, because $\mathbf{h} = T(\mathbf{c}, \mathbf{e}, \mathbf{g})$.



Theorem 2.4.2. The 3 ball-isometric sets in K_2^n are the retracts not containing a 3-cube.

Proof. It remains to show that if R is a retract not containing a 3-cube, R is 3 ball-isometric. Assume R is such a retract. Let $S \subseteq R$ be the intersection of R with some ball about a point of R. Since R is a retract, S is isometric. We wish to show that S is also a retract. In fact, the somewhat intricate proof to follow shows this using only that S is an isometric subset of a 3-cube-free retract, R.

Assuming that S is not a retract, there will be $\mathbf{x}, \mathbf{y}, \mathbf{z} \in S$ such that $\mathbf{u} = T(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is not in S. Pick $\mathbf{x}, \mathbf{y}, \mathbf{z}$ to have this property subject primarily to minimizing $d(\mathbf{u}, \mathbf{x}) + d(\mathbf{u}, \mathbf{y}) + d(\mathbf{u}, \mathbf{z})$ and secondarily to minimizing $\min(d(\mathbf{u}, \mathbf{x}), d(\mathbf{u}, \mathbf{y}), d(\mathbf{u}, \mathbf{z}))$. Without loss of generality, take $\mathbf{u} = \mathbf{0}$ and assume $|\mathbf{x}| \le |\mathbf{y}| \le |\mathbf{z}|$.

First, we will show that $|\mathbf{x}| = 1$. Assume $|\mathbf{x}| \ge 2$. Note that the sets of coordinates equal to 1 in $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ are mutually disjoint, because $\mathbf{0} = T(\mathbf{x}, \mathbf{y}, \mathbf{z})$. Since S is isometric, it has a path of length $|\mathbf{x}| + |\mathbf{y}|$ from $\mathbf{y}$ to $\mathbf{x}$. Let $\mathbf{y}'$ be adjacent to $\mathbf{y}$ on this path. Clearly, $|\mathbf{y}'| = |\mathbf{y}| \pm 1$. If $|\mathbf{y}'| = |\mathbf{y}| - 1$, we can replace $\mathbf{x}, \mathbf{y}, \mathbf{z}$ by $\mathbf{x}, \mathbf{y}', \mathbf{z}$, so the choice $\mathbf{x}, \mathbf{y}', \mathbf{z}$ contradicts the primary minimization assumption. Thus, $|\mathbf{y}'| = |\mathbf{y}| + 1$. Then $T(\mathbf{x}, \mathbf{y}', \mathbf{z}) = \mathbf{e} = \mathbf{x} \wedge \mathbf{y}'$, a weight one vector. If $\mathbf{e} \in S$, then since $T(\mathbf{e}, \mathbf{y}, \mathbf{z}) = \mathbf{0}$, a contradiction to the primary minimization assumption is found. Thus, $\mathbf{e} \notin S$. But, $T(\mathbf{x}, \mathbf{y}', \mathbf{z}) = \mathbf{e}$ and

$$d(\mathbf{e}, \mathbf{x}) + d(\mathbf{e}, \mathbf{y}') + d(\mathbf{e}, \mathbf{z}) = |\mathbf{x}| - 1 + |\mathbf{y}| + |\mathbf{z}| + 1 = |\mathbf{x}| + |\mathbf{y}| + |\mathbf{z}| ,$$

and $d(\mathbf{e}, \mathbf{x}) < |\mathbf{x}|$, so the choice $\mathbf{x}, \mathbf{y}', \mathbf{z}$ contradicts the secondary minimization constraint.

So, let $|\mathbf{x}| = 1$. Let $\mathbf{y}'$ be adjacent to $\mathbf{y}$ on a shortest path in S from $\mathbf{y}$ to $\mathbf{x}$. By the same reasoning as before, $|\mathbf{y}'| = |\mathbf{y}| + 1$. Since $\mathbf{y}' \in I(\mathbf{x}, \mathbf{y})$, $\mathbf{y}' = \mathbf{y} + \mathbf{x}$, so we have $\mathbf{y} + \mathbf{x} \in S$. Similarly, $\mathbf{z} + \mathbf{x} \in S$. The same reasoning applied to a shortest path from $\mathbf{y}$ to $\mathbf{z}$ shows that $\mathbf{y} + \mathbf{e} \in S$, for some $\mathbf{e}$ of weight one and $\mathbf{e} \le \mathbf{z}$. Thus, $T(\mathbf{y} + \mathbf{x}, \mathbf{z} + \mathbf{x}, \mathbf{y} + \mathbf{e}) = \mathbf{y} + \mathbf{x} + \mathbf{e} \in R$. Also, $\mathbf{x} + \mathbf{e} = T(\mathbf{0}, \mathbf{z} + \mathbf{x}, \mathbf{y} + \mathbf{x} + \mathbf{e}) = (\mathbf{z} + \mathbf{x}) \wedge (\mathbf{y} + \mathbf{x} + \mathbf{e}) \in R$. Let $\mathbf{x} + \mathbf{e} + \mathbf{f}$ be the first step on a shortest path in R from $\mathbf{x} + \mathbf{e}$ to $\mathbf{x} + \mathbf{e} + \mathbf{y}$. Thus, $|\mathbf{f}| = 1$ and $\mathbf{f} \le \mathbf{y}$. Now, we will show R contains the 3-cube $\{\mathbf{0}, \mathbf{x}, \mathbf{e}, \mathbf{f}, \mathbf{x} + \mathbf{e}, \mathbf{x} + \mathbf{f}, \mathbf{e} + \mathbf{f}, \mathbf{x} + \mathbf{e} + \mathbf{f}\}$. There are four elements of this set that have not yet been shown to be in R. These can all be obtained as T combinations of $\mathbf{0}$ with two other points of R, i.e., as the $\wedge$ of two points of R, as follows.

$$\mathbf{e} = \mathbf{z} \wedge (\mathbf{x} + \mathbf{e} + \mathbf{f})$$

$$\mathbf{f} = \mathbf{y} \wedge (\mathbf{x} + \mathbf{e} + \mathbf{f})$$

$$\mathbf{x} + \mathbf{f} = (\mathbf{x} + \mathbf{y}) \wedge (\mathbf{x} + \mathbf{e} + \mathbf{f})$$

$$\mathbf{e} + \mathbf{f} = (\mathbf{y} + \mathbf{e}) \wedge (\mathbf{x} + \mathbf{e} + \mathbf{f})$$

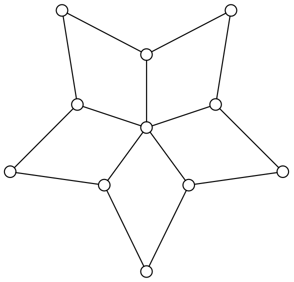
Thus, we have contradicted the assumption that R has no 3-cube. ∎

An immediate consequence of this result is that any 3 ball-isometric set, R, is also k ball-isometric, for any larger k. The intersection with any ball about a point of R must be 3-cube-free, because R has no 3-cubes. Thus, the intersection is always 3 ball-isometric so R is 4 ball-isometric. But, since any 3 ball-isometric set is 4 ball-isometric, R is 5 ball-isometric, and so on.

Unsolved Problem. To what extent do these theorems and proofs extend to arbitrary bipartite graphs?

Any isometric subset of K_2^n can be viewed as a type of bipartite graph, without reference to 0-1 vectors, since there is essentially only one way to fit such graphs isometrically into K_2^n. It is relatively easy to verify that any tree is a retract in K_2^n and that the Cartesian product of two retracts is another retract [27]. Thus, Cartesian products of any number of trees is a retract. An interesting fact [28] is that the only retracts which are regular graphs are the graphs of some n-cube.

The Cartesian product of any two trees is a 3-cube-free retract. The class of 3-cube-free retracts still includes a fair number of graphs. For example, the graph below is a 3-cube-free retract which is not contained in the product of two trees.



2.5. The Directed Graph and Associated Polyhedron

To any 2-clause, say $a \vee b = 1$, or $a \vee b$ for short, there are two implications $\bar{a}$ => b and $\bar{b}$ => a, each of which is equivalent to the 2-clause in the sense of Boolean logic. The 1-clause $a \vee a$ is equivalent to $\bar{a}$ => a. For any 2SAT system on the variables $x_1, \ldots, x_n$, there is an important directed graph [24], which we will call the *implication graph*. The vertices are the $2n$ literals $x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n$. For each 2-clause $y \vee z$, we put in the two edges $\bar{y} \rightarrow z$ and $\bar{z} \rightarrow y$. For 1-clauses of the form $y \vee y$ we put in the edge $\bar{y} \rightarrow y$. For clauses of the form $y \vee \bar{y}$, no edges are put in, because the clause is a tautology and can be removed from the 2SAT system to give an equivalent system.

We restate Theorem 1 of [24].

Theorem 2.5.1. A 2SAT system is on $n \geq 1$ variables is consistent if and only if the implication graph does not contain a directed cycle going through both a literal and its complement.

In terms of the implication graph, degenerate coordinates can be easily recognized.

Proposition 2.5.2. Given a consistent 2SAT system in variables $x_1, \ldots, x_n$, $n \geq 1$, coordinate i is degenerate on the solution set if and only if the implication graph has a directed path from x_i to $\bar{x}_i$, or from $\bar{x}_i$ to x_i.

Proof. If such directed paths do exist, then x_i => $\bar{x}_i$ or $\bar{x}_i$ => x_i are derivable by chaining implications equivalent to the clauses of the 2SAT system. These implications are equivalent to $x_i = 0$ and $x_i = 1$, respectively. Hence, the i^{th} coordinate is degenerate.

On the other hand, if the neither directed path exists, the system remains consistent when either the clause $x_i \vee x_i$, or the clause $\bar{x}_i \vee \bar{x}_i$ are added to the system, by the criterion of Theorem 1, so coordinate i is not degenerate. ∎

All degenerate coordinates can be removed easily from a consistent 2SAT system to obtain a smaller equivalent system, by removing all clauses which mention these coordinates. We next show that if a 2SAT system has no degenerate coordinates, the solution set is a retract precisely when there are no cycles in the implication graph, i.e., it is acyclic. Rather than prove this directly, a polyhedral result will be established concurrently, thus showing a connection between retracts and convexity.

Definition. Given a 2SAT system with $n \geq 1$ variables, $x_1, \ldots, x_n$ the *associated polyhedron* is the solution set of a system of linear inequalities in n real variables $u_1, \ldots, u_n$. The inequalities corresponding to each clause are as follows. Assume i and j are arbitrary with $i \neq j$.

2SAT	Polyhedron
$x_i \vee x_i$	$u_i > 0$
$\bar{x}_i \vee \bar{x}_i$	$-u_i > 0$
$x_i \vee \bar{x}_i$ or $\bar{x}_i \vee x_i$	no equation
$x_i \vee x_j$	$u_i + u_j > 0$
$x_i \vee \bar{x}_j$	$u_i - u_j > 0$
$\bar{x}_i \vee x_j$	$-u_i + u_j > 0$
$\bar{x}_i \vee \bar{x}_j$	$-u_i - u_j > 0$

The associated polyhedron is convex, being the intersection of half spaces. This polyhedron is constructed so that given any vector in the associated polyhedron, a 2SAT solution can be found by setting x_i to 1 if $u_i > 0$, x_i to 0 if $u_i < 0$, and x_i to either value if $u_i = 0$. For example, if $u_i + u_j > 0$ then either $u_i > 0$ or $u_j > 0$, so the clause $x_i \vee x_j$ will be satisfied. The associated polyhedron will be called *complete* if every solution to the 2SAT system can obtained by this conversion from some vector in the associated polyhedron.

Theorem 2.5.3. Let a 2SAT system in $n \geq 1$ variables have solution set with no degenerate coordinates. Then the following are equivalent.
A) The solution set is a retract.
B) The implication graph is acyclic.
C) The associated polyhedron is complete.

Proof.
A implies B. Consider a 2SAT system in $n \geq 1$ variables whose solution set has no degenerate coordinates. Suppose that the solution set is a retract, but that the graph has a directed cycle through distinct vertices representing the literals y and z. From the 2SAT equations we can derive y => z and z => y, and therefore, $y = z$ is true for every solution of the 2SAT system. If y and z are disjoint then the two coordinates involved are equivalent and the solution set is not a retract, a contradiction. If y and z are negations of each other $y = z$ never holds, so the solution set is empty and therefore all coordinates are degenerate, a contradiction.

B implies C. To prove this part we do not need nondegeneracy. Simply assume we have a 2SAT system, in variables $x_1, \ldots, x_n$, $n \geq 1$, with acyclic implication graph. Let **s** be any solution and let $\{z_1, \ldots, z_n\}$ be the n literals which are equal to 1 at **s**. Since the graph is acyclic, by Szpilrajn's theorem [29] on linear extensions of partial orders, the set can be ordered so that if $z_i \rightarrow z_j$ is an edge of the graph then $i < j$. Rearrange the names of the variables so that z_i involves variable x_i. Now, for each i, set u_i to i if $x_i = 1$ and set u_i to $-i$ if $x_i = 1$. If i and j are arbitrary indices with $i < j$ then $z_i \vee z_j$ and $\bar{z}_i \vee z_j$ are the only 2-clauses involving x_i and x_j which can be in the system, since $\bar{z}_i \vee \bar{z}_j$ implies **s** is not a solution and $z_i \vee \bar{z}_j$ would produce the edge $z_j \rightarrow z_i$ in the implication graph. In either of the two 2-clauses which are possible the left hand side of the corresponding u inequality evaluates to $j \pm i$, a positive number. The inequalities coming from 1-clauses are obviously satisfied. Thus, a point $\mathbf{u} = (u_1, \ldots, u_n)$ in the associated polyhedron has been found corresponding to **s**. Since this can be done for every such **s**, the polyhedron is complete.

C implies A. Nondegeneracy is not required for this part either. It will be shown that the set of solutions of the 2SAT problem which correspond to vectors in the associated polyhedron form a connected subset of

K_2^n. It then follows that if the polyhedron is complete the solution set is a retract. Let **r** and **s** be solutions of the 2SAT system which can be derived from the vectors in the polyhedron **u** and **v**, respectively. Because the polyhedron is topologically open, **u** and **v** can be perturbed slightly so that no coordinates are exactly zero. Also, it can be assumed that **u** and **v** are in ‘‘general position’’ so that on any point on the segment between them at most one coordinate is zero. As a point moves along the segment from **u** to **v** the point stays in the polyhedron and the solution to the 2SAT problem which it may represent changes by at most one coordinate at a time. Hence **r** and **s** are connected by a path in the solution set. ∎

Note: Suppose arbitrary positive scale factors are introduced into the inequalities for the associated polyhedron. That is, suppose for some inequality, say $u_i - u_j > 0$, we substitute instead the inequality $\alpha u_i - \beta u_j > 0$, for some positive α and β. We may do this for all inequalities, using different α and β for each inequality. Surprisingly, if the implication graph is acyclic, this modified polyhedron is still complete. In the proof of ‘‘B implies C’’ above, we set u_i to be $\pm i$. Instead, set u_i to be $\pm\gamma^i$, where γ is twice the ratio of the maximum of all α’s and β’s to the minimum of all α’s and β’s, i.e., γ is some very large number. Then the resulting vector represents the 2SAT solution **s** in the modified polyhedron. The fact that the modified polyhedron is still complete will be used in the next chapter.

2.6. Contraction Mappings

Definition. If $\mathbf{X}$ is a metric space a mapping $F: \mathbf{X} \to \mathbf{X}$ is a *contraction mapping* if for any $\mathbf{x}, \mathbf{y} \in \mathbf{X}$, $d(F(\mathbf{x}), F(\mathbf{y})) \le d(\mathbf{x}, \mathbf{y})$.

Clearly, the contraction mappings form a semigroup under composition, and this semigroup contains the isometry group. This section deals only with contractions of K_2^n and their relevance to T closed sets.

Proposition 2.6.1. The set of fixed points of a contraction mapping is T closed.

Proof. Let $\mathbf{x}, \mathbf{y}, \mathbf{z}$ be fixed points of a contraction F. Let $s(\mathbf{u}) = d(\mathbf{u}, \mathbf{x}) + d(\mathbf{u}, \mathbf{y}) + d(\mathbf{u}, \mathbf{z})$. Since F is a contraction,

$$d(F(\mathbf{u}), F(\mathbf{x})) + d(F(\mathbf{u}), F(\mathbf{y})) + d(F(\mathbf{u}), F(\mathbf{z})) \le s(\mathbf{u}),$$

$$d(F(\mathbf{u}), \mathbf{x}) + d(F(\mathbf{u}), \mathbf{y}) + d(F(\mathbf{u}), \mathbf{z}) \le s(\mathbf{u}),$$

$$s(F(\mathbf{u})) \le s(\mathbf{u})\,.$$

Recall that $\mathbf{u} = T(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is the unique point minimizing $s(\mathbf{u})$. Thus, F fixes $T(\mathbf{x}, \mathbf{y}, \mathbf{z})$. ∎

In the following we will use iterated composition of maps, for which the superscript notation will be used. Thus, a map F is idempotent if and only if $F = F^2$.

Proposition 2.6.2. The image of an idempotent contraction is a retract.

Proof. Let $F: K_2^n \to K_2^n$ be an idempotent contraction. The set of fixed points of F is exactly $F(K_2^n)$, the image of F, so by Proposition 1, the image is T closed. To show $F(K_2^n)$ is connected, let $\mathbf{x}^1, \ldots, \mathbf{x}^m$ be a slow walk in K_2^n with $\mathbf{x}^1, \mathbf{x}^m \in F(K_2^n)$. Then,

$$\mathbf{x}^1 = F(\mathbf{x}^1), F(\mathbf{x}^2), \ldots, F(\mathbf{x}^{m-1}), F(\mathbf{x}^m) = \mathbf{x}^m$$

is a slow walk in $F(K_2^n)$, connecting $\mathbf{x}^1$ with $\mathbf{x}^m$ in $F(K_2^n)$. ∎

If G is any map from a finite set to itself there is an idempotent map derivable from G. The sequence $G, G^2, G^3, \ldots$ must eventually contain some map twice, because there are only a finite number of maps from the finite set to itself. Let $i > 0$ be minimal such that G^i appears elsewhere in the sequence, and let $q > 0$ be minimal such that $G^{i+q} = G^i$. Finally, take k to be the minimal positive integer such that $kq \ge i$. Letting $kq = i + j$ gives,

$$G^{2kq} = G^{j+(k-1)q} G^{i+q} = G^{j+(k-1)q} G^{i} = G^{j+(k-2)q} G^{i+q} = \ldots = G^{j} G^{i} = G^{kq} \ .$$

Hence, G^{kq} is idempotent. The set of fixed points of G^{kq} can be described in two ways. For example, it is the set of points fixed by at least one of the maps $G, G^2, \ldots$. Also, it is the *stable image* of G in that it is the intersection of the images of all the G^t, $t = 1, 2, \ldots$. When G is a contraction on K_2^n, so is G^{kq} and we have the following corollary of Proposition 2.

Corollary 2.6.3. The stable image of any contraction is a nonempty retract.

The set of fixed points of a contraction of *Euclidean* space is convex. Thus, Proposition 2 shows that retracts of K_2^n are one possible way to define "convex" sets in K_2^n.

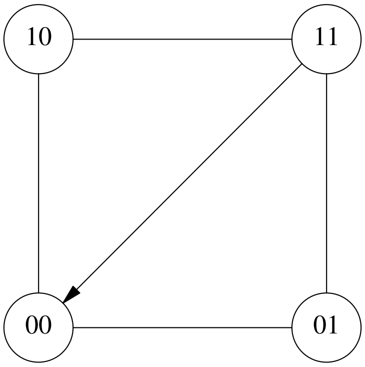
Proposition 2 also explains where the name "retract" comes from. In topology a point set is a retract of a topological space whenever it is the image of an idempotent continuous mapping of the space. Here contractions replace continuous mappings. Topologists employ concepts stronger than retracts such as "deformation retracts". We claim that any reasonable extension of these definitions to K_2^n still gives the same family of sets we have been calling retracts. Rather than explicitly stating these generalizations, we will show next how any retract (with more than one point) can be obtained as the image of an idempotent contraction and further that the mapping obtained has special properties.

Definition. Given a 2-clause C equivalent to $(x_i = a) \vee (x_j = b)$ the *pinch map* $P_C \colon K_2^n \to K_2^n$ is given by

$$P_C(\mathbf{x}) = \begin{cases} \mathbf{x} & \text{if } (x_i = a) \vee (x_j = b) \\ \mathbf{x} \oplus \mathbf{e}^i \oplus \mathbf{e}^j & \text{otherwise,} \end{cases}$$

where $\mathbf{e}^k$ denotes the unit vector with a 1 in position k.

Each pinch map is an idempotent contraction map whose image is the solution set of the 2-clause. The pinch map only operates on two coordinates of a vector, so it can be viewed by its action on a 2-cube. If the clause C is $\bar{x}_1 \vee \bar{x}_2$, the map P_C on K_2^2 takes $(1,1)$ to $(0,0)$ and fixes all other points.



A sufficient condition for a composition of pinch maps to be idempotent will now be developed. First, form the implication graph of the clauses. The *transitive closure* of a directed graph is found by adding the edge $\mathbf{y} \to \mathbf{z}$ every time there is a directed path from $\mathbf{y}$ to $\mathbf{z}$ in the original graph. A directed graph is said to be *transitively closed* if there are no new edges in the transitive closure.

Proposition 2.6.4. If $C_1, \ldots, C_m$, $m > 1$ are distinct 2-clauses and for each integer k such that $1 \le k \le m$, the implication graph generated by the set of clauses $C_1, \ldots, C_k$ is transitively closed, then $P_{C_m} \cdots P_{C_2} P_{C_1}$ is idempotent and the set of fixed points is the solution set of all m clauses.

Proof. Note, the hypothesis that the graph is transitively closed implies that there are no directed cycles. A directed cycle through a literal y would mean the loop $y \to y$ is in the transitive closure, but edges $y \to y$ are never in the implication graph. Similarly, there can be no directed path from a literal to its negation, because the C_i are not 1-clauses.

The proof is by induction. Clearly the statement of the theorem is true for $m = 1$. Assume it is true for all $m < r$. Let $F = P_{C_{r-1}} \cdots P_{C_1}$ and let S be the image of F. Let $C_1, \ldots, C_r$ satisfy the hypothesis of the theorem. Since P_{C_r} and F are themselves idempotent, $P_{C_r}F$ can be shown to be idempotent by showing that $P_{C_r}(S) \subseteq S$.

Suppose C_r is equivalent to $y \Rightarrow z$, $\mathbf{s} \in S$ and that $P_{C_r}(\mathbf{s}) = \mathbf{t}$ and $\mathbf{t} \notin S$. Since $\mathbf{s}$ doesn't satisfy C_r, $y(\mathbf{s}) = 1$ while $z(\mathbf{s}) = 0$. Thus, $y(\mathbf{t}) = 0$ and $z(\mathbf{t}) = 1$. Now, $\mathbf{t}$ makes false some previous 2-clause, C_j, which $\mathbf{s}$ satisfies. Since $\mathbf{t}$ differs from $\mathbf{s}$ in only two coordinates, C_j is equivalent to $z \Rightarrow u$ for some literal u with $u(\mathbf{t}) = 0$, or C_j is equivalent to $v \Rightarrow y$ with $v(\mathbf{t}) = 1$. It can be assumed that the first case holds, because the second can be made equivalent to it by using the contrapositive forms of $y \Rightarrow z$ and $v \Rightarrow y$.

Assuming $C_j \equiv (z \Rightarrow u)$, the transitive closure of the directed graph on all r clauses contains the edge $y \longrightarrow u$. But, by the hypothesis of transitive closure, $y \longrightarrow u$ must be equivalent to some C_i, $i < r$. By transitive closure and the comments made at the beginning of the proof, u is disjoint from y and z, i.e., involves a variable distinct from both y and z. Thus, $u(\mathbf{s}) = u(\mathbf{t})$. However, $u(\mathbf{t}) = 0$ and $y(\mathbf{s}) = 1$ and C_i has value one for $\mathbf{s}$. This implies $u(\mathbf{s}) = 1$, a contradiction. Therefore, $P_{C_r}F$ is idempotent.

Finally, it must be shown that the image of $G = P_{C_r}F$ is the solution set of the conjunction of all r clauses. Since the image of G is contained in S and any point in the image of P_{C_r} satisfies C_r, all points in the image of G satisfy all clauses. On the other hand, if a point $\mathbf{x}$ satisfies all r clauses, $P_{C_i}(\mathbf{x}) = \mathbf{x}$ for each $i \leq r$, so $G(\mathbf{x}) = \mathbf{x}$ and $\mathbf{x}$ is in the image. This completes the induction. ■

Theorem 2.6.5. If $R \subseteq K_2^n$ is a retract and $|R| \geq 2$, then for some $m \geq 0$ there is a collection of m distinct 2-clauses $C_1, \ldots, C_m$ such that for each $0 \leq k \leq m$, $P_{C_k} \cdots P_{C_1}$ is idempotent with set of fixed points equal to the solution set of the system $C_1, \ldots, C_k$. In addition, R is the solution set of the system $C_1, \ldots, C_m$.

Proof. The proof is in two parts. First we show the theorem is true in the case R is a subcube. Thus, let Q be any subcube of K_2^n, $|Q| \geq 2$. If Q is n-dimensional then the statement of the theorem is trivially true by letting $m = 0$. Assume Q is the set of all points with $x_1 = 0$, let's say $C_1 \equiv \bar{x}_1 \vee x_n$ and $C_2 \equiv \bar{x}_1 \vee \bar{x}_n$. Note $n \neq 1$ because $|Q| \geq 2$. This will meet the requirements with $m = 2$, and a similar pair of clauses will work whenever Q has co-dimension one.

If Q is smaller, a sequence of pairs of pinch maps will reduce the dimension of the image by one each step. If Q has co-dimension k an isometry can be applied to make Q the set of all points with $x_1 = x_2 = \ldots = x_k = 0$. Then the requirements of the theorem are met with $m = 2k$ and $C_1 \equiv \bar{x}_1 \vee x_n$, $C_2 \equiv \bar{x}_1 \vee \bar{x}_n$, $C_3 \equiv \bar{x}_2 \vee x_n$, $C_4 \equiv \bar{x}_2 \vee \bar{x}_n$,..., $C_{2k-1} \equiv \bar{x}_k \vee x_n$, $C_{2k} \equiv \bar{x}_k \vee \bar{x}_n$.

Assume R is a retract which is not a cube and R has no degenerate coordinates. Form the 2SAT system consisting of all 2-clauses which are true on R. Since there are no degenerate coordinates there are no nontrivial 1-clauses which are true for R. Thus, Theorem 2.2.1 shows that R is the solution set of the system. Theorem 2.5.3 shows that the implication graph of the system is acyclic. Any edge in the transitive closure of the implication graph corresponds to a 2-clause which holds on R, because the corresponding implication is derivable from the original implications. Thus, the implication graph is transitively closed.

For any edge $y \longrightarrow z$ in the implication graph let the *length* of that edge be the length of the *longest* directed path from y to z. The lengths of $y \longrightarrow z$ and $\bar{z} \longrightarrow \bar{y}$ are the same because the contrapositive of each component of a directed path results in another directed path with the same length. Hence, we may let the length of a clause of the system be the length of either of its corresponding edges. Let m be the number of clauses in the system and order the clauses so that their lengths are nonincreasing. If $u \longrightarrow v$ and $v \longrightarrow w$ are edges in the implication graph, then the length of $u \longrightarrow w$ is larger than the lengths of each of $u \longrightarrow v$ and $v \longrightarrow w$. Thus, the implication graph formed by the first k clauses is transitively closed. The conditions of Proposition 4 are met, so the statement of the theorem is established for this case.

The only remaining case is when R is a retract with degenerate coordinates and R is not a cube. This is handled by forming the smallest subcube, Q, containing R. First, apply pinch maps to map K_2^n onto Q. Then, apply maps which take Q onto R. The combined sequence satisfies the conditions of the theorem. ■

Why is $|R| \geq 2$ required? If $\mathbf{x}$ and $\mathbf{y}$ are adjacent, $P_C(\mathbf{x})$ and $P_C(\mathbf{y})$ are adjacent for any 2-clause, C. Thus, compositions of pinch maps are not only contractions, but *unit distance preserving*. Thus, if G is a composition of pinch maps and $n \ge 1$, then $|G(K_2^n)| \ge 2$.

2.7. Finding Short Cycles of Contractions

In this section we eventually show that there is a polynomial time algorithm for locating fixed points of contractions of K_2^n. First, we establish that contractions must have short cycles, that is, there is a point which comes back to itself after a small number of iterations of the contraction. We begin with a result not about contractions, but about affine mappings. A more general result appeared in [30].

Proposition 2.7.1. Any $GF(2)$-affine transformation from K_2^n, $n \ge 1$, to itself has a point with period 2^j for some $2^j \le 2n$.

Proof. For the duration of this proof only, let + stand for ⊕, addition modulo two. Let an affine map on K_2^n be $G(\mathbf{x}) \equiv A\mathbf{x} + \mathbf{c}$, where A is a linear operator and $\mathbf{c}$ is a constant. This is the standard representation of any affine map. A bit of characteristic two linear algebra shows

$$G^{2^j}(\mathbf{x}) + \mathbf{x} = A^{2^j}\mathbf{x} + \mathbf{x} + (A^{2^j-1} + \cdots + A + I)\mathbf{c}$$

$$= (A^{2^j} + I)\mathbf{x} + (A+I)^{2^j-1}\mathbf{c} \;\; = (A+I)^{2^j-1}((A+I)\mathbf{x} + \mathbf{c}), \qquad (*)$$

where I denotes the identity operator. From linear algebra, the null space of $(A+I)^m$ stabilizes for $m \ge n$, to some vector space, say Z. Then, $A+I$ induces a nonsingular operator on the vector space K_2^n modulo Z. Hence, there is a solution $\mathbf{x}$ to $(A+I)\mathbf{x} + \mathbf{c} = \mathbf{0}$ (mod Z). As long as $2^j - 1 \ge n$, then by (*), there is an $\mathbf{x} \in K_2^n$ such that $G^{2^j}(\mathbf{x}) + \mathbf{x} = \mathbf{0}$. For any $n \ge 1$, there is a j such that $2^j \le 2n$ and $2^j > n$, or $2^j - 1 \ge n$. □

Since any isometry of K_2^n is an affine transformation, we have shown that isometries have short cycles. In fact, for some values of n there exist isometries with shortest period $2n$. Let n be a power of 2, and define F on K_2^n as follows. To form $F(\mathbf{x})$, cyclically rotate the coordinates of $\mathbf{x}$ by one position and then complement the first coordinate. It can be shown that every point of K_2^n has period $2n$.

Lemma 2.7.2. If a contraction F on K_2^n permutes the elements of a set S, then $F(Q) \subseteq Q$, where Q is the central cube of S.

Proof. Recall that the central cube of S is the set of all points $\mathbf{x} \in K_2^n$ which minimize $\nu(\mathbf{x}, S)$. To simplify notation we will sometimes use $F\mathbf{x}$ to denote $F(\mathbf{x})$. Since F is a contraction,

$$\sum_{\mathbf{s} \in S} d(F\mathbf{x}, \mathbf{s}) = \sum_{\mathbf{s} \in S} d(F\mathbf{x}, F\mathbf{s}) \le \sum_{\mathbf{s} \in S} d(\mathbf{x}, \mathbf{s}) \text{ , so } \quad \nu(F\mathbf{x}, S) \le \nu(\mathbf{x}, S) \,.$$

Thus, $F(Q) \subseteq Q$. □

Theorem 2.7.3. If F is a contraction of K_2^n, $n \ge 1$, there exists j, $2^j \le 2n$, such that some point has period 2^j under F.

Proof. Let S be the stable image of F. Cor. 2.6.3 states that S is a nonempty retract. Also, F permutes the elements of S. Let Q be the central cube of S, which is contained in S by Cor. 2.3.3. By Lemma 2, $F(Q) \subseteq Q$, so in fact, F permutes the elements of Q. Thus, some power of F is the compositional inverse of F restricted to Q. Since both F and its inverse are contractions of Q, F is an isometry of Q to itself. Thus, by Proposition 1, F has a short cycle, since Q is isometric to some K_2^m. □

Suppose we are given a contraction map F in the form of an *oracle*, in the sense that when presented with a point $\mathbf{x}$ the oracle returns $F(\mathbf{x})$. We wish to find a short cycle of F using no more information about F than provided by the oracle. This requires developing a few more ideas about K_2^n.

One fact we will use is that the lattice of T closed sets in K_2^n has a height bounded by a polynomial in n. That is, let $S_0 \subset S_1 \subset \cdots \subset S_k$ be a strictly ascending chain of T closed sets. In their 2SAT descriptions, the clauses which are true for S_{i+1} are a proper subset of those true for S_i. Since there are $2n^2$ possible 1- or 2-clauses, $k \le 2n^2$. In the following $h = h(n)$ will be the largest possible value of k, for which there is a strictly ascending chain of T closed sets $S_0 \subset S_1 \subset \cdots \subset S_k$. We will need only the bound $h \le 2n^2$.

For any set S, let the T *closure* of S, denoted $Cl(S)$, be the intersection of all T closed sets containing S. Since every component of a T closed set is a retract, if S is connected, $Cl(S)$ is a retract.

If S is a set such that $d(F\mathbf{x}, F\mathbf{y}) = d(\mathbf{x}, \mathbf{y})$ whenever $\mathbf{x}, \mathbf{y} \in S$, we will say F is *distance preserving* on S.

Proposition 2.7.4. If F is a contraction of K_2^n which is distance preserving on a connected set S, then F is distance preserving on $Cl(S)$ and $T(F\mathbf{x}, F\mathbf{y}, F\mathbf{z}) = F(T(\mathbf{x}, \mathbf{y}, \mathbf{z}))$, for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in S$.

Proof. Since connected sets are rigid (Theorem 1.3.1), there is an isometry H of K_2^n such that the composite map $G = HF$ is the identity on S. Since the set of fixed points of a contraction is T closed (Proposition 2.6.1), G is the identity on all of $Cl(S)$. Since G is distance preserving on $Cl(S)$ and H is an isometry $F = H^{-1}G$ is distance preserving on $Cl(S)$.

Since the T operation is doubly symmetric, it commutes with the isometry H. Thus, for $\mathbf{x}, \mathbf{y}, \mathbf{z} \in Cl(S)$,

$$HF(T(\mathbf{x}, \mathbf{y}, \mathbf{z})) = T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(HF\mathbf{x}, HF\mathbf{y}, HF\mathbf{z}) = HT(F\mathbf{x}, F\mathbf{y}, F\mathbf{z}) .$$

Apply H^{-1} to far left and far right sides to obtain $FT(\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(F\mathbf{x}, F\mathbf{y}, F\mathbf{z})$, as required. ∎

Our goal is to use the F oracle to produce a retract R, where F is distance preserving and $F(R) \subseteq R$. Then R contains a short cycle of F, by the same reasoning as in the proof of Theorem 3. We begin by showing how to produce sets where F is distance preserving.

Proposition 2.7.5. For any contraction F on K_2^n and nonempty set $S \subseteq K_2^n$, F is distance preserving on $F^i(S)$, for some $i \le \nu(S)$.

Proof. Recall that $\nu(S)$ is the sum of the distances of all unordered pairs of points in S. For $\mathbf{x}, \mathbf{y}$ any such pair, $d(F^i\mathbf{x}, F^i\mathbf{y})$, $i = 0, 1, 2, \ldots$, is a nonincreasing sequence. Thus, $\nu(F^i(S))$ is also a nonincreasing sequence. Therefore, for some $i \le \nu(S)$, $\nu(F^i(S)) = \nu(F^{i+1}(S))$. This requires $d(F^i\mathbf{x}, F^i\mathbf{y}) = d(F^{i+1}\mathbf{x}, F^{i+1}\mathbf{y})$, for every $\mathbf{x}, \mathbf{y} \in S$. ∎

To continue with the problem of finding a short cycle, select any point $\mathbf{x}$ and find $F(\mathbf{x})$. If $\mathbf{x} = F(\mathbf{x})$, we can stop, having found a short cycle. Otherwise form the set $U = \{\mathbf{x}, \mathbf{y}^1, \mathbf{y}^2, \ldots, \mathbf{y}^m\}$, such that

$$\mathbf{x}, \mathbf{y}^1, \mathbf{y}^2, \ldots, \mathbf{y}^m, F(\mathbf{x})$$

forms a shortest path from $\mathbf{x}$ to $F(\mathbf{x})$. Note U does not include $F(\mathbf{x})$. Define $U^i = F^i(U)$ and let $W = U \cup U^1 \cup \cdots \cup U^h$ and then define $W^i = F^i(W)$. By Proposition 5, there is some $j \le \nu(W)$, such that F is distance preserving on W^j. Since there can be at most h members in a strictly ascending chain of nonempty T closed sets, there is a k, $0 \le k \le h$, such that

$$Cl(U^j \cup U^{j+1} \cup \cdots \cup U^{j+k}) = Cl(U^j \cup \cdots \cup U^{j+k+1}) .$$

Let $V = U^j \cup \cdots \cup U^{j+k}$ and $R = Cl(V)$ will be a retract which will satisfy our requirements. First, V is connected because its elements can be formed into the following slow walk.

$$F^j\mathbf{x}, F^j\mathbf{y}^1, \ldots, F^j\mathbf{y}^m, F^{j+1}\mathbf{x}, F^{j+1}\mathbf{y}^1, \ldots, F^{j+1}\mathbf{y}^m, F^{j+2}\mathbf{x}, \ldots, F^{j+3}\mathbf{x}, \ldots, F^{j+k}\mathbf{x}, \ldots, F^{j+k}\mathbf{y}^m .$$

This is a slow walk because $d(F^j\mathbf{y}^m, F^{j+1}\mathbf{x}) \le d(\mathbf{y}^m, F\mathbf{x}) = 1$. Thus, R is a retract. Furthermore, F is distance preserving on $V \subseteq W^j$, so by Proposition 4, F is distance preserving on R, and F commutes with T on R. Now, by choice of k,

$$F(V) = U^{j+1} \cup \cdots \cup U^{j+k+1} \subseteq Cl(V) = R .$$

Since F commutes with T on V,

$$F(Cl(V)) \subseteq Cl(F(V)) \subseteq Cl(R) = R .$$

Thus, we have achieved the final requirement that $F(R) \subseteq R$. It follows that all sets W^i, $i \ge j$ are subsets of

R and therefore F is distance preserving on each of these sets. In particular, F is distance preserving on W^j, for any $j \geq \nu(W)$. Thus, we could have taken $j \geq \nu(W)$ at the beginning, rather than testing each W^i for the distance preserving property. This will simplify bounding the total computation.

Theorem 2.7.6. Given an oracle for computing a contraction F on K_2^n, $n \geq 1$, there is an algorithm which finds a point with period 2^j, for some $2^j \leq 2n$, using $O(n^8)$ evaluations of F and $O(n^5)$ additional operations.

Proof. As defined above, $|W|$ is $O(nh)$, so $\nu(W) \leq n|W|^2$ is $O(n^3 h^2)$. Since $|U|$ is $O(n)$, it takes $O(n^4 h^2)$ and therefore $O(n^8)$ evaluations of F, to find W^j, $j = n|W|^2$. This dominates the number of evaluations of F that will be required in all. The set V can be found by finding which clauses apply to the sets $U^j, U^{j+1}, \ldots, U^{j+h}$. This requires testing $O(n^2)$ clauses on $O(nh)$ vectors, or $O(n^5)$ operations to find the 2SAT clauses which delimit R. This dominates the required calculations, aside from computing F.

Since F is distance preserving on R and takes R to itself, F is an isometry of the central cube of R, which is contained in R. This central cube will therefore contain a short cycle. We do *not* know how to find the central cube of a retract, so a slightly more complicated procedure will be used.

Begin by assuming the value of j for which there is a point in R with period 2^j. There are roughly $\log_2 n$ of these possibilities. First consider $j = 0$, i.e., look for a fixed point. A trick is to form the set

$$S = \{(\mathbf{x}, F\mathbf{x}) \mid \mathbf{x} \in R\} .$$

Because F commutes with T on R, S is a T closed subset of K_2^{2n}. The fixed points of F can be found by intersecting S with the diagonal $D = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in K_2^n\}$, another T closed set. A way to find the intersection is to represent both S and D as solutions sets of 2SAT systems and then to solve the conjunction of the two systems.

To reduce the computational effort, form a set V', such that $|V'|$ is $O(n^2)$ and $Cl(V') = Cl(V) = R$. A way to form V' is to begin with the empty set, and for each 1- or 2-clause *not* in the 2SAT system for R, put one vector of V into V' which does *not* satisfy that clause. When this process is complete, V' will satisfy the same 2SAT system as R and have cardinality $O(n^2)$. Since $Cl(V') = R$,

$$S = Cl(\{(\mathbf{x}, F\mathbf{x}) \mid \mathbf{x} \in V'\}) .$$

Thus, finding the 2SAT clauses for S amounts to testing all clauses on all $O(n^2)$ vectors in this set whose closure is S. This can be done in $O(n^4)$ operations. A 2SAT system for D can easily be written down. For example, the system consisting of the clauses $\bar{z}_i \vee z_{n+i}$ and $z_i \vee \bar{z}_{i+n}$, for $i = 1, 2, \ldots, n$, will work.

Assuming a fixed point is not found, increase j by 1 and look for a solution to $F^k(\mathbf{x}) = \mathbf{x}$, $k = 2^j$. Here we can replace S by

$$\{(\mathbf{x}, F^k\mathbf{x}) \mid \mathbf{x} \in R\} = Cl(\{(\mathbf{x}, F^k\mathbf{x}) \mid \mathbf{x} \in V'\}) ,$$

and intersect with D. Eventually, a fixed point of F^k is found for some $k \leq 2n$. ∎

Unsolved Problem. Find a polynomial time algorithm which for *any* function $F: K_2^n \to K_2^n$ finds either a short cycle of F or $\mathbf{x}, \mathbf{y} \in K_2^n$ such that $d(F\mathbf{x}, F\mathbf{y}) > d(\mathbf{x}, \mathbf{y})$.

The final two results of this chapter will show that *all* short cycles of a contraction can be found in polynomial time.

Proposition 2.7.7. Given a fixed point of a contraction F on K_2^n, $n \geq 1$, a 2SAT system describing the set of all fixed points of F can be found with $O(n^3)$ evaluations of F and $O(n^4)$ additional operations.

Proof. Without loss of generality let $\mathbf{0}$ be the given fixed point. Proposition 2.6.1 states that the set, S, of fixed points of F is T closed. To illustrate the method, it will be shown how to determine if the clause $\bar{x}_1 \vee \bar{x}_2$ is true on all members of S. If this is not the case, there is a point $\mathbf{z} = (1, 1, z_3, \ldots, z_n)$ in S. Under the assumption that such a point exists, the point $\mathbf{y}^1 = (1, 1, 0, \ldots, 0)$ is in $I(\mathbf{0}, \mathbf{z})$.

For any $\mathbf{v}\in I(\mathbf{0},\mathbf{z})$, $d(\mathbf{0},\mathbf{v})+d(\mathbf{v},\mathbf{z})=|z|$, and since F is a contraction fixing $\mathbf{0}$ and $\mathbf{z}$, $d(\mathbf{0},F\mathbf{v})+d(F\mathbf{v},\mathbf{z})\le |z|$, so $F(\mathbf{v})\in I(\mathbf{0},\mathbf{z})$, from which $d(\mathbf{0},F(\mathbf{v}))=d(\mathbf{0},\mathbf{v})=|\mathbf{v}|$.

Thus, if the point $\mathbf{z}$ exists $|F(\mathbf{y}^1)|=2$. If $|F(\mathbf{y}^1)|\neq 2$, we can stop, knowing that the 2-clause does apply to S. On the other hand if $F(\mathbf{y}^1)=\mathbf{y}^1$, we have found a fixed point with first two coordinates 1, so the 2-clause does not apply everywhere on S. In the event that neither situation holds, let $\mathbf{y}^2=\mathbf{y}^1\vee F(\mathbf{y}^1)$, where we use $\vee$ of *vectors* to denote coordinatewise Boolean disjunction. Under our assumptions $|\mathbf{y}^2|>2$, and $\mathbf{y}^2=T(\mathbf{y}^1,F\mathbf{y}^1,\mathbf{z})\in I(\mathbf{0},\mathbf{z})$.

Again, if $|F(\mathbf{y}^2)|\neq|\mathbf{y}^2|$ we can stop, having shown $\mathbf{z}$ cannot exist. Again, if $F(\mathbf{y}^2)=\mathbf{y}^2$, $\mathbf{y}^2$ satisfies the requirements of $\mathbf{z}$. In the third case, the vector $\mathbf{y}^3=\mathbf{y}^2\vee F(\mathbf{y}^2)$ has larger weight than $\mathbf{y}^2$ and must be on a shortest path from $\mathbf{0}$ to $\mathbf{z}$.

It is clear how to continue this process and since $|\mathbf{y}^i|$, $i=1,2,\ldots$ is increasing, it can go on for at most n steps. Eventually, we find out whether the clause applies or does not apply, using $O(n)$ evaluations of F and $O(n^2)$ additional operations. A similar procedure can be used to test all 1- or 2-clauses, to obtain a 2SAT description of S. ∎

Corollary 2.7.8. There is an algorithm to locate a fixed point of a contraction F on K_2^n, $n\ge 1$, which requires $O(n^8)$ evaluations of F and $O(n^5)$ additional operations.

Proof. Theorem 6 gives a point $\mathbf{x}$ such that $G(\mathbf{x})=\mathbf{x}$, where $G=F^k$, for some $k\le 2n$. Apply Proposition 7 to find all fixed points of G. Call the T closed set V. Notice that $F(V)\subseteq V$, because $GF(\mathbf{v})=FG(\mathbf{v})=F(\mathbf{v})$ whenever $\mathbf{v}\in V$. Thus, F permutes the elements of V, and F must be distance preserving on V, because F^k is the identity on V.

Let $\mathbf{u}=T(\mathbf{x},\mathbf{y},\mathbf{z})$, with $\mathbf{u},\mathbf{x},\mathbf{y},\mathbf{z}\in V$. Then,

$$d(F\mathbf{u},F\mathbf{x})+d(F\mathbf{u},F\mathbf{y})+d(F\mathbf{u},F\mathbf{z})=d(\mathbf{u},\mathbf{x})+d(\mathbf{u},\mathbf{y})+d(\mathbf{u},\mathbf{z})$$

$$=\tfrac{1}{2}\,\nu(\{\mathbf{x},\mathbf{y},\mathbf{z}\})=\tfrac{1}{2}\,\nu(\{F\mathbf{x},F\mathbf{y},F\mathbf{z}\})=d(\mathbf{w},F\mathbf{x})+d(\mathbf{w},F\mathbf{y})+d(\mathbf{w},F\mathbf{z}),$$

where $\mathbf{w}=T(F\mathbf{x},F\mathbf{y},F\mathbf{z})$. Hence, $\mathbf{w}=F(\mathbf{u})$, so F commutes with T on V.

To find a fixed point of F, we may use the same trick as at the end of the proof of Theorem 6, letting $S=\{(\mathbf{x},F\mathbf{x})\mid \mathbf{x}\in V\}$. We can again replace V by V', a set of cardinality $O(n^2)$, whose T closure is V. Then the 2SAT clauses for S are those that hold on $\{(\mathbf{x},F\mathbf{x})\mid \mathbf{x}\in V'\}$. Finally V can be intersected with the diagonal D to give a fixed point of F, if one exists. ∎

3. Hereditary Families

3.1. Hereditary Families and Simple Sets

This section abstractly considers properties of families of subsets of K_2^j, for j arbitrary. By a *family*, $\boldsymbol{F}$, we will mean a set, each member of which is a subset of some K_2^n. $\boldsymbol{F}(n)$ will denote the members of $\boldsymbol{F}$ which are subsets of K_2^n.

Definition. A family $\boldsymbol{F}$ is *natural* if for all n, $\boldsymbol{F}(n)$ is closed under isometries of K_2^n and if Φ: $K_2^n \to K_2^{n+1}$ is any mapping preserving Hamming distance, $\Phi(S)$ is in $\boldsymbol{F}(n+1)$ if and only if S is in $\boldsymbol{F}(n)$.

Just about any family defined in terms of a geometric property will be a natural family. For example, the connected subsets of K_2^n form such a family. But, this family is not even closed under intersection with cubes. Based on retracts and other sets studied so far, the following definition encompasses most of the good properties.

Definition. A family $\boldsymbol{F}$ is *hereditary* if it is natural and the following statements hold for each $S \in \boldsymbol{F}(n)$, $n \geq 0$.
H1) $S \cap Q \in \boldsymbol{F}$ for each cube $Q \subseteq K_2^n$.
H2) $S \cup (S \oplus \mathbf{t}) \in \boldsymbol{F}$ for each $\mathbf{t}$ with unit norm.
H3) $S \cap (S \oplus \mathbf{t}) \in \boldsymbol{F}$ for each $\mathbf{t}$ with unit norm.

Property H1 requires that membership in a family be preserved under *restriction* to cubes. Property H2 combined with property H1 requires that membership be preserved under *projection* to cubes. Property H2 combined with naturalness implies that if $S \in \boldsymbol{F}(n)$ then $K_2 \times S \in \boldsymbol{F}(n+1)$, and that in fact, $K_2^m \times S \in \boldsymbol{F}(n+m)$.

Suppose $\boldsymbol{F}$ is a family with the property that if $S \in \boldsymbol{F}(n)$ then $S^c \in \boldsymbol{F}(n)$, where S^c is the complement of S. For such families properties H2 and H3 are equivalent, by application of De Morgan's law. Thus, H3 is a kind of complemented version of H2. Some hereditary families discussed previously are: retracts, cubes, stars, ellipsoids, and quasicubes. The first two of these families are not closed under complementation.

The family of isometric sets is natural and satisfies H1 and H2, but not H3. For example, $K_2^3 \backslash \{000, 111\}$, the isometrically embedded 6-cycle pictured in section 1.4, is an isometric set for which H3 doesn't apply. By definition, the family of isometric sets is the largest family of connected sets such that H1 holds. As a bonus the family is natural and H2 holds. The main goal of this section is to find the largest hereditary family of connected sets. Subsequent sections of this chapter deal with more restricted hereditary families, but all families that we introduce in this chapter will be shown to contain all retracts and all stars. A somewhat unexpected tool is the following definition of the "Euler characteristic" of a set.

Definition. For $S \subseteq K_2^n$ let $\chi(S) = c_0(S) - c_1(S) + c_2(S) - \ldots$, where $c_i(S)$ is the number of i-dimensional subcubes of S.

Proposition 3.1.1. If $\boldsymbol{F}$ is a hereditary family of connected sets then $\chi(S) = 1$ for each nonempty $S \in \boldsymbol{F}$.

Proof. (Induction). The conclusion is true for *every* nonempty subset of K_2^n for $n \leq 1$. Suppose it is true for nonempty sets in $\boldsymbol{F}(n-1)$. Let S be any nonempty set in $\boldsymbol{F}(n)$. Let $S_0 = S \cap \{\mathbf{x} | x_1 = 0\}$ and $S_1 = S \cap \{\mathbf{x} | x_1 = 1\}$. These are both in $\boldsymbol{F}(n)$. If S_0 is empty, by naturalness and the inductive hypothesis, $\chi(S) = \chi(S_1) = 1$. A similar comment can be made if S_1 is empty. It can therefore be assumed that neither S_0 nor S_1 is empty. Let $\mathbf{e} = (1, 0, 0, \ldots, 0)$ and let $V = S \cap (S \oplus \mathbf{e})$. Note V is in $\boldsymbol{F}(n)$. Furthermore, V is nonempty. This is because S is connected so there is a path from a point in S_0 to a point in S_1, and this path must sometime use an edge such that the difference between the two endpoints is $\mathbf{e}$. Thus, there is an $\mathbf{x} \in S_0$ such that $\mathbf{x} \oplus \mathbf{e} \in S_1$, so $\mathbf{x}$ and $\mathbf{x} \oplus \mathbf{e}$ are both in V.

The subcubes of *any* $S \in K_2^n$ fall into three mutually exclusive classes.
i) subcubes of S_0,

ii) subcubes of S_1,
iii) subcubes invariant under translation by $\mathbf{e}$.
Let $c^i_d(S)$, $c^{ii}_d(S)$, and $c^{iii}_d(S)$ count the number of d-dimensional subcubes of S in each of the three classes. Then,

$$\chi(S) = \sum_{d\geq0}(-1)^d c^i_d(S) + \sum_{d\geq0}(-1)^d c^{ii}_d(S) + \sum_{d\geq0}(-1)^{d+1} c^{iii}_{d+1}(S) .$$

Let V_0 be the set of points in V with first coordinate 0. Since $V = V_0 \cup (V_0 \oplus \mathbf{e})$, $c^{iii}_{d+1}(S) = c_d(V_0)$. Therefore,

$$\chi(S) = \chi(S_0) + \chi(S_1) - \sum_{d\geq0}(-1)^d c_d(V_0) = \chi(S_0) + \chi(S_1) - \chi(V_0) . \qquad (*)$$

Equation (*) is valid for any set S. Since S_0,S_1 and V_0 are nonempty members of $\boldsymbol{F}$ and are contained in $(n-1)$-cubes, by the induction hypothesis $\chi(S_0) = \chi(S_1) = \chi(V_0) = 1$. Thus, $\chi(S) = 1 + 1 - 1 = 1$. ∎

Definition. A set $S \subseteq K^n_2$ is *simple* if for each cube, Q, in K^n_2, either $S \cap Q$ is empty or $\chi(S \cap Q) = 1$.

It immediately follows that if $S \subseteq K^n_2$ is simple, so is $S \cap Q$ for each cube, Q. The next goal is to prove that the simple sets form a hereditary family. It is easiest to start by first proving it is a self-complementary family.

Proposition 3.1.2. The complement of a simple set is simple.

Proof. Assuming $S \subseteq K^n_2$ is simple and $S \neq K^n_2$, we will prove that $\chi(S^c) = 1$. The proposition is then proved by applying this statement to $S \cap Q$ for all cubes Q.

Let $c_d = c_d(S)$ and $\bar{c}_d = c_d(S^c)$. If S is empty then

$$\chi(S^c) = \sum_{d=0}^{d=n}(-1)^d 2^{n-d}\binom{n}{d} = 2^n(1 - \tfrac{1}{2})^n = 1 .$$

Thus, it can be assumed that S is nonempty and that $c_n = \bar{c}_n = 0$.

There are $2n$ $(n-1)$-cubes in K^n_2. A d-cube is contained in $\binom{n-d}{1}$ $(n-1)$-cubes. Hence, if the expression for $\chi(S \cap Q)$ is summed for all $(n-1)$-cubes, Q, the result is

$$\binom{n}{1}c_0 - \binom{n-1}{1}c_1 + \binom{n-2}{1}c_2 - \ldots \pm \binom{1}{1}c_{n-1} .$$

The only way $\chi(S \cap Q) \neq 1$ is if $S \cap Q$ is empty, in which case S^c has an $(n-1)$-cube. Thus,

$$\binom{n}{1}c_0 - \binom{n-1}{1}c_1 + \binom{n-2}{1}c_2 - \ldots = 2n - \bar{c}_{n-1} .$$

This argument generalizes to summing $\chi(S \cap Q)$ over all cubes, Q, of co-dimension k, to give

$$\binom{n}{k}c_0 - \binom{n-1}{k}c_1 + \binom{n-2}{k}c_2 - \ldots = 2^k\binom{n}{k} - \bar{c}_{n-k} . \qquad (*)$$

Now, sum all lefthand sides of (*) after multiplying each by $(-1)^k$, for $0 \leq k \leq n$ to obtain,

$$\sum_{k=0}^{n}(-1)^k\sum_{j=0}^{n-1}(-1)^j\binom{n-j}{k}c_j = \sum_{j=0}^{n-1}(-1)^j c_j \sum_{k=0}^{n}(-1)^k\binom{n-j}{k} = \sum_{j=0}^{n-1}(-1)^j c_j 0^{n-j} = 0 .$$

Doing the same sum for the righthand sides of (*), we obtain

$$0 = \sum_{k=0}^{n}(-2)^k\binom{n}{k} - (-1)^n \quad (\bar{c}_0 - \bar{c}_1 + \bar{c}_2 - \ldots) = (-1)^n - (-1)^n\chi(S^c) ,$$

so $\chi(S^c) = 1$. ∎

Proposition 3.1.3. The simple sets form a hereditary family of connected sets.

Proof. First we show that any simple set is connected. Suppose, to the contrary that S is simple and disconnected. Let $\mathbf{x}$ and $\mathbf{y}$ be two points of S, selected to have minimal distance between them subject to the constraint that they are in different components of S. Due to minimality, the cube, Q, having opposite corners $\mathbf{x}$ and $\mathbf{y}$ must not intersect S in any other points. But, then $\chi(S \cap Q) = 2$, a contradiction.

By definition of simple, simple sets form a natural family satisfying H1. By Proposition 2, property H3 implies property H2, so only H3 need be proved.

Let $\mathbf{e} = (1, 0, 0, \ldots, 0)$ and let S be a simple set such that $V = S \cap (S \oplus \mathbf{e})$ is nonempty. For any set U, let U_0 and U_1 be the subsets where the first coordinate is 0 and 1, respectively.

Assume that Q is a cube such that $V \cap Q$ is nonempty. It must be shown that $\chi(V \cap Q) = 1$. Let $\hat{Q} = Q \cup (Q \oplus \mathbf{e})$. This is a cube which may or may not equal Q, but certainly contains Q. Let $W = S \cap \hat{Q}$. By equation (*) in the proof of Proposition 1, for any set W,

$$\chi(W) = \chi(W_0) + \chi(W_1) - \chi((W \cap (W \oplus \mathbf{e}))_0) \,.$$

We have $W \cap (W \oplus \mathbf{e}) = V \cap \hat{Q}$, so W_0, W_1 and W are nonempty. Also, W_0, W_1 and W are simple, so these sets have characteristic one. Thus, $\chi((V \cap \hat{Q})_0) = 1$. Since $(V \cap \hat{Q})_1 = (V \cap \hat{Q})_0 \oplus \mathbf{e}$, $\chi((V \cap \hat{Q})_1) = 1$. Finally, by the same equation (*),

$$\chi(V \cap \hat{Q}) = \chi((V \cap \hat{Q})_0) + \chi((V \cap \hat{Q})_1) - \chi((V \cap \hat{Q})_0) = 1 \,.$$

Since Q is either all of $\hat{Q}$ or one half of it, Q is either $\hat{Q}$, $\hat{Q}_0$ or $\hat{Q}_1$. Thus, $V \cap Q$ is equal to one of the sets $V \cap \hat{Q}$, $(V \cap \hat{Q})_0$, and $(V \cap \hat{Q})_1$. All three sets have characteristic one, so $\chi(V \cap Q) = 1$. ∎

Propositions 1,2 and 3 can be condensed as follows.

Theorem 3.1.4. The family of simple sets is the unique largest hereditary family of connected sets. Furthermore, the complement of a simple set is simple.

3.2. Additional Facts About Simple Sets

This section takes a more detailed look at simple sets, ending with a "polynomial time" recognition result. The first result shows there are no nontrivial simple sets which are preserved by the antipodal map of K_2^n. This shows a difference with isometric sets, because it is easy to generate isometric sets preserved by the antipodal map.

Proposition 3.2.1. If $S \subseteq K_2^n$ is simple with the property that $\mathbf{s} \in S$ implies $\bar{\mathbf{s}} \in S$, then S is empty or all of K_2^n.

Proof. Let Φ: $K_2^n \to K_2^n$ be the map which takes $\mathbf{s}$ to $\bar{\mathbf{s}}$. Assuming $\Phi(S) = S$, if Q is any subcube of S, so is $\Phi(Q)$. The only cubes $Q \subseteq K_2^n$ such that $\Phi(Q) = Q$ are the empty set and K_2^n. To see this, suppose $\mathbf{x} \in Q$, where $\Phi(Q) = Q$. Notice $d(\mathbf{x}, \Phi(\mathbf{x})) = d(\mathbf{x}, \mathbf{x} \oplus (1, \ldots, 1)) = n$, and any cube with two points at distance n must be at least n-dimensional, so $Q = K_2^n$.

For the $c_d(S)$ subcubes of S with dimension d, $0 \le d < n$, Φ is an involution with no fixed elements. Thus, if $S \ne K_2^n$ each $c_d(S)$, $0 \le d$, is even and $\chi(S)$ is also even. However, for nonempty simple sets S, $\chi(S) = 1$, a contradiction. ∎

Proposition 3.2.2. $\chi(S \times V) = \chi(S)\,\chi(V)$, for any subsets S and V of K_2^n.

Proof. All d-cubes of $S \times V$ are of the form $Q^{(1)} \times Q^{(2)}$, where $Q^{(1)}$ is a j-cube of S and $Q^{(2)}$ is a $(d - j)$-cube of V, for some j. Thus,

$$c_d(S \times V) = \sum_j c_j(S) \cdot c_{d-j}(V) \,. \tag{*}$$

Define the "cube-polynomial" of a set S to be

$$c(S,z)=\sum_j c_j(S)z^j \ .$$

It follows from (*) that $c(S\times V,z)=c(S,z)\,c(V,z)$. Since $c(S,-1)=\chi(S)$, the substitution $z=-1$ establishes the proposition. ⁝

Proposition 3.2.3. The Cartesian product of simple sets is simple.

Proof. Let $S\subseteq K_2^k$ and $T\subseteq K_2^m$ be any simple sets and let $Q\subseteq K_2^{k+m}$ be an arbitrary cube such that $(S\times T)\cap Q$ is nonempty. Write $Q=Q^{(1)}\times Q^{(2)}$ for cubes $Q^{(1)}\subseteq K_2^k$ and $Q^{(2)}\subseteq K_2^m$. Then, by the previous proposition,

$$\chi((S\times T)\cap Q)=\chi(S\cap Q^{(1)})\cdot\chi(T\cap Q^{(2)})=1\cdot 1=1\ .$$

⁝

The use of a number like the Euler characteristic to define simple sets suggests that these sets are in some sense topologically contractable. Our next goal is to show that simple sets are "simply connected" in a strong, discretized, sense.

Definition. Let G be a bipartite graph without loops or multiple edges and let W and U be two walks in G, both starting at vertex $\mathbf{x}$ and terminating at vertex $\mathbf{y}$. Say W can be *deformed* into U if there is a finite sequence of transformations, each one of the following two types, taking W to U. Let T and T' denote arbitrary walks, possibly empty.
i) a walk having vertex sequence of the form $T,\mathbf{a},\mathbf{b},\mathbf{a},T'$ can be transformed to the walk $T,\mathbf{a},T'$, for any two adjacent vertices $\mathbf{a}$ and $\mathbf{b}$.
ii) a walk having vertex sequence of the form $T,\mathbf{a},\mathbf{b},\mathbf{c},T'$ can be transformed to the walk $T,\mathbf{a},\mathbf{d},\mathbf{c},T'$, if $\mathbf{a},\mathbf{b},\mathbf{c}$ and $\mathbf{d}$ are four distinct vertices which induce a 4-cycle in G.

These transformations bear a similarity to the path homotopies in the definition of the Poincaré fundamental group of a topological space. One important difference is that neither of our transformations can increase the length of a walk, although transformation i) decreases the length by two. Thus, the following definition is not exactly what we would call a discrete version of simple connectivity, but a stronger version of it.

Definition. Let G be a bipartite graph without loops or multiple edges. Say G is *metrically simply connected* if for any two vertices $\mathbf{x}$ and $\mathbf{y}$, any walk W from $\mathbf{x}$ to $\mathbf{y}$ and any shortest path P from $\mathbf{x}$ to $\mathbf{y}$, W can be deformed to P.

Theorem 3.2.4. The induced graph of a simple set is metrically simply connected.

Proof. Let $S\subseteq K_2^n$ be simple and suppose that W is a walk in S from $\mathbf{x}$ to $\mathbf{y}$ and that P is a shortest path in S from $\mathbf{x}$ to $\mathbf{y}$. Since simple sets are isometric, P has length $d(\mathbf{x},\mathbf{y})$. It will be shown that W can be deformed to P by induction on the length of W. This is clearly true whenever the walk has length less than two. Assume that the result is true whenever the walk has length less than l, for some $l\geq 2$, and that W has length l.

First, the result can be established in the special case that $\mathbf{x}=\mathbf{y}$, i.e., that W is a circuit and P has length zero. Let $\mathbf{z}$ be the second vertex of W. Let W' be W with its first step removed. Let P' be the unit length path from $\mathbf{z}$ to $\mathbf{x}$. The inductive hypothesis applies to W' and P' to yield that W' can be deformed to P'. The same sequence of transformations will take W to the walk $\mathbf{x},\mathbf{z},\mathbf{x}$. Finally, a transformation of type i) will take this walk to the zero length walk P, as required.

Now assume P has length at least one. Let the second vertex in P be $\mathbf{x}\oplus\mathbf{e}$, where $\mathbf{e}$ has unit norm, and by isometry we can assume $\mathbf{e}=(1,0,0,\ldots,0)$ and $\mathbf{x}$ has first coordinate zero. Let $S=S_0\cup S_1$ be the partition of S by the first coordinate. Since $\mathbf{y}\in S_1$, there is a first point, say $\mathbf{z}$, in the walk W whose successor in this walk lies in S_1. Now, $V=S_0\cap(S_1\oplus\mathbf{e})$ is simple, by H3 and H1, and V contains $\mathbf{x}$ and $\mathbf{z}$. Let P' be a path in V of length $d(\mathbf{x},\mathbf{z})$ from $\mathbf{x}$ to $\mathbf{z}$ and let W' be the initial portion of W which terminates at the first occurrence of $\mathbf{z}$. Since both P' and W' are in S and W' is shorter than W, by the inductive hypothesis, W' can be deformed to P'.

Using only type ii) transformations it is possible to deform the walk $P', (\mathbf{z}+\mathbf{e})$ to a walk lying in S_1, except for the first vertex. This is done by applying the first transformation on the tail end of the walk and subsequently moving towards the beginning of the walk. This works because both V and $V \oplus \mathbf{e}$ are subsets of S. Let $P' = \mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_m$, where $\mathbf{p}_1 = \mathbf{x}$ and $\mathbf{p}_m = \mathbf{z}$. The sequence of walks obtained is

$$\mathbf{p}_1, \cdots, \mathbf{p}_{m-1}, \mathbf{p}_m, \mathbf{p}_m \oplus \mathbf{e}$$

$$\mathbf{p}_1, \cdots, \mathbf{p}_{m-1}, \mathbf{p}_{m-1} \oplus \mathbf{e}, \mathbf{p}_m \oplus \mathbf{e}$$

$$\mathbf{p}_1, \cdots, \mathbf{p}_{m-2}, \mathbf{p}_{m-2} \oplus \mathbf{e}, \mathbf{p}_{m-1} \oplus \mathbf{e}, \mathbf{p}_m \oplus \mathbf{e}$$

$$\cdots$$

$$\mathbf{p}_1, \mathbf{p}_2 \oplus \mathbf{e}, \cdots, \mathbf{p}_{m-1} \oplus \mathbf{e}, \mathbf{p}_m \oplus \mathbf{e} \, .$$

Let this last walk be called P''. Note that $W = W', (\mathbf{z} \oplus \mathbf{e}), \hat{W}$ for some walk $\hat{W}$. The first sequence of transformations takes this to $P', (\mathbf{z} \oplus \mathbf{e}), \hat{W}$. The above sequence of type ii) transformations takes this to $P'', \hat{W}$.

The important thing is that the original walk W has been deformed in S to a walk whose first and *second* vertices agree with P. Thus, $P = \mathbf{x}, \ddot{P}$ and $P'', \hat{W} = \mathbf{x}, \ddot{W}$, where $\ddot{P}$ and $\ddot{W}$ have the same initial and terminal vertices. Now, using the inductive hypothesis, $\ddot{W}$ can be deformed into $\ddot{P}$, so W can be deformed into P. ∎

Next we prove that the statement of Theorem 2.3.5 is true for all simple sets, not just retracts.

Theorem 3.2.5. If $S, Q \subseteq K_2^n$ with S simple and Q a cube, if the projection of S to Q is all of Q, then S contains a subcube parallel to Q.

Proof. Since the projection to any cube can be obtained by a series of projections to cubes of co-dimension one and because simple sets satisfy H1 and H2, we may assume Q has co-dimension one (as in the proof of Theorem 2.3.5). In fact, by isometry, it can be assumed that $Q = \{\mathbf{x} | x_1 = 0\}$. Now S is a simple set such that $Q = S_0 \cup (S_1 \oplus \mathbf{e})$, where $\mathbf{e} = (1, 0, 0, \ldots, 0)$. If $Q \subseteq S_0$ or $Q \subseteq S_1 \oplus \mathbf{e}$ there is nothing to prove. Suppose, then, that $\mathbf{x} \in Q \backslash S_0$ and $\mathbf{y} \in (Q \oplus \mathbf{e}) \backslash S_1$. Since S^c is simple, S^c is connected, and by a now familiar argument, on a path in S^c from $\mathbf{x}$ to $\mathbf{y}$ there is a pair of points of the form $\mathbf{z}$ and $\mathbf{z} \oplus \mathbf{e}$. Thus, $S_0 \cup (S_1 \oplus \mathbf{e})$ does not contain $(0, z_2, z_3, \ldots, z_n)$, so by contradiction, S has a subcube parallel to Q. ∎

This theorem will next be applied to obtain a result about *maximal* subcubes of simple sets. These are the subcubes of a set which are not contained in any larger subcubes. One reason the maximal subcubes are important is that to solve the problem of covering a set by the smallest number of subcubes, only the maximal subcubes need to be considered. The next result does not show how to solve the minimum cube cover problem for simple sets, but at least will show that the number of maximal subcubes is rather small.

Theorem 3.2.6. If S is a simple set containing a d-cube, $d \geq 0$, then the number of maximal subcubes in S is no more than $|S| + 1 - 2^d$.

Proof. (Induction). Clearly, the statement holds for any simple set in K_2^n, $n = 0$ or 1. Assume the statement to be true for simple sets in K_2^{n-1}, $n \geq 2$, and let $S \subseteq K_2^n$ be nonempty and simple. Let S_0,S_1 and $\mathbf{e} = (1, 0, 0, \ldots, 0)$ be as frequently defined. Let $T = S \cap (S \oplus \mathbf{e})$ and $U = S \cup (S \oplus \mathbf{e})$. Let $\boldsymbol{M}(X)$ denote the set of maximal subcubes of a set $X \subseteq K_2^n$. We will define an injective map Ψ from $\boldsymbol{M}(S)$ to the *disjoint* union of $\boldsymbol{M}(T_0)$ and $\boldsymbol{M}(U_0)$.

Specifically, suppose $Q \in \boldsymbol{M}(S)$. If $Q \subseteq T$, then define $\Psi(Q)$ to be Q_0 as a member of $\boldsymbol{M}(T_0)$. Clearly Q_0 is a maximal subcube of T_0, since were it contained in a larger subcube of T_0, Q would be in a larger subcube of T, so Q would not be maximal in $S \supseteq T$.

If Q is not contained in T, either $Q \subseteq S_0$ or $Q \subseteq S_1$. If $Q \subseteq S_0$ let $\Psi(Q)$ be Q as a subcube of U_0 and if $Q \subseteq S_1$ let $\Psi(Q)$ be $Q \oplus \mathbf{e}$ as a subcube of U_0. It must be shown that in either case $\Psi(Q) \in \boldsymbol{M}(U_0)$. Assume that $Q \subseteq S_0$ since the other case is very similar. If Q is contained in a larger subcube, say R_0, of U_0, construct the cube $R = R_0 \cup (R_0 \oplus \mathbf{e})$. The simple set $S \cap R$, when projected to R_0, covers R_0 entirely. Hence, by

Theorem 5 either $R_0 \subseteq S$ or $R_0 \oplus \mathbf{e} \subseteq S$. We know $Q \oplus \mathbf{e}$ is not contained in S since this would imply that Q is contained in T. Hence $R_0 \subseteq S$, contradicting $Q \in \boldsymbol{M}(S)$.

Injectivity of Ψ follows from its definition. Clearly if $\Psi(Q) \in \boldsymbol{M}(T_0)$, $Q = \Psi(Q) \cup (\Psi(Q) \oplus \mathbf{e})$ and if $\Psi(Q) \in \boldsymbol{M}(U_0)$, $Q = \Psi(Q)$ or $Q = \Psi(Q) \oplus \mathbf{e}$, but not both.

Now, let d be the largest dimension of a subcube of S, $d \geq 0$. If $d = n$, $S = K_2^n$ and S only has one maximal cube, so the statement of the theorem obviously holds in this case. Thus, it can be assumed that $d < n$. By isometry of K_2^n, it can be assumed that some d-cube lies entirely in S_0. If S_1 is empty, S lies in an $(n-1)$-dimensional cube, and the inductive hypothesis handles this case. Assume that S_1 is nonempty. Since S_0 and S_1 are nonempty, T_0 is nonempty.

Our only need for introducing Ψ is that its injectivity shows

$$|\boldsymbol{M}(S)| \leq |\boldsymbol{M}(T_0)| + |\boldsymbol{M}(U_0)| \, . \qquad (*)$$

Note by inclusion exclusion, $|S| = |S_0| + |S_1| = |T_0| + |U_0|$, $|\boldsymbol{M}(U_0)| \leq |U_0| + 1 - 2^d$ and $|\boldsymbol{M}(T_0)| \leq |T_0| + 1 - 2^{d'}$, where d' is the dimension of some subcube of T_0. Simply using the fact that $d' \geq 0$, $|\boldsymbol{M}(T_0)| \leq |T_0|$. Combining this with (*) gives $|\boldsymbol{M}(S)| \leq |S| + 1 - 2^d$, as required. ∎

The final result in this section is a theorem which provides a way to quickly check if a set is simple. The idea is to chop the set into two pieces and check if each piece is simple and if the two pieces glue together properly.

Theorem 3.2.7. A set $S \subseteq K_2^n$ is simple if and only if S is isometric and S_0, S_1 and $S_0 \cap (S_1 \oplus \mathbf{e})$ are simple, where S_0 and S_1 are the subsets of S having first coordinate equal to 0 and 1 respectively, and $\mathbf{e} = (1, 0, 0, \ldots, 0)$.

Proof. Any simple set is isometric because simple sets are connected and satisfy H1. If S is simple, S_0, S_1 and $S_0 \cap (S_1 \oplus \mathbf{e})$ are easily seen to be simple by the hereditary property. Thus, the ‘‘only if’’ part of the theorem is true.

Let S be any set which satisfies the conditions stated in the ‘‘if’’ part of the theorem. Let Q be any cube such that $S' = S \cap Q$ is nonempty. We must show that $\chi(S') = 1$. If either $S_0 \cap Q$ or $S_1 \cap Q$ is empty, then $S \cap Q$ equals either $S_1 \cap Q$ or $S_0 \cap Q$, and $\chi(S') = 1$ because S_0 and S_1 are simple.

Assume that neither $S_0 \cap Q$ nor $S_1 \cap Q$ is empty. This implies $Q \oplus \mathbf{e} = Q$. By equation (*) in the proof of Proposition 3.1.1,

$$\chi(S') = \chi(S_0 \cap Q) + \chi(S_1 \cap Q) - \chi((S_0 \cap (S_1 \oplus \mathbf{e})) \cap Q) \, . \qquad (*)$$

Since S is isometric, $S \cap Q$ is connected. Furthermore, since $S_0 \cap Q$ and $S_1 \cap Q$ are nonempty some path in $S \cap Q$ connecting a point in $S_0 \cap Q$ to a point in $S_1 \cap Q$ contains a point of $S_0 \cap (S_1 \oplus \mathbf{e}) \cap Q$, where the path crosses from S_0 to S_1, so $S_0 \cap (S_1 \oplus \mathbf{e}) \cap Q$ is nonempty. Since all three sets on the righthand side of (*) are nonempty and simple, $\chi(S') = 1 + 1 - 1 = 1$. ∎

This immediately leads to an algorithm to test for a set to be simple. Let $i(n, m)$ be the number of operations required to test for an m-element subset of K_2^n to be isometric, and let $s(n, m)$ be the number of operations required to test for simplicity. Since Theorem 7 reduces testing a subset of K_2^n to testing three sets in K_2^{n-1}, by direct application of the theorem, $s(n, m) \leq$

$$i(n, m) + w(n, m) + \underset{\substack{m_0 + m_1 + 2m_I = m \\ m_0, m_1, m_I \geq 0}}{\mathrm{Max}} s(n-1, m_0 + m_I) + s(n-1, m_1 + m_I) + s(n-1, m_I) \, .$$

The overhead in splitting the set into three sets is represented by $w(n, m)$ and is certainly $O(nm \log m)$. Also, m_I, m_0, m_1 are defined by $|S_0 \cap (S_1 \oplus \mathbf{e})| = m_I$, $|S_0| = m_0 + m_I$ and $|S_1| = m_1 + m_I$. By 1.4.5 we have that $i(n, m)$ is $O(nm^2)$. It follows that $s(n, m)$ is $O(n^2 m^2)$, by induction on n.

3.3. Isometric Sequences

The isometric subsets of K_2^n form a large family of sets somewhat like convex sets in Euclidean geometry. This chapter looks into stronger versions of the isometric property. One way to do this is to demand that the points in the set can be ordered so that certain subsets are also isometric. The following definition will be proved to be "too strong" in the sense that only cubes possess this property.

Definition. $S \subseteq K_2^n$ is said to be *cyclically isometric* if S is empty or if $|S| = m \geq 1$ and S can be written $\{\mathbf{s}^1, \ldots, \mathbf{s}^m\}$ such that $\{\mathbf{s}^{i+1}, \mathbf{s}^{i+2}, \ldots, \mathbf{s}^{i+j}\}$ is isometric for each $i \geq 1$ and $j \geq 1$, with indices taken modulo m. Such an ordering is called a *cyclic isometric ordering* of S.

Theorem 3.3.1. The cyclically isometric subsets of K_2^n are precisely the cubes. The reflected Gray code order gives a cyclic isometric ordering of a cube.

Proof. First, it will be shown that any cyclically isometric set must be a cube. Let $S \subseteq K_2^n$ be such a set. Clearly S is isometric and therefore connected. Suppose some 2-cube $Q = \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}\}$ intersects S in exactly the three points $\mathbf{a}, \mathbf{b}, \mathbf{c}$, where $\mathbf{b}$ has unit distance from the other two points. Wherever $\mathbf{b}$ lies in the cyclic ordering of S, the set $S \backslash \{\mathbf{b}\}$ is required to be isometric. However, this is a contradiction because $Q \cap (S \backslash \{\mathbf{b}\}) = \{\mathbf{a}, \mathbf{c}\}$ is not connected. Thus, no 2-cube meets S in exactly three points. Since S is connected S must be a cube, by the No3) condition of Proposition 1.4.3.

Next, it must be shown that the reflected Gray code order of a cube is cyclically isometric. For example, 000, 001, 011, 010, 110, 111, 101, 100 is a cyclic isometric order of a 3-cube.

Recall that if a nonnegative integer i has binary representation $(\beta_{n-1}, \beta_{n-2}, \ldots, \beta_1, \beta_0)$ then the i^{th} point in the reflected Gray code is $G(i) = (\beta_{n-1}, \beta_{n-1} \oplus \beta_{n-2}, \ldots, \beta_2 \oplus \beta_1, \beta_1 \oplus \beta_0)$. Now, given i and j, $0 \leq i < j < 2^n$, let their binary representations be $i = (\mathbf{r}0\mathbf{s})_2$ and $j = (\mathbf{r}1\mathbf{t})_2$, for some words $\mathbf{r}, \mathbf{s}, \mathbf{t}$. Let $i' = (\mathbf{r}1\bar{\mathbf{s}})_2$ and $j' = (\mathbf{r}0\bar{\mathbf{t}})_2$. Note $G(i')$ differs from $G(i)$ in a single coordinate and $G(i') \oplus G(i) \leq G(j) \oplus G(i)$, as 0-1 vectors, so $G(i') \in I(G(i), G(j))$. By a similar argument, $G(j') \in I(G(i), G(j))$.

Let $[i, j] = \{k \mid i \leq k \leq j\}$ and $(i, j) = \{k \mid i < k < j\}$. If $\bar{\mathbf{s}} \leq \mathbf{t}$ then $i' \in [i, j]$ and $\bar{\mathbf{t}} \leq \mathbf{s}$ so $j' \leq i$ and $j' \notin (i, j)$. If $\bar{\mathbf{s}} \geq \mathbf{t}$ then $\bar{\mathbf{t}} \geq \mathbf{s}$ so $j' \in [i, j]$ and $i' \notin (i, j)$. Thus, it is true that $G(i')$ or $G(j')$ lies in $\{G(i), G(i+1), \ldots, G(j)\}$ and that $G(i')$ or $G(j')$ lies in $\{G(j), G(j+1), \ldots, G(2^n - 1), G(0), \ldots, G(i)\}$.

If S is a set such that for any two distinct points of S there is a point of S in the interval between them and at a unit distance from one of them, then S is isometric. Thus, for all i and j the sets $\{G(i), G(i+1), \ldots, G(j)\}$ and $\{G(j), G(j+1), \ldots, G(2^n - 1), G(0), \ldots, G(i)\}$ are isometric. ∎

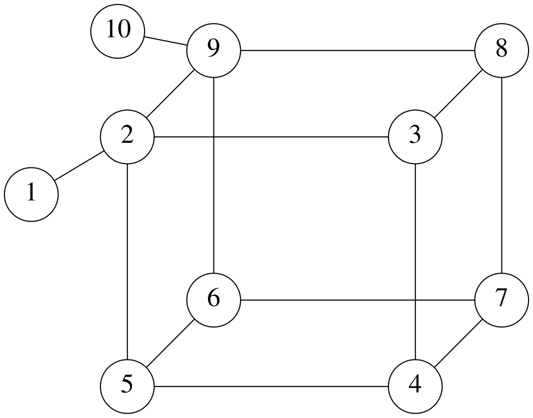
Although the only sets having cyclic isometric orders are cubes, the reflected Gray code is not the only cyclic isometric order for cubes. Each cyclic isometric order must be a Hamiltonian circuit of the cube it spans. This is because all sets of the form $\{\mathbf{x}^i, \mathbf{x}^{i+1}\}$ must be isometric and thus $\mathbf{x}^i$ and $\mathbf{x}^{i+1}$ differ in only one coordinate. It is therefore possible to specify such an order by its "change sequence" i.e., the sequence of coordinate directions in which the cyclic order moves. The following is the change sequence of a cyclic isometric order of K_2^4 which can't be obtained from the reflected Gray code by isometry of K_2^4.

$$1, 2, 3, 4, 3, 2, 3, 4, 1, 4, 3, 2, 3, 4, 3, 2 .$$

Clearly, it would be interesting to relax the definition of cyclic isometric to allow sets other than cubes. One possibility is *linearly isometric* sets which are those sets S which can be written, $S = \{\mathbf{s}^1, \ldots, \mathbf{s}^m\}$, where $|S| = m$ and for each $1 \leq i < j \leq m$, $\{\mathbf{s}^i, \ldots, \mathbf{s}^j\}$ is isometric. If S is any such set and Q is any cube, it can be shown that $S \cap Q$ is another set of this type. However, this is not true of *projection* to subcubes. For example, in K_2^5 let

$$S = \{00001, 00000, 00100, 01100, 01000, 11000, 11100, 10100, 10000, 10010\} .$$

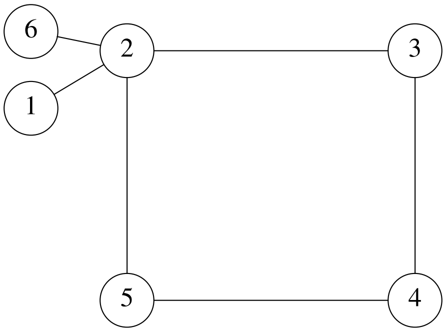
The induced subgraph is pictured below.



The labels correspond to the order in which S is listed and in this order S is linearly isometric. But, the projection to the subcube $0{*}{*}{*}{*}$ is

$$\{00001, 00000, 00100, 01100, 01000, 00010\}$$

which can be seen to be not linearly isometric since the induced subgraph of K_2^5 does not have a Hamiltonian path.



It is an open problem to characterize linearly isometric sets, but since they do not possess the hereditary property H2, they may not be the most interesting family to study. The following definition does lead to a hereditary family.

Definition. $S \subseteq K_2^n$ is *isometrically shellable* if S is empty or if $|S| = m > 0$ and S can be written as $\{\mathbf{s}^1, \ldots, \mathbf{s}^m\}$ such that $\{\mathbf{s}^1, \ldots, \mathbf{s}^i\}$ is isometric for each $1 \le i \le m$.

Theorem 3.3.2. The isometrically shellable sets form a hereditary family.

Proof. The family is clearly natural.

To show property H1 applies, let $S = \{\mathbf{s}^1, \ldots, \mathbf{s}^m\}$ be an "isometric shelling" of S. If $Q \subseteq K_2^n$ is any cube which meets S, let the, say l, members of $S \cap Q$ be $\mathbf{s}^{q(j)}$, $1 \le j \le l$, and assume they are ordered such that $j < k \Rightarrow q(j) < q(k)$. For any i, $1 \le i \le l$, $\{\mathbf{s}^{q(1)}, \mathbf{s}^{q(2)}, \ldots, \mathbf{s}^{q(i)}\} = \{\mathbf{s}^1, \mathbf{s}^2, \ldots, \mathbf{s}^{q(i)}\} \cap Q$, an isometric set because isometric sets have property H1. Thus, isometrically shellable sets have property H1.

As usual, let S_0 and S_1 be the subsets where S has first coordinate 0 and 1, respectively, and let $\mathbf{e} = (1, 0, 0, \ldots, 0)$. Before establishing H2 and H3, we first show that if $S = S_0$, then $S \cup (S \oplus \mathbf{e})$ is isometrically shellable. If $S = \{\mathbf{s}^1, \ldots, \mathbf{s}^m\}$ is an isometric shelling of S, then it easily follows that $\{\mathbf{s}^1, \ldots, \mathbf{s}^m, \mathbf{s}^1 \oplus \mathbf{e}, \ldots, \mathbf{s}^m \oplus \mathbf{e}\}$ is an isometric shelling of $S \cup (S \oplus \mathbf{e})$.

To complete the proof of H2, it need only be shown that for any isometrically shellable set S, $U_0 = S_0 \cup (S_1 \oplus \mathbf{e})$ is isometrically shellable. The same trick that worked for H1 works here. That is, U_0 is ordered the same way as S. The only problem is that a member of U_0 might correspond to two members of S. In such cases the first appearance in S will be taken. Let $\pi\colon K_2^n \to K_2^n$ be the map which replaces the first coordinate of a vector with 0, so we have $U_0 = \pi(S)$. For each $\mathbf{u} \in U_0$ let $j(\mathbf{u}) = \min\{i|(\pi(\mathbf{s}^i) = \mathbf{u})\}$. Letting $|U_0| = l$, label the members of U_0 so that $U_0 = \{\mathbf{u}^1,\ldots,\mathbf{u}^l\}$, where $f < g => j(\mathbf{u}^f) < j(\mathbf{u}^g)$. Note that $\{\mathbf{u}^1,\ldots,\mathbf{u}^h\} = \pi\{\mathbf{s}^1,\ldots,\mathbf{s}^k\}$, where $k = j(\mathbf{u}^h)$. Thus, $\{\mathbf{u}^1,\ldots,\mathbf{u}^h\}$ is isometric because π takes isometric sets to isometric sets, as follows from H1 and H2 for isometric sets.

Establishing H3 requires a bit more work because isometric sets themselves do not have this property. Let $V_0 = S_0 \cap (S_1 \oplus \mathbf{e})$. These are the points of S which, under π, have two preimages in S. For each $\mathbf{v} \in V_0$, let $j(\mathbf{v}) = \max\{i|\pi(\mathbf{s}^i) = \mathbf{v}\}$. Letting $|V_0| = l$, label the members of V_0 so that $V_0 = \{\mathbf{v}^1,\ldots,\mathbf{v}^l\}$, and whenever $f < g$, $j(\mathbf{v}^f) < j(\mathbf{v}^g)$. It will be shown that for any $h \le l$, $\{\mathbf{v}^1,\ldots,\mathbf{v}^h\}$ is isometric. To accomplish this we need only show that if $\mathbf{v}^f$ and $\mathbf{v}^g$ are in this set and $d(\mathbf{v}^f,\mathbf{v}^g) > 1$, then a third point of this set lies between them.

Clearly, there is no harm in assuming $f < g$. Making this assumption, let $k = j(\mathbf{v}^g)$, so that $\mathbf{v}^f, \mathbf{v}^f \oplus \mathbf{e}, \mathbf{v}^g$ and $\mathbf{v}^g \oplus \mathbf{e}$ are all in the set $\hat{S} = \{\mathbf{s}^1,\ldots,\mathbf{s}^k\}$. Either $\mathbf{v}^g = \mathbf{s}^k$ or $\mathbf{v}^g \oplus \mathbf{e} = \mathbf{s}^k$. Assume $\mathbf{v}^g = \mathbf{s}^k$, without loss of generality. Since $\hat{S}$ is isometric, there is a path of length $d(\mathbf{v}^g,\mathbf{v}^f)$ from $\mathbf{v}^g$ to $\mathbf{v}^f$ in $\hat{S}$. This path must only pass through points with first coordinate zero. Let $\mathbf{s}'$ be the point immediately after $\mathbf{v}^g$ on this path. By assumption $\hat{S} \backslash \{\mathbf{v}^g\}$ is also isometric. This means there is a path of length two from $\mathbf{v}^g \oplus \mathbf{e}$ to $\mathbf{s}'$ in $\hat{S} \backslash \{\mathbf{v}^g\}$. Hence, $\mathbf{s}' \oplus \mathbf{e}$ must lie in $\hat{S} \backslash \{\mathbf{v}^g\}$. Since both $\mathbf{s}'$ and $\mathbf{s}' \oplus \mathbf{e}$ are in $\hat{S}$, $\mathbf{s}' \in \{\mathbf{v}^1,\ldots,\mathbf{v}^g\}$, and the assertion has been proved. This establishes H3, because if V_0 is isometrically shellable then so is the set $S \cap (S \oplus \mathbf{e}) = V_0 \cup (V_0 \oplus \mathbf{e})$. ⁝

Since isometrically shellable sets are connected, a consequence of Theorems 2 and 3.1.4 is that isometrically shellable sets are simple.

Theorem 3.3.3. The maximal subcubes of an isometrically shellable set can be ordered such that no cube is in the union of the previous cubes.

Proof. The statement of the theorem will not be proved directly, but rather it will be shown that,

*) if S is a nonempty isometrically shellable set, and $Q_1, Q_2, \ldots, Q_k$ is any collection of $k > 0$ distinct maximal subcubes of S, then some point is contained in exactly one of the Q_i.

To prove the theorem from *), first take *all* maximal subcubes of S. By *), one of these cubes is not contained in the union of the others. Make this cube the last cube in the order. Now, apply *) to all remaining cubes. Again, a cube not contained in the other remaining cubes is found. Make this the second to last cube in the order. By repeating this, an ordering of all cubes is obtained with the desired properties.

We now prove *). Let $S = \{\mathbf{s}^1,\ldots,\mathbf{s}^m\}$ be a nonempty set with isometric shelling as labeled. Let $Q_1,\ldots,Q_k$, $k > 0$, be distinct maximal subcubes of S. Let j be maximal such that $\mathbf{s}^j \in Q_1 \cup \cdots \cup Q_k$. Let $\hat{S} = \{\mathbf{s}^1,\ldots,\mathbf{s}^j\}$ and let N be the set of neighbors in $\hat{S}$ of $\mathbf{s}^j$, not including $\mathbf{s}^j$. Let $\hat{Q}$ be the smallest subcube of K_2^n containing $\mathbf{s}^j$ and N. Since $\hat{S} \backslash \{\mathbf{s}^j\}$ is simple, and the complement of a simple set is simple, the set $X = \hat{Q} \backslash (\hat{S} \backslash \{\mathbf{s}^j\}) = \{\mathbf{s}^j\} \cup (\hat{Q} \backslash \hat{S})$ is also simple. But, $\hat{Q} \backslash \hat{S}$ is disjoint from N, so it has no neighbors of $\mathbf{s}^j$, so $\mathbf{s}^j$ is the only member of some component of X. Since X is simple and therefore connected, the only possibility is that $\hat{Q} \backslash \hat{S}$ is empty, i.e., $\hat{Q} \subseteq \hat{S}$.

Thus, $\hat{Q}$ is the unique maximal subcube of $\hat{S}$ containing $\mathbf{s}^j$. Each Q_i is a maximal subcube of $\hat{S}$, so precisely one of them contains $\mathbf{s}^j$, the one that equals $\hat{Q}$. ⁝

From the point of view of this thesis, isometrically shellable sets are very important. There remain several unsolved problems concerning these mysterious sets. For example, we do not know if all simple sets are isometrically shellable. Furthermore, the next section concerns a subfamily of isometrically shellable sets, but here again it is not known if the inclusion is proper. Both the family of simple sets and the family of orthant sets, of the next section, are known to be closed under complementation. Thus, both inclusions would be proper if the following question had negative answer.

Unsolved Problem. Is the complement of every isometrically shellable set isometrically shellable?

In truth, the author has spent more time on this problem than on anything else in this thesis. This problem (in a different form) also is raised in the Ph.D. thesis of Kathy Hoke [31]. Attempting to solve this problem was the motivation for most of the results in this chapter.

3.4. Orthant Sets

A useful correspondence can be made between the orthants of $\mathbf{R}^n$ and the vertices of the n-cube. It is most useful to let $K_2^n = \{\pm 1\}^n$. Then, the correspondence is that $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in K_2^n$ *represents* the closed orthant

$$\{\mathbf{y} \in \mathbf{R}^n \mid x_i y_i \geq 0,\ i = 1, 2, \ldots, n\}.$$

This correspondence is good because two "adjacent" orthants, in the sense that they have $(n-1)$-dimensional intersection, correspond to adjacent vertices of the n-cube. Using this correspondence and convexity an interesting hereditary family can be constructed.

Definition. A subset S of K_2^n is an *orthant set* if there is a convex subset Y of $\mathbf{R}^n$ such that S is the set of representatives of the closed orthants which Y meets.

It is clear that because there is an isometry of $\mathbf{R}^n$ which permutes the orthants in a manner matching any given isometry of the n-cube, orthant sets are taken to orthant sets by isometries of K_2^n. Also, by inclusion of $\mathbf{R}^{n-1}$ in $\mathbf{R}^n$, orthant sets in K_2^{n-1} produce orthant sets in K_2^n. Thus, the orthant sets form a natural family.

Given any convex set $Y \subseteq \mathbf{R}^n$, we may arbitrarily select a single point from each closed orthant which Y meets. Let Z be the convex hull of all these points. Note Y and Z represent the same orthant set, say S, and Z is a polytope with at most $|S|$ vertices. Moreover, there is a convex neighborhood of Z which meets the same closed orthants as Z. If a closed orthant meets Z we may select a point from this neighborhood of Z which is in the *interior* of that orthant. Hence, the vertices of the representing polytope may be assumed to each have only nonzero coordinates.

Theorem 3.4.1. If $S \subseteq K_2^n$ is an orthant set then S^c is an orthant set.

Proof. Let $S \subseteq K_2^n$ be an orthant set with $m > 0$ members. (If S is empty, the complement of S is obviously an orthant set because it is represented by all of $\mathbf{R}^n$.) Let S be represented by some polytope Z. For each member of S, select a point of Z in the corresponding orthant. By considering each of these points to be a row vector, from these m vectors construct an $m \times n$ real matrix X. Let

$$A = \{\mathbf{a} \in \mathbf{R}^n \mid X\mathbf{a} < \mathbf{0}\}.$$

A is a convex set and therefore represents some orthant set $P \subseteq K_2^n$. We claim $P = S^c$.

First, we show P and S are disjoint. Suppose, to the contrary that P meets S. Then there is some row $\mathbf{x}$ of X, which is in the same orthant as some $\mathbf{a} \in A$. This is impossible because $(\mathbf{x}, \mathbf{a}) < 0$ from the definition of A.

Finally, we show $P \cup S = K_2^n$. Suppose, to the contrary, that there is some closed orthant which does not meet A or Z. It will be assumed that this is the positive orthant, because essentially the same proof applies for an arbitrary orthant. By assumption, there is no solution $\mathbf{a}$ to $X\mathbf{a} < 0$ and $\mathbf{a} \geq 0$. By a relative of the Farkas' lemma due to Ville [32,p.248], this implies the existence of a row m-vector $\mathbf{y}$, such that $\mathbf{y}\,X \geq \mathbf{0}$, $\mathbf{y} \geq \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$. By application of a scale factor, it can be assumed that $\mathbf{y}$ has unit coordinate sum. Thus, $\mathbf{y}$ corresponds to a convex combination of the rows of X such that the result is in the positive orthant. Since Z is the convex hull of the rows of X, Z meets the closed positive orthant, a contradiction. ∎

Theorem 3.4.2. The orthant sets form a hereditary family.

Proof. We already know that the orthant sets are a natural family closed under complementation. Thus, we need only prove properties H1 and H2. Let Z be a polytope representing an orthant set $S \subseteq K_2^n$. As shown earlier it can be assumed that Z meets the *interior* of every closed orthant it meets. Thus,

$Z' = \{\mathbf{z} \in Z | z_1 > 0\}$ is a convex set representing $S_1 = \{\mathbf{s} \in S | s_1 = 1\}$. Likewise, the intersection of S with *any* cube of co-dimension one is an orthant set. This is all that's required to establish H1.

To establish H2 it will be shown that $U = S \cup \{(-s_1, s_2, \ldots, s_n) | (s_1, s_2, \ldots, s_n) \in S\}$ is an orthant set. Let Z be a polytope representing S and let $\hat{Z} = \{(0, z_2, \ldots, z_n) | \mathbf{z} \in Z\}$, the projection of Z to an axis plane. This is convex and represents U. ∎

Corollary 3.4.3. Orthant sets are simple.

Proof. All that must be shown is that orthant sets are connected, since by Theorem 2 the orthant sets form a hereditary family and by Theorem 3.1.4 a hereditary family of connected sets contains only simple sets.

Let Z be a polytope which represents some orthant set S. Let $\mathbf{x}, \mathbf{y} \in Z$ correspond to $\mathbf{q}, \mathbf{r} \in S$, respectively. It may be assumed that $\mathbf{x}$ and $\mathbf{y}$ lie in the topological interior of Z and $\mathbf{x}$ and $\mathbf{y}$ have no coordinates equal to zero. Suppose that as a point moves gradually along the segment from $\mathbf{x}$ to $\mathbf{y}$, anytime it moves into a new orthant the new orthant is a neighbor of the old orthant. Then the segment represents a connected subset of S containing $\mathbf{q}$ and $\mathbf{r}$.

To show that this assumption can be met, note that the convex combination $(1 - t)\mathbf{x} + t\mathbf{y}$, $0 \le t \le 1$, has i^{th} coordinate equal to zero at the single value $t = t^{(i)} = x_i/(x_i - y_i)$. If $x_i - y_i = 0$ or if $t^{(i)}$ is not in the unit interval, coordinate i is never zero. The point $\mathbf{y}$ can be replaced by any point $\mathbf{y}'$ in some small neighborhood of $\mathbf{y}$, and still be in the same open orthant and in Z. The $t^{(i)}$, $1 \le i \le n$, are now functions of $\mathbf{y}'$. For $i \ne j$, $t^{(i)} = t^{(j)}$ on a set of measure zero in this neighborhood. Hence, there is a $\mathbf{y}'$ for which no two coordinates are zero at any point on the segment from $\mathbf{x}$ to $\mathbf{y}'$. As a point moves on the segment from $\mathbf{x}$ to $\mathbf{y}'$, the sequence of orthants whose interiors contain that point represent the desired path in S. ∎

The proof of this corollary made use of getting things into "general position". The proof of the next theorem is similar in this respect. Basically, we can pick any point in the interior of a polytope and homothetically contract and expand the polytope about this point. If we could be sure that only one orthant was lost or gained at a time the proof would be trivial. In order to make the proof rigorous, we begin with the lemma below about orthants in R^n.

Lemma 3.4.4. Let X and Y be any two distinct closed orthants of R^n. There exists a vector $\mathbf{v} \in R^n$ such that for any $a > 0$, $X + a\mathbf{v} \subseteq X$ and $Y \subseteq Y + a\mathbf{v}$, while for any $a < 0$, $X \subseteq X + a\mathbf{v}$ and $Y + a\mathbf{v} \subseteq Y$. Furthermore, $\mathbf{v}$ has the following property. Let $\mathbf{p} \in X$ and $\mathbf{q} \in Y$ be any points such that $\{(1 - t)\mathbf{p} + t\mathbf{q} | 0 \le t \le 1\} \backslash (\{\mathbf{p}\} \cup \{\mathbf{q}\})$ is disjoint from $X \cup Y$. Then $\mathbf{p} \notin X + a\mathbf{v}$ and $\mathbf{q} \notin Y - a\mathbf{v}$ for any $a > 0$.

Proof. Associated to any orthant of R^n is that member of $\{\pm 1\}^n$ which is in its interior. If $\mathbf{x}$ is associated with X and $\mathbf{y}$ with Y, we claim $\mathbf{v} = \mathbf{x} - \mathbf{y}$ satisfies all requirements stated in the lemma. Assume, without loss of generality that X is the positive orthant. Then $\mathbf{v} \ge \mathbf{0}$. It follows that if $a > 0$, $X + a\mathbf{v} \subseteq X$ and if $a < 0$, $X \subseteq X + a\mathbf{v}$.

Now suppose $\mathbf{p}$ and $\mathbf{q}$ are in X and Y, respectively, and there is no point in the open segment between them which lies in X or Y. The approach is to show that there is some coordinate where $\mathbf{p}$ is zero and $\mathbf{v}$ is positive. If $\mathbf{p}$ is zero in some coordinate where $\mathbf{v}$ is positive, then $\mathbf{p} \notin X + a\mathbf{v}$, for $a > 0$. The statements about Y follow by interchanging the roles of X and Y in the proof.

First, assume $\mathbf{p} \ne \mathbf{q}$. Note that there must be some coordinate where $\mathbf{p}$ is zero and $\mathbf{y}$ is –1. If not, wherever $\mathbf{q}$ is negative, $\mathbf{p}$ is positive and for sufficiently small t, $(1 - t)\mathbf{p} + t\mathbf{q}$ is in the positive orthant, contradicting the hypothesis. Thus, $\mathbf{p}$ is zero in some coordinate where $\mathbf{v}$ is positive.

If $\mathbf{p} = \mathbf{q}$, $\mathbf{p}$ must be zero in any coordinate where $\mathbf{v}$ is positive, and there is at least one such coordinate, since $\mathbf{v} \ne \mathbf{0}$. ∎

Theorem 3.4.5. If $S \subseteq K_2^n$, $n \ge 1$, is an orthant set and $\mathbf{s} \in S$ then there is a sequence $P_1, P_2, \cdots, P_{2^n}$ of orthant sets such that $P_1 = \{\mathbf{s}\}$, $P_{|S|} = S$, and for each i, $1 \le i < 2^n$, $P_i \subseteq P_{i+1}$, and for each set in the sequence $|P_i| = i$.

Proof. Take any full dimensional polytope representing S and replace it by a compact convex set W, such that a neighborhood of W also represents S. Furthermore, W will be assumed to have analytic bounding manifold. In the interior of W pick a point $\mathbf{w}$ such that $\mathbf{w}$ represents $\mathbf{s}$ and has no coordinates zero. Now define the function $f: \mathbf{R}^n \rightarrow \mathbf{R}$ by

$$f(\mathbf{z}) = \min \{ t \geq 0 | \mathbf{w} + t^{-1}(\mathbf{z} - \mathbf{w}) \in W \} \,.$$

By convention $f(\mathbf{w}) = 0$. This is a convex function, which is analytic for $\mathbf{z} \neq \mathbf{w}$. Also, letting $F_r = \{ \mathbf{z} | f(\mathbf{z}) \leq r \}$, then $F_0 = \{ \mathbf{w} \}$ and $F_1 = W$, which represents S. Our hope is that as r increases from zero to infinity, the orthant set represented by F_r increases in steps of size at most one. Unfortunately, this might not be the case, but it will be shown that some translate of f by a small vector has the desired property. Clearly, if $f(\mathbf{z})$ is replaced by $f(\mathbf{z} + \mathbf{c})$ the sets F_r are replaced by the sets $F_r - \mathbf{c}$, and for any sufficiently short $\mathbf{c}$, $F_0 - \mathbf{c}$ and $F_1 - \mathbf{c}$ still represent $\{ \mathbf{s} \}$ and S, respectively.

Let X be an arbitrary closed orthant. The smallest r for which F_r meets X is the minimum of $f(\mathbf{z})$ for $\mathbf{z} \in X$. Since $f(\mathbf{z})$ goes to infinity as $\mathbf{z}$ goes to infinity, in searching for the minimum of f we can restrict attention to some large but compact subset of X. Hence, the minimum of $f(\mathbf{z})$, $\mathbf{z} \in X$, is *achieved* at some point $\mathbf{p} \in X$. It can't be achieved at two points because $f(\mathbf{p}) = f(\mathbf{p}')$ together with convexity of f would imply that the minimum is achieved at all points on the segment between $\mathbf{p}$ and $\mathbf{p}'$. Then analyticity of f would imply that f is constant along the line containing this segment. This would contradict that $f(\mathbf{z})$ goes to infinity as $\mathbf{z}$ goes to infinity.

For any closed orthant X we have the function

$$g_X(\mathbf{c}) = \min \{ f(\mathbf{z} + \mathbf{c}) | \mathbf{z} \in X \}.$$

a continuous function of $\mathbf{c}$.

Let Y be any closed orthant distinct from X. Assume that $\mathbf{p}$ is the minimizer of f in X and $\mathbf{q}$ is the minimizer in Y. Suppose that $f(\mathbf{p}) = f(\mathbf{q})$. The condition of the lemma holds because any point in the interior of the segment from $\mathbf{p}$ to $\mathbf{q}$ has a value of f not larger than $f(\mathbf{p})$ and therefore does not lie in X or Y. The vector $\mathbf{v}$ given by the lemma will now have the property that for any $a > 0$, $g_X(a\mathbf{v}) > g_Y(a\mathbf{v})$ and $g_X(-a\mathbf{v}) < g_Y(-a\mathbf{v})$.

What has just been done applies equally well to the translate of f by $\mathbf{c}$. Thus, on each line parallel to the direction $\mathbf{v}$ there is at most one point $\mathbf{c}$ such that $g_X(\mathbf{c}) = g_Y(\mathbf{c})$. Hence, for any two orthants the solutions $\mathbf{c}$ to $g_X(\mathbf{c}) = g_Y(\mathbf{c})$ have measure zero. Therefore, arbitrarily short vectors $\mathbf{c}$ exist such that $g_X(\mathbf{c}) \neq g_Y(\mathbf{c})$ for every two closed orthants X and Y. For such a $\mathbf{c}$ the sets $F_r - \mathbf{c}$ as r goes from zero to infinity represent the desired sequence of orthant sets. ∎

Since orthant sets are isometric, the initial part of the sequence, $P_1, P_2, \ldots, P_{|S|}$, is an isometric shelling of S. Thus,

Corollary 3.4.6. Orthant sets are isometrically shellable.

It is not clear how far nondegeneracy arguments can be pushed. Suppose A and B are two polytopes, $\mathbf{a} \in A$ and $\mathbf{b} \in B$. For any $0 \leq t \leq 1$ and $r \geq 0$ let $C(t, r)$ be the homothetic expansion by factor r of the polytope $(1 - t)A + tB$ about the point $(1 - t)\mathbf{a} + t\mathbf{b}$. If the size of the orthant set of $C(t, r)$ changed by at most one for small changes in t and r, the following conjecture about "deforming" orthant sets would be easy to prove.

Conjecture. If G and H are two orthant sets with $|G| < |H|$, then there is a sequence of orthant sets $S_1, S_2, \ldots, S_m$ with $S_1 = G$, $S_m = H$, and for each i, $1 \leq i < m - 1$, $|G| \leq |S_i| \leq |H|$ and the symmetric difference of S_i and S_{i+1} is a one element set.

We do not have a rapid method for testing $S \subseteq K_2^n$ for being an orthant set. At least it can be seen that this problem is decidable. Let $T = S^c$. It was shown in the proof of Theorem 1 that if S is an orthant set, there will be real vectors $\mathbf{z}^1, \ldots, \mathbf{z}^m$, one for each member of S and real vectors $\mathbf{a}^1, \ldots, \mathbf{a}^l$, one for each member of T, such that $(\mathbf{z}^i, \mathbf{a}^j) < 0$ for all i and j. Furthermore, if such vectors can be found, the convex hull of the $\mathbf{z}^i$ will represent S. Suppose, instead, that this convex hull contains a point $\mathbf{x}$ in a closed orthant corresponding to a member of T. Then there is an $\mathbf{a}^j$ in the same closed orthant, so $(\mathbf{x}, \mathbf{a}^j) \geq 0$, contradicting the constraints $(\mathbf{z}^i, \mathbf{a}^j) < 0$.

The problem of representing an orthant set can therefore be viewed as solving the system $(\mathbf{z}^i, \mathbf{a}^j) < 0$, subject to the constraints that each $\mathbf{z}^i$ and each $\mathbf{a}^j$ lie in predetermined orthants. This does not appear as easy to solve as a linear program, but it can be solved in a number of operations bounded by some function of n, by a very general theorem of Tarski [33,p.323].

3.5. Scale Free Orthant Sets

In the last section, in the proof of Theorem 3.4.1, it was shown that the complement of any orthant set can be represented by the solution set of a system $A\mathbf{x} < \mathbf{0}$, for some matrix A. Since every complement of an orthant set is also an orthant set, all orthant sets can be so represented.

Given an $m \times n$ real matrix A, say A' is a *scaling* of A if it results from A by multiplying the entries by positive real numbers, possibly all distinct. Clearly, the relationship of one matrix being a scaling of another is an equivalence relation.

Definition. A *scale free system*, $A\mathbf{x} < \mathbf{0}$, is one such that the solution set of each scaled system $A'\mathbf{x} < \mathbf{0}$ meets the same set of closed orthants as the original one.

Definition. $S \subseteq K_2^n$ is a *scale free orthant* set if it is an orthant set that can be represented by a scale free system.

Since scale free orthant sets are orthant sets, they are included in every hereditary family in this chapter. It will be shown that they, too, form a hereditary family. For the moment, it is easy to see that they form a natural family. The coordinate permutation isometries of K_2^n correspond to permuting the columns of A and the translation isometries of K_2^n correspond to negating certain columns of A. The resulting systems are still scale free. Moreover, if there is a scale free system in the variables $x_1, \ldots, x_n$ which produces $S \subseteq K_2^n$, then adjoining the single equation $x_{n+1} < 0$ gives another scale free system, producing $S \times \{-1\} \subseteq K_2^{n+1}$. Hence, scale free orthant sets form a natural family.

At this point, the reader may think that this family is not very extensive, but the note at the end of section 2.5 in effect shows that all retracts are scale free orthant sets. Another major class of scale free orthant sets are the stars. Identifying K_2^n with $\{\pm 1\}^n$, suppose S is a star with center $(-1, -1, \ldots, -1)$. We will show how to construct a scale free representation of S. For every $\mathbf{u} \in S^c$, construct a real vector $\hat{\mathbf{u}}$ from $\mathbf{u}$ by changing every -1 to a 0 and leaving the $+1$ entries unchanged. Consider the system of equations in $\mathbf{x}$,

$$\hat{\mathbf{u}}^T \mathbf{x} < 0, \quad \text{for all } \mathbf{u} \in S^c . \qquad (*)$$

Since $\hat{\mathbf{u}}$ is a member of the closed orthant containing $\mathbf{u}$, no solution $\mathbf{x}$ may be in the same orthant as a $\mathbf{u} \in S^c$. This will also be true of any scaling of the system (*). It remains to show that any member of S is represented by a solution of (*). For any $\mathbf{s} \in S$, form $\underline{\mathbf{s}}$ by changing all $+1$ coordinates to 0 and leaving all -1 coordinates fixed. We claim $\hat{\mathbf{u}}^T \underline{\mathbf{s}} < 0$, for every $\mathbf{u} \in S^c$.

Note, $\mathbf{u}$ must have a $+1$ in some coordinate where $\mathbf{s}$ is -1; otherwise $\mathbf{u}$ would be a member of the star S. In the inner product $\hat{\mathbf{u}}^T \underline{\mathbf{s}}$, the only nonzero summands are $+1$'s from $\hat{\mathbf{u}}$ multiplied by -1's from $\underline{\mathbf{s}}$. Thus, the inner product is negative and will be negative for any scaling of $\hat{\mathbf{u}}$. Since $\underline{\mathbf{s}}$ is in the closed orthant containing $\mathbf{s}$, all of S is represented.

Lemma 3.5.1. If $A\mathbf{x} < \mathbf{0}$ is a scale free system, then if any inequality $(\mathbf{a}' + \mathbf{b}')^T \mathbf{x} < 0$, where $\mathbf{a}'$ and $\mathbf{b}'$ are scalings of any two rows of A, is adjoined to the system, another scale free system producing the same scale free orthant set results.

Proof. Without loss of generality, assume $\mathbf{a}'$ and $\mathbf{b}'$ are scalings of the first two rows of A. Since the new system can only be more restrictive than the original system, if the lemma is false, we can assume there is some closed orthant not meeting the solution set of the new system, but meeting the solution set of the original system. Without loss of generality, let this orthant be the positive orthant.

By Ville's theorem, there is a vector $\mathbf{y} \ge 0$ and real number $\gamma \ge 0$ such that,

$$\mathbf{y}^T A + \gamma(\mathbf{a}' + \mathbf{b}') \ge \mathbf{0}, \quad (\mathbf{y}^T, \gamma) \ne \mathbf{0} . \qquad (**)$$

Define a vector $\mathbf{w}$ of the same dimension as $\mathbf{y}$, and let $w_i = y_i$, for $i \geq 3$. For $i = 1, 2$, let $w_i = y_i + \gamma$. Now select A' to be a scaled copy of A where only the first two rows may be changed. If $w_1 \neq 0$, change the first row from $\mathbf{a}$ to $w_1^{-1}(y_1\mathbf{a} + \gamma\mathbf{a}')$, and if $w_2 \neq 0$, change the first row from $\mathbf{b}$ to $w_2^{-1}(y_2\mathbf{b} + \gamma\mathbf{b}')$. By (**) we have that $\mathbf{w}^T A' \geq \mathbf{0}$, $\mathbf{w} \geq \mathbf{0}$ and $\mathbf{w} \neq \mathbf{0}$. Then, by Ville's theorem, the system $A'\mathbf{x} < \mathbf{0}$ will not meet the positive orthant, a contradiction.

Thus, the system with $(\mathbf{a}' + \mathbf{b}')^T\mathbf{x} < 0$ adjoined will represent the same orthant set as the original system. Furthermore, the new system is scale free because any scaling of it can be achieved by first scaling the original (scale free) system and then applying the first part of the lemma. :

Given any scale free system, all that matters is whether a given entry is positive, negative or zero. Any scale free system can therefore be represented by a matrix with entries from $\{\pm 1, 0\}$. The lemma above shows how to form new rows of the matrix without affecting the scale free set represented. Given any two rows $\mathbf{a}$ and $\mathbf{b}$, the following table shows the possible entries of $\mathbf{a}' + \mathbf{b}'$, as functions of the entries of $\mathbf{a}$ and $\mathbf{b}$.

□	–1	0	+1
–1	–1	–1	?
0	–1	0	+1
1	?	+1	+1

In this table the symbol "?" denotes that the value of the combination can be any of $-1, 0, +1$, depending on the choice of scaling. In presenting a scale free system there is no harm in adjoining all rows of the "□ closure" of the original rows to the system. The □ closure is the set of all row vectors one can obtain by repeated application of □ to the original rows. Alternatively, it is the set of $-1, 0, +1$ "sign patterns" in all sums of scaled versions of the original rows.

Theorem 3.5.2. For every matrix A whose rows are a □ closed subset of $\{\pm 1, 0\}^n$, the system $A\mathbf{x} < \mathbf{0}$ is scale free. The closed orthants met by the solution set are those not containing any of the rows.

Proof. Let A be a matrix whose rows are a □ closed subset of $\{\pm 1, 0\}^n$. Clearly, the solutions to $A\mathbf{x} < \mathbf{0}$ never contain a point $\mathbf{x}$ in the same closed orthant as any of the rows of A.

Suppose there is no solution $\mathbf{x}$ in, say, the positive orthant. By Ville's theorem, there is a $\mathbf{y} \geq \mathbf{0}$, $\mathbf{y} \neq \mathbf{0}$ such that $\mathbf{y}^T A \geq \mathbf{0}$. This means a sum of scaled rows of A is nonnegative. The sign pattern of this scaled combination is in the □ closure of the rows of A, by definition of □ closure. By assumption then, some row of A is of the form $\{1, 0\}^n$, i.e., in the positive orthant.

Thus, the closed orthants meeting the solution set of the system are precisely those orthants not containing any of the rows of A. Furthermore, our argument would work just as well if an arbitrary scaling was applied to the entries of A, so the system is scale free. :

Corollary 3.5.3. The family of scale free orthant sets is hereditary and so is the family of complements of scale free orthant sets.

Proof. We already know the scale free orthant sets form a natural family. Given any scale free orthant set $S \subseteq \{\pm 1\}^n$, let V be the □ closed subset of $\{\pm 1, 0\}^n$ generated by the rows of some defining linear system for S. Now, Theorem 2 can be applied to give □ closed spaces defining the sets derived from S, as is done below. In each case, it is straightforward to verify that the desired set is produced.

To prove H1 holds, it is sufficient to show $S \cap \{\mathbf{s} \mid s_1 = 1\}$ is scale free orthant. A □ closed space producing it is the □ closure of $V \cup \{(-1, 0, 0, \ldots, 0)\}$.

To establish H2, it is sufficient to show $S \cup \{(-s_1, s_2, \ldots, s_n) \mid (s_1, s_2, \ldots, s_n) \in S\}$ is scale free orthant. A □ closed set for this space is,

$$\{(0, v_2, \ldots, v_n) \mid (0, v_2, \ldots, v_n) \in V\}.$$

To establish H3, it is sufficient to show $S \cap \{(-s_1, s_2, \ldots, s_n) \mid (s_1, s_2, \ldots, s_n) \in S\}$ scale free orthant. A □ closed set producing this space is,

$$\{\pm 1, 0\} \times \{(v_2, \ldots, v_n) \mid (v_1, v_2, \ldots, v_n) \in V,\ \text{for some } v_1\}\,.$$

To establish that the complements of scale free orthant sets are also hereditary, not much more work needs to be done. A family satisfies H2 if and only if the complementary family satisfies H3, so we need only establish H1. The scale free set defined by the $\square$ closed set,

$$\{(+1, v_2, \ldots, v_n) \mid (v_1, v_2, \ldots, v_n) \in V,\ \text{for some } v_1 \neq -1\}$$

is $S \cup (\{-1\} \times \{\pm 1\}^{n-1})$. The complement of this $S^c \cap \{\mathbf{s} | s_1 = 1\}$, establishing H1.

Finally, it must be shown that the complements of scale free sets form a natural family. But, if $\boldsymbol{F}$ is a natural family with property H1, it is easily shown that the complements form a natural family. ∎

Theorem 2 tells us that any $\square$ closed set "produces" a scale free orthant set, but it leaves open the problem of finding a $\square$ closed set, given a scale free orthant set. This is solved by the following result, which shows that for every scale free orthant set, there is a smallest $\square$ closed set.

Theorem 3.5.4. Let $V \subseteq \{\pm 1, 0\}^n$ be a $\square$ closed set producing the scale free orthant set $S \subseteq \{\pm 1\}^n$. If $\mathbf{q} \in \{\pm 1, \ast\}^n$ denotes a maximal subcube of S^c, then $\ddot{\mathbf{q}}$, formed by changing all $\ast$'s to 0's, is a member of V. Furthermore, the $\square$ closure of the set of all such $\ddot{\mathbf{q}}$ produces S.

Proof. Under the assumptions in the statement of the theorem, let Q, represented by the vector $\mathbf{q}$, be a maximal subcube of S^c. For every point in Q there must be a member of V in the same closed orthant. The convex hull of all such members of V meets each closed orthant containing a point of Q. It follows, by taking an appropriate convex combination, that there is a point in the convex hull of these members of V, which is zero in every direction of Q. Taking an example, let $\mathbf{q} = (\ast, \ast, \ast, +1, -1, +1)$. Then, the convex hull contains some real vector $\mathbf{x} = (0, 0, 0, x_4, x_5, x_6)$. Note, $x_4 \geq 0$, $x_5 \leq 0$, $x_6 \geq 0$, because $\mathbf{x}$ is the convex combination of vectors with this property.

By definition of $\square$, there will be a $\square$ combination of the corresponding members of V to yield the sign vector of $\mathbf{x}$, say $\mathbf{v} = (0, 0, 0, v_4, v_5, v_6)$. Since V is $\square$ closed, by assumption, $\mathbf{v} \in V$. Since S^c represents the set of orthants met by V, none of v_4, v_5, v_6 may be zero, since this would mean Q was not a maximal cube in S^c. It follows $\mathbf{v} = (0, 0, 0, +1, -1, +1) = \ddot{\mathbf{q}}$. This argument generalizes to show that for any $\mathbf{q}$ describing a maximal subcube, $\ddot{\mathbf{q}} \in V$.

To complete the proof, it must be shown that some element of the $\square$ closure of the $\ddot{\mathbf{q}}$'s lies in the same closed orthant as an arbitrary point, $\mathbf{t}$, in S^c. But, $\mathbf{t}$ is in at least one maximal subcube of S^c, represented by the vector $\mathbf{q}$, say. Then, $\ddot{\mathbf{q}}$ itself is in the same orthant as $\mathbf{t}$. ∎

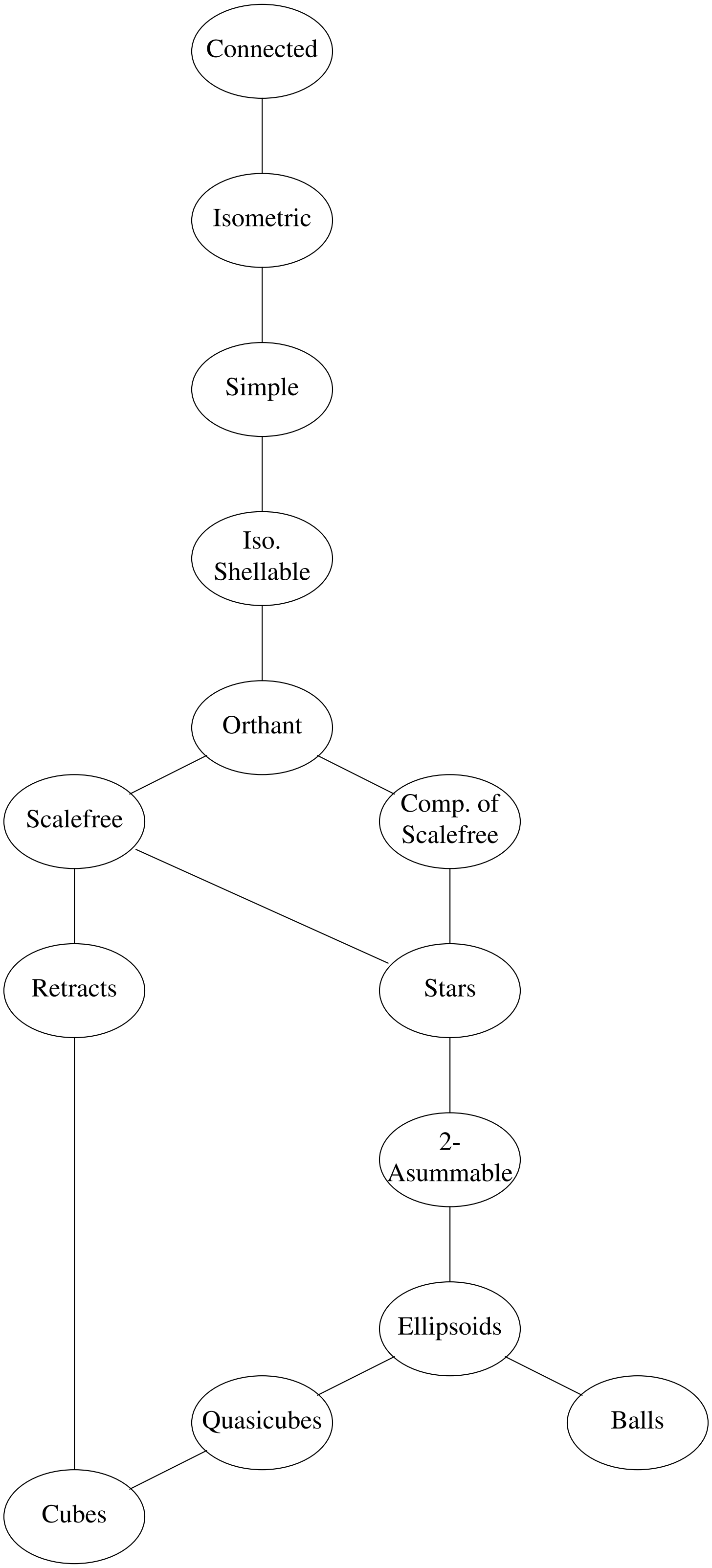
This theorem provides a reasonably effective way to determine if a set is scale free orthant. This will be used to answer the important question, "Is every orthant set also scale free orthant?" The following example shows that the answer is "No". In $\{\pm 1\}^4$, let $S =$

$$\{(-1, -1, -1, -1), (-1, -1, -1, +1), (-1, -1, +1, +1), (-1, +1, +1, +1), (+1, +1, +1, +1)\}\,.$$

The subgraph induced by S is a path of length 4 and S is isometric. Thus, S is a retract (since all isometrically induced trees are retracts) and therefore a scale free orthant set. Since the family of orthant sets is closed under complementation, the set $R = S^c$ is also an orthant set, but Theorem 4 will allow us to show that R is not scale free.

The maximal subcubes of $R^c\,(= S)$ are $\mathbf{q}^1 = (-1, -1, -1, \ast)$, $\mathbf{q}^2 = (-1, -1, \ast, +1)$, $\mathbf{q}^3 = (-1, \ast, +1, +1)$ and $\mathbf{q}^4 = (\ast, +1, +1, +1)$. However, a possible value of $\ddot{\mathbf{q}}^1 \square \ddot{\mathbf{q}}^4$ is $(-1, 0, 0, +1)$. This vector is in the closed orthant containing $(-1, +1, -1, +1) \notin R^c$. Thus, R^c is not the complement of a scale free orthant set, since this would contradict Theorem 4. Therefore, as claimed, R is not a scale free orthant set.

The next chapter does not discuss any new set families of K_2^n, so the following diagram summarizes the inclusion relationships of most of the important families that have been discussed. All families below the isometric sets are hereditary, with the exception of balls. As mentioned before, the author does not know if the two inclusions involving the isometrically shellable sets are strict.


Connected
Isometric
Simple
Iso. Shellable
Orthant
Scalefree
Comp. of Scalefree
Retracts
Stars
2-Asummable
Ellipsoids
Quasicubes
Balls
Cubes

4. Partitioning, Covering and Packing Hamming Spaces

This chapter is a collection of diverse topics concerning the classical combinatorial questions of partitioning, covering and packing, as they relate to K_2^n, and in some cases K_b^n.

4.1. Hamiltonian Decompositions

We begin with a discussion of graph decompositions into cycles. A problem stated by Ringel in a 1955 paper [34] is to show that the graph of an even-dimensional cube has a Hamiltonian decomposition. The decomposition in this problem is an *edge*-decomposition. That is, in K_2^n we wish to find a collection of Hamiltonian cycles such that each edge of K_2^n appears in exactly one of the cycles. Since each Hamiltonian cycle contains two edges incident to each vertex, $n/2$ Hamiltonian cycles are required. Clearly, n must be even for the decomposition to be possible. If n is a power of two and greater than one, the paper by Ringel provides such a decomposition.

Ringel's problem was completely solved using a paper published by Aubert and Schneider in 1982 [35], as noted by J.C. Bermond [36]. Let C_m denote the graph which is a cycle of m vertices, $m \geq 3$. A result in that paper is,

I) If G is 4-regular and has a Hamiltonian decomposition then $G \times C_m$ also has a Hamiltonian decomposition, for any $m \geq 3$.

Prior to this result, there was the result of Kotzig [37],

II) $C_m \times C_l$ has a Hamiltonian decomposition.

Other results useful for the case of K_b^n are the result of Myers [38] that

III) K_b^2 has a Hamiltonian decomposition, $b \geq 2$,

and the well known result (see [39,p.89]) that,

IV) K_b has a Hamiltonian decomposition for $b = 2k+1$, $k \geq 1$.

The following theorem is a compilation of results that have appeared elsewhere, it is included in this thesis because it shows that a gradual accumulation of results led to the complete solution of an important problem.

Theorem 4.1.1. For $n \geq 1$, $b \geq 2$, K_b^n has a Hamiltonian decomposition exactly when the degree is even, i.e. $2|n(b-1)$.

Proof. It is clear that when the degree of the regular graph K_b^n is odd there is no Hamiltonian decomposition.

For purposes of this proof only, if G and H are graphs on identical vertex sets define $G+H$ to be that graph with the same vertex set and a number of edges from $\mathbf{x}$ to $\mathbf{y}$ equal to the sum of the number from $\mathbf{x}$ to $\mathbf{y}$ in G and the number from $\mathbf{x}$ to $\mathbf{y}$ in H. In our application G and H will never have edges spanning the same vertex pair. This "addition" is commutative and associative, but it does not distribute with Cartesian product, ×. Instead, we have the rather unusual property

$$(G_1 + G_2) \times (H_1 + H_2) = (G_1 \times H_1) + (G_2 \times H_2) \ . \qquad (*)$$

The proof uses induction on n. Results III and IV handle the smallest n for which a decomposition must be found.

For larger n for which $2|n(b-1)$, write $n = s+t$, $s \geq t$, where $2|s(b-1)$, $2|t(b-1)$, and $s-t$ is minimized. If b is odd $s-t \leq 1$ and if b is even, all of n, s, t are even and $s-t \leq 2$. In all cases $s \leq 2t$. Using the inductive hypothesis for K_b^s and K_b^t,

$$K_b^n = (G_1 + \cdots + G_{s'}) \times (H_1 + \cdots + H_{t'}) ,$$

where each G_i is a cycle on b^s vertices, H_j is a cycle on b^t, $s' = s(b-1)/2$ and $t' = t(b-1)/2$. Since $s' \le 2t'$, this can be rearranged by (*) to give the sum of t' terms each of which is of the form $G_i \times H_j$ or $(G_i + G_{i+1}) \times H_j$. Result II shows that each term of the first type can be decomposed into two Hamiltonian cycles of K_b^n, while result I shows that each term of the second type can be decomposed into three Hamiltonian cycles of K_b^n. After decomposing all terms, we have a Hamiltonian decomposition of K_b^n. ∎

4.2. Edge-Decomposition Into Other Hamming Spaces

To aid in finding decompositions, it is helpful to know if K_b^n can be decomposed into graphs isomorphic to K_c^l. If so, any decompositions of K_c^l will give a decomposition of K_b^n.

If $b \ne c$ it may be difficult to discover if such a decomposition exists. For example, K_v has an edge-decomposition into copies of K_k, $k < v$, if and only if a $2-(v,k,1)$ balanced incomplete block design exists. We therefore restrict attention to decompositions of K_b^n into copies of K_b^l.

Definition. An edge-decomposition of a graph G into other graphs $H_1, \ldots, H_t$ is *resolvable* if the set $\{H_1, \ldots, H_t\}$ has a partition into vertex-decompositions of G.

It is trivial to see that for $l \le n$, there is a *vertex*-decomposition of K_b^n into copies of K_b^l. The case of edge-decomposition is not much more difficult.

Proposition 4.2.1. K_b^n has an edge-decomposition into copies of K_b^l if and only if $l | n$, and if $l | n$ there exists a resolvable edge-decomposition.

Proof. Since K_b^n has degree $n(b-1)$ and K_b^l has degree $l(b-1)$, it is necessary that $l | n$. As an example of how to do this when $l | n$, take $l = 2$, $n = 6$. A decomposition consists of all cylinders of the form $**wxyz$, $wx**yz$ or $wxyz**$, where w, x, y and z are arbitrary elements of K_b. Each edge of K_b^6 is in exactly one of these copies of K_b^2. Furthermore, all of the cylinders of the form $**wxyz$ are a vertex-decomposition of K_b^6. Also, the cylinders $wx**yz$ are a vertex-decomposition, as are $wxyz**$. Thus, the edge-decomposition is resolvable. ∎

A curious problem is to find examples of edge-decompositions of K_b^n by K_b^l which are *not* resolvable. We do not know of a single example. The following problem is a special case of this.

Unsolved Problem. Is there an edge-decomposition of K_2^{2n} by C_4 (the 4-cycle) which does not resolve into vertex-decompositions?

4.3. Decompositions Into Short Cycles

Since $K_2^2 \approx C_4$, Proposition 4.2.1 tells us that there is an edge-decomposition of K_2^n by C_4 precisely when $2 | n$. Next, we will obtain conditions for the edge-decomposition of K_2^n by C_6. Since six does not divide 2^n, such a decomposition will never be resolvable. The n-cube has $n2^{n-1}$ edges so a necessary condition for the C_6 decomposition to exist is that $6 | n2^{n-1}$ or $3 | n$. Since each C_6 has an even number of edges at each node, we also have that $2 | n$, so $6 | n$.

The first case where a C_6 decomposition might exist is K_2^6. This can be done, as the following computer-aided decomposition shows. First, remove all edges from K_2^6 which are in a C_6 formed by the vertex sequence,

$$001abc,\ 011abc,\ 010abc,\ 110abc,\ 100abc,\ 101abc$$

where a, b, c are arbitrary 0-1 parameters. Thus, 8 copies of C_6 have been removed from the edge set of K_2^6. It can be seen that the remaining graph has two components. Complementation of all coordinates is an isometry between these two components, so only one component need be decomposed into six-cycles.

The computer found the following decomposition of one component.

a) 000000, 010000, 010100, 000100, 100100, 100000

b) 000000, 000100, 001100, 001110, 001010, 001000

c) 000000, 000001, 100001, 100011, 100010, 000010

d) 000001, 001001, 001101, 000101, 010101, 010001

e) 000001, 000011, 100011, 100111, 100101, 000101

f) 000010, 001010, 001011, 000011, 010011, 010010

g) 000010, 000011, 000111, 100111, 100110, 000110

h) 000100, 000101, 000111, 001111, 001110, 000110

i) 000110, 000111, 010111, 010101, 010100, 010110

j) 001000, 001001, 001011, 001111, 001101, 001100

k) 010000, 010001, 010011, 010111, 010110, 010010

l) 100000, 100001, 100101, 100100, 100110, 100010

The remaining piece can be decomposed by applying the antipodal map to each of these 12 cycles. Of the 32 copies of C_6 in this decomposition only 12 are *induced* C_6's. These are the first 8 cycles together with c) and e) in the list above and their complements. We have not been able to find a decomposition into C_6's which are all induced.

Proposition 4.3.1. K_2^n has an edge-decomposition into copies of C_6 if and only if $6|n$.

Proof. It was shown previously that $6|n$ is necessary. Using Proposition 4.2.1 and the decomposition for K_2^6, a decomposition for all multiples of six is obtained. ⁚

For arbitrary C_j, $j \geq 10$, we do not know for which n K_2^n has an edge-decomposition into copies of C_j. For any $k \geq 1$, Theorem 4.1.1 allows us to decompose the $2k$-cube into cycles of length 2^{2k}. For each n which is a multiple of $2k$, resolvable edge-decompositions of the n-cube into cycles of length 2^{2k} can then be obtained by Proposition 4.2.1. Our final cycle decomposition also uses cycles whose length is a power of 2, but under the much stronger constraint that the cycles are induced from isometric sets, or they are *isometric cycles*, for short. The longest isometric cycle which fits in the n-cube has length only $2n$, for $n \geq 2$. For example, in K_2^4, the following 8 points induce an isometric cycle.

0000, 0001, 0011, 0111, 1111, 1110, 1100, 1000

Theorem 4.3.2. If $n = 2^k$, $k \geq 1$, K_2^n has a resolvable edge-decomposition into isometric cycles of length $2n$.

Proof. Our construction is based on the binary Hamming code, although in principle this proof does not require prior knowledge of the Hamming code.

Let $n = 2^k$, $k \geq 1$. The coordinates of points in K_2^n will be indexed by $0, 1, \ldots, n-1$, from left to right. Let the appropriate unit vectors be $\mathbf{e}^i$, $0 \leq i < n$. A map $Syn\colon K_2^n \rightarrow K_2^k$ called the *syndrome* is defined to be $GF(2)$-linear, in that $Syn(\mathbf{x} \oplus \mathbf{y}) = Syn(\mathbf{x}) \oplus Syn(\mathbf{y})$, and defined on the unit vectors such that $Syn(\mathbf{e}^i) = [i]$ is the 0-1 k-vector which represents i in binary notation. Let

$$H = \{\mathbf{h} \mid h_0 = 0 \text{ and } Syn(\mathbf{h}) = \mathbf{0}\}\,.$$

This is essentially the set of Hamming code vectors and as such has the property that the distance between any two distinct vectors in H is at least three. This is because Syn is linear so the sum of any two vectors in H is again in H, and H has no vectors of weight 1 or 2 because for $i \neq 0$, $[i] \neq \mathbf{0}$ and for $i \neq j$, $[i]\oplus[j] \neq \mathbf{0}$.

Define the following sequence of vectors.

$$\mathbf{f}^0 = \mathbf{0}, \mathbf{f}^1 = \mathbf{e}^{n-1}, \mathbf{f}^2 = \mathbf{e}^{n-2}, \ldots, \mathbf{f}^{n-1} = \mathbf{e}^1$$

and for $0 \leq i$, let $\mathbf{f}^{i+n} = \mathbf{f}^i \oplus \mathbf{e}^0$. Thus, the sequence $\{\mathbf{f}^i\}$ has period $2n$. Let $F = \{\mathbf{f}^i \mid i \geq 0\}$. Furthermore, define $\sigma\colon K_2^n \to K_2^n$ to be the "summation" function which is $GF(2)$-linear and such that $\sigma(\mathbf{e}^i) = \mathbf{e}^i \oplus \cdots \oplus \mathbf{e}^{n-1}$. Finally, for any $\mathbf{x} \in K_2^n$, let $C(\mathbf{x}) = \sigma(F \oplus \mathbf{x})$.

Our first claim is that for any $\mathbf{x}$, $C(\mathbf{x})$ induces an isometric $2n$-cycle. Since $C(\mathbf{x}) = \sigma(F) \oplus \sigma(\mathbf{x})$, and translation is an isometry, it is only necessary to show that $\sigma(F)$ induces an isometric cycle. However, the sequence

$$\sigma(\mathbf{f}^0), \sigma(\mathbf{f}^1), \ldots, \sigma(\mathbf{f}^{n-1}), \sigma(\mathbf{f}^n), \sigma(\mathbf{f}^{n+1}), \ldots, \sigma(\mathbf{f}^{2n-1})$$

is

$$(0,\ldots,0), (0,\ldots,0,1), \ldots, (0,1,\ldots,1), (1,\ldots,1), (1,\ldots,1,0), \ldots, (1,0,\ldots,0)\,,$$

which is an isometric $2n$-cycle.

The next step in our proof is to show that the collection of $2n$-cycles $C(\mathbf{h})$ for all $\mathbf{h} \in H$ forms a vertex-decomposition of K_2^n. First, $C(\mathbf{h}^1)$ meets $C(\mathbf{h}^2)$ if and only if for some i and j, $\sigma(\mathbf{f}^i \oplus \mathbf{h}^1) = \sigma(\mathbf{f}^j \oplus \mathbf{h}^2)$. Since σ is a bijection, this happens if and only if $\mathbf{f}^i \oplus \mathbf{h}^1 = \mathbf{f}^j \oplus \mathbf{h}^2$, or $\mathbf{f}^i \oplus \mathbf{f}^j = \mathbf{h}^1 \oplus \mathbf{h}^2$. But if $\mathbf{h}^1 \oplus \mathbf{h}^2 \neq \mathbf{0}$, this cannot occur because $\mathbf{h}^1 \oplus \mathbf{h}^2$ would have weight at least three and first coordinate equal to zero. No sum of two members of F is of this form. It follows that the $C(\mathbf{h})$ are vertex-disjoint. Secondly, the cardinality of H is 2^{n-k-1}, because Syn is surjective. Finally, each $C(\mathbf{h})$ has $2n$ elements and $2n \times 2^{n-k-1} = 2^n$, so the $C(\mathbf{h})$ partition the vertices of K_2^n. To obtain the vertex-decomposition we have only used the fact that H is a set of 2^{n-k-1} vectors with first coordinate zero and distance at least three between vectors. There are other examples of such sets, i.e., the codes of Vasilev and Schonheim [40,p.162]. However, to obtain the edge-decomposition to follow, unique properties of the Hamming code will be used.

Since translation is an isometry, for any fixed vector $\mathbf{s}$, the $2n$-cycles $C(\mathbf{h} \oplus \mathbf{s})$, as $\mathbf{h}$ varies over H, form a vertex partition. It only remains to find some set S such that for each edge of K_2^n there is exactly one $\mathbf{s} \in S$ such that the vertex-partition $\{C(\mathbf{h} \oplus \mathbf{s}) \mid \mathbf{h} \in H\}$ contains that edge.

First, we will look at what happens when $C(\mathbf{x})$ meets $C(\mathbf{y})$, assuming $\mathbf{x} \neq \mathbf{y}$ and $x_0 = y_0 = 0$. These cycles have intersecting vertex sets whenever for some i and j, $\mathbf{f}^i \oplus \mathbf{x} = \mathbf{f}^j \oplus \mathbf{y}$, or equivalently, $\mathbf{x} \oplus \mathbf{y} = \mathbf{f}^i \oplus \mathbf{f}^j$. This can happen only when $\mathbf{x} \oplus \mathbf{y}$ has weight one or two. In such cases the only way to write $\mathbf{x} \oplus \mathbf{y}$ as the sum of two elements of F is as $\mathbf{f}^i \oplus \mathbf{f}^j$, $\mathbf{f}^j \oplus \mathbf{f}^i$, $\mathbf{f}^{i+n} \oplus \mathbf{f}^{j+n}$ and $\mathbf{f}^{j+n} \oplus \mathbf{f}^{i+n}$. Thus, if $C(\mathbf{x})$ meets $C(\mathbf{y})$ there will be exactly four vertices of intersection:

$$\sigma(\mathbf{f}^i \oplus \mathbf{x}) = \sigma(\mathbf{f}^j \oplus \mathbf{y}) \tag{i}$$

$$\sigma(\mathbf{f}^j \oplus \mathbf{x}) = \sigma(\mathbf{f}^i \oplus \mathbf{y}) \tag{ii}$$

$$\sigma(\mathbf{f}^{i+n} \oplus \mathbf{x}) = \sigma(\mathbf{f}^{j+n} \oplus \mathbf{y}) \tag{iii}$$

$$\sigma(\mathbf{f}^{j+n} \oplus \mathbf{x}) = \sigma(\mathbf{f}^{i+n} \oplus \mathbf{y})\,. \tag{iv}$$

Suppose that $C(\mathbf{x})$ and $C(\mathbf{y})$ have an edge in common. This can only happen if $i - j$ is ±1 modulo $2n$, or $i - (j + n)$ is ±1 modulo $2n$. Since $\mathbf{f}^{j+n} = \mathbf{e}^0 \oplus \mathbf{f}^j$, in either case there is an integer p, equal to i or j, such that $Syn(\mathbf{f}^i \oplus \mathbf{f}^j) = Syn(\mathbf{f}^p \oplus \mathbf{f}^{p+1})$. For any p, $Syn(\mathbf{f}^p \oplus \mathbf{f}^{p+1})$ equals $[2^r - 1]$ for some r, $0 < r \leq k$, In other words, the syndrome vector is some number of 0's followed by some positive number (r) of 1's. This is because the modulo two sum of the binary representations of two consecutive integers always has this form. Thus, $Syn(\mathbf{x} \oplus \mathbf{y}) = Syn(\mathbf{f}^i \oplus \mathbf{f}^j) = [2^r - 1]$.

At last, we are ready to specify the set S. Let $S = \{\mathbf{e}^1, \mathbf{e}^3, \ldots, \mathbf{e}^{n-1}\}$. For any distinct $\mathbf{s}^1, \mathbf{s}^2 \in S$ and any $\mathbf{h}^1, \mathbf{h}^2 \in H$,

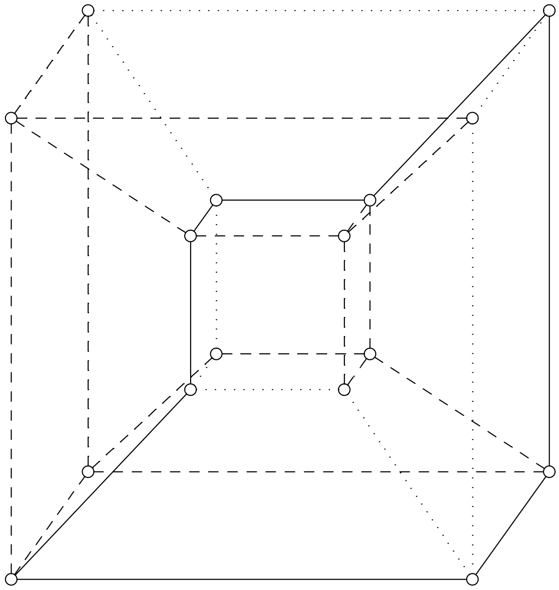
$$Syn((\mathbf{s}^1 \oplus \mathbf{h}^1) \oplus (\mathbf{s}^2 \oplus \mathbf{h}^2)) = Syn(\mathbf{s}^1 \oplus \mathbf{s}^2) = Syn(\mathbf{e}^{2a+1} \oplus \mathbf{e}^{2b+1}) = [2a+1] \oplus [2b+1] \,.$$

The rightmost coordinate of $[2a+1] \oplus [2b+1]$ is zero, so the syndrome is never of the form $[2^r - 1]$. Thus, by the result of the preceding paragraph, $C(\mathbf{h}^1 \oplus \mathbf{s}^1)$ and $C(\mathbf{h}^2 \oplus \mathbf{s}^2)$ will not have an edge in common. Note K_2^n has $n2^{n-1}$ edges while

$$|S| \cdot |H| \cdot 2n = |S| \cdot 2^n = (n/2)2^n = n2^{n-1} \,,$$

so every edge is in one and only one of the specified $2n$ cycles. ∷

As an example of this theorem, the figure below shows an edge-decomposition of K_2^4 four isometric copies of C_8, indicated in the figure by the four types of edges. It can be seen that there are two pairs of vertex disjoint cycles.



4.4. Vertex-Decompositions and Odd Covers

In this section we investigate some aspects of partitions of K_2^n into subcubes. A paper of Baum and Neuwirth [41] showed that there are many ways to partition K_2^n into $GF(2)$-affine spaces of equal dimension such that no two spaces are parallel, in that one is a translate of the other. We start off by showing the negative result that this cannot be done when the affine spaces are restricted to be subcubes. In fact, we prove a much stronger result that "odd covers" by nonparallel subcubes do not exist.

Definition. An *odd cover* of a set S is a collection of subsets of S such that each element of S is contained in an odd number of these subsets.

Every partition is an odd cover and every odd cover is a cover, so the concept of odd cover lies between these two more familiar concepts.

Theorem 4.4.1. In any odd cover of the points of K_2^n, $n \geq 1$, by proper subcubes, there is at least one pair of parallel subcubes.

Proof. The proof uses the fact that every Boolean function has a unique representation as a $GF(2)$-polynomial [42]. For any subcube Q of K_2^n, consider the polynomial representation of the characteristic function of Q. For example, the cube $1{*}1{*}1$ in K_2^5 has polynomial $x_1 x_3 x_5$, because $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)$ is in the cube if and only if $x_1 x_3 x_5 = 1$. Every cube containing $(1,1,\ldots,1)$ has a polynomial which is a single monomial. A variable x_i appears in this monomial if and only if i is not a direction of the cube. An extreme case of this is all of K_2^n. The characteristic function is the constant function 1, whose single monomial is 1.

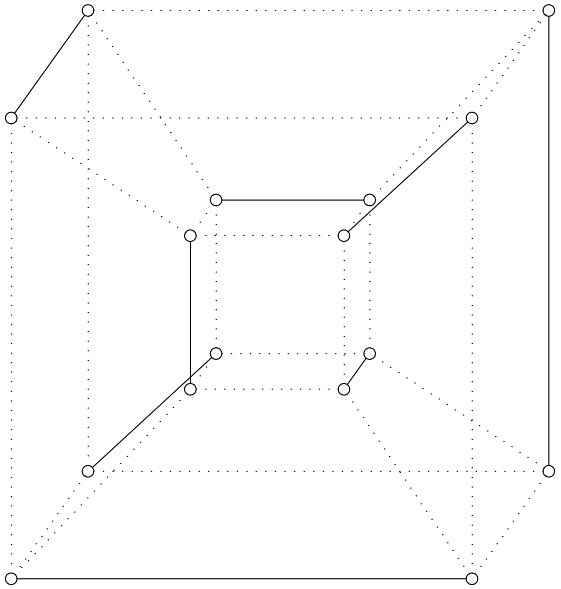
Any cube can be translated so that it passes through $(1,1,\ldots,1)$. Thus, the characteristic function for any cube is found by translating the arguments of some monomial, and therefore of the form

$$f(\mathbf{x}) = (x_{i(1)} \oplus t_{i(1)}) \cdots (x_{i(k)} \oplus t_{i(k)}), \quad 1 \le i(1) < i(2) < \cdots < i(k) \le n,$$

where $\mathbf{t} = (t_1, \ldots, t_n)$, is the translation vector. Note that when f is expanded by the distributive property, the untranslated monomial $x_{i(1)} \cdots x_{i(k)}$ appears, and this is the monomial of largest degree in the expansion of f.

In any odd cover, the modulo 2 sum of the characteristic functions must be the constant 1. By uniqueness of the polynomial representation, all higher degree monomials must cancel as the polynomials for the subcubes are added together. Let Q be a cube of maximal co-dimension in the odd cover. Let k be the co-dimension of Q. The characteristic function of Q contains a monomial of degree k. To cancel this, some other cube, R, in the odd cover must have this monomial in its polynomial. Now, R must have co-dimension at least k, and by maximality, it has co-dimension exactly k. Thus, Q and R are parallel because the monomials of highest degree in their polynomials are equal. ∎

In spite of the theorem, there may still be interesting decompositions into cubes. For example, by considering a vertex-decomposition of K_2^4 into two copies of C_8, and taking alternating edges, a vertex-decomposition of K_2^4 into K_2^1's was obtained and is pictured below. It has the property that it contains no decomposed K_2^2 or K_2^3. Thus, even though the decomposition has parallel K_2^1's, as assured by Theorem 1, none of these are adjacent.



If someone were to present a collection of subcubes of K_2^n and claim that these cubes form a vertex-decomposition of K_2^n, this claim would be easy to verify or disprove. First, it could be easily checked that the cubes were mutually disjoint. The next check is that the sum of the cardinalities of the cubes is 2^n. The claim is true if and only if both conditions are met.

In the case where the cubes are disjoint but the sum of the cardinalities is less than 2^n, one might ask for a specific point not in any of the cubes. This can be found by a "recursive splitting" approach. Split K_2^n into two copies of K_2^{n-1}, say X and Y. By intersecting each cube with X and then with Y, a collection of subcubes of X and a collection of subcubes of Y are generated. The total cardinality in one of these collections must be less than 2^{n-1}. Working recursively on such a halfspace, a single point not in any of the original subcubes is quickly found.

Essentially the same remarks hold concerning decompositions into affine spaces; however, there is a real problem in extending this to verifying odd covers by cubes or affine spaces. This is the topic of the next section.

4.5. Verifying Odd Covers

Given a collection of $GF(2)$-affine subspaces of K_2^n, we would like to be able to tell if all points are in an odd number of affine spaces. One helpful observation is that the parity of the sum of the cardinalities of all sets equals the parity of the number of points which are oddly covered. Thus, for $n \geq 1$, if the sum of the cardinalities is not even, not all points are covered an odd number of times. In fact, if the sum is odd, the recursive splitting strategy described at the end of the previous section can be used to quickly converge on a point which is covered an even number of times. If K_2^n, $n \geq 2$, is split into two halfcubes X and Y, and each affine space of the collection is intersected with X and Y, one of the two resulting collections of affine spaces has odd cardinality sum. The recursive algorithm is then applied to the "odd" halfcube. The recursion must stop at $n = 1$. Then there are two points, one oddly covered, the other evenly covered, and this second point is the one sought.

What can be done if the cardinality sum is even? From this point on we will assume that the subsets A_i, $1 \leq i \leq a$, in a proposed odd cover are given as affine spaces. For any affine space B, the sets $A_i \cap B$ must form an odd cover of B. The cardinality sum test can be applied to B, because it is possible to compute $|A_i \cap B|$ by Gaussian reduction. In the remainder of this section we will show that a procedure roughly as simple as repeatedly applying this test with randomly selected spaces B will quickly reveal any collection that is not an odd cover as such. The lemma that makes it all work concerns the intersection of random affine hyperplanes with an arbitrary set.

Lemma 4.5.1. Suppose $S \subseteq K_2^n$, $n \geq 1$, and $|S| = m$. Let L be a uniform randomly selected $GF(2)$-affine hyperplane of K_2^n, and let $r = m - 2|S \cap L|$. Then,

$$\Pr\{|r| > \alpha\sqrt{m}\} < \alpha^{-2} ,$$

for any real $\alpha \geq 1$.

Proof. This is a straightforward application of Chebyshev's inequality. To apply this inequality, we must compute the mean and variance of r. Note that the number of affine hyperplanes is $2(2^n - 1)$. Thus, the mean of r is

$$(2(2^n-1))^{-1} \sum_L (m - 2|S \cap L|) = m - (2^n - 1)^{-1} \sum_L |S \cap L| .$$

But, for each hyperplane L, L^c is a hyperplane and $|S \cap L| + |S \cap L^c| = m$, so the mean is $m - (2^n - 1)^{-1}(2^n - 1)m = 0$.

To compute the variance,

$$\sum_L (m - 2|S \cap L|)^2 = \sum_L m^2 - 4m \sum_L |S \cap L| + 4 \sum_L |S \cap L|^2 . \qquad (*)$$

We just noted that $\sum_L |S \cap L| = (2^n - 1)m$ so the first two terms on the righthand side of (*) sum to $-2(2^n - 1)m^2$. Let $L(\mathbf{s}) = 1$ if $\mathbf{s} \in L$ and let $L(\mathbf{s}) = 0$ otherwise. Then $|S \cap L| = \sum_{\mathbf{s} \in S} L(\mathbf{s})$ so,

$$|S \cap L|^2 = |S \cap L| + \sum_{\substack{\mathbf{s}^1 \neq \mathbf{s}^2 \\ \mathbf{s}^1, \mathbf{s}^2 \in S}} L(\mathbf{s}^1) L(\mathbf{s}^2) .$$

For any distinct points $\mathbf{s}^1$ and $\mathbf{s}^2$, the number of non-zero vectors $\mathbf{l}$ for which $(\mathbf{l}, \mathbf{s}^1 \oplus \mathbf{s}^2) = 0 \pmod 2$ is $2^{n-1} - 1$. Since each hyperplane L corresponds uniquely to $\mathbf{l} \neq \mathbf{0}$ and $c \in \{0,1\}$ such that $L = \{\mathbf{x} | (\mathbf{l}, \mathbf{x}) = c \pmod 2\}$, the number of L with $L(\mathbf{s}^1) = L(\mathbf{s}^2) = 1$ is $2^{n-1} - 1$. Thus,

$$\sum_L |S \cap L|^2 = (2^n - 1)m + (2^{n-1} - 1)m(m-1) ,$$

and (*) evaluates to

$$-2(2^n-1)m^2+4(2^n-1)m+2(2^n-2)m(m-1)=2(2^n-1)m+2(m-m^2)\,.$$

The variance of r is this number divided by $2(2^n-1)$, and noticing that $m-m^2 \le 0$, this variance is at most m, and the standard deviation is at most $\sqrt{m}$.

Now, Chebyshev's inequality states that the probability of finding r at distance more than α times its standard deviation from its mean is less than α^{-2}, and the result follows. ∎

Theorem 4.5.2. There is a probabilistic algorithm with the following properties. Let A_i, $1 \le i \le a$, $a \ge 1$, be a collection of affine subspaces of K_2^n, $n \ge 1$, each specified as the solution set of a list of independent $GF(2)$-linear equations. The algorithm either returns a point evenly covered by the A_i or returns the statement that the A_i form an odd cover. The algorithm takes $O(an^3)$ operations and returns an incorrect response with probability less than 1/4.

Proof. For technical reasons this problem of verifying an odd cover will be replaced by the problem of verifying an "even cover". An instance of the odd cover problem is easily transformed to an instance of the even cover problem by adding all of K_2^n as an additional affine space. Thus, the problem will be to find a point which lies in an odd number of the affine spaces, if such a point exists. The procedure is fairly simple.

```
1) $k \leftarrow 0$.
2) Compute $\sum_i |A_i|$. If this is odd go to 7).
3) $k \leftarrow k+1$.
4) If $k > n$, STOP, returning "even cover".
5) Randomly select an affine hyperplane $L$ and replace each $A_i$ by $A_i \cap L$.
6) Go to 2).
7) Find an oddly covered point by recursive splitting and STOP, returning this point.
```

First, the total work in this procedure is $O(an^3)$ because it takes $O(n)$ passes of $O(an^2)$ work per pass. The selection of L amounts to selecting $\mathbf{l} \in K_2^n \backslash \{\mathbf{0}\}$ and $c \in K_2$ randomly and setting $L = \{\mathbf{x} | (\mathbf{l},\mathbf{x}) = c \,(\mathrm{mod}\ 2)\}$. Intersecting L with an A_i can be done by updating the Gaussian reduction in $O(n^2)$ operations. The cardinalities of A_i required in 2) are easily computed from their dimensions. The one-time recursive splitting in step 7) can be done in $O(an^3)$ steps.

Anytime the procedure halts in step 7) the procedure produces a correct result. It is only necessary to bound the probability of incorrectly halting in step 4).

Let $S \subseteq K_2^n$ be the set of oddly covered points. Let $L_1, L_2, \ldots$ be an infinite sequence of random $GF(2)$-affine hyperplanes.

Let $B_k = L_1 \cap L_2 \cap \cdots \cap L_k$, and $B_0 = K_2^n$. The parity of $\sum_i |A_i \cap B_k|$ equals the parity of $|S \cap B_k|$. Since in step 2) the A_i have been replaced by $A_i \cap B_k$, if any $|S \cap B_k|$ is odd for any $0 \le k \le n$, the procedure exits to step 7) and returns a correct answer.

In fact, it will be shown that if $|S| > 0$, then $|S \cap B_k| = 1$, for some $0 \le k \le n$, with some probability bounded away from zero. Starting with any set S of cardinality m, call a *good event* a selection of a sequence of hyperplanes such that for some $k \ge 0$,

$$|S \cap B_0| > |S \cap B_1| > \cdots > |S \cap B_k| = 1\,.$$

For an integer $m \ge 1$ define $p(m)$ to be the *minimum* probability of a good event as S varies over all cardinality m subsets of K_2^n. Furthermore, for any real $s \ge 1$ define $q(s)$ to be the minimum of $p(m)$ as m ranges over all integers such that $1 \le m \le s$. Note $p(1) = 1$, $q(s) = 1$ for $1 \le s < 2$, and $q(s)$ is a nonincreasing function of s.

Now, the lemma, with $\alpha = m^{1/4}$, states that if $|S| = m \ge 2$ and L_1 is a random hyperplane, then with probability of at least $1 - m^{-1/2}$,

$$0 < \tfrac{1}{2}\,(m - m^{3/4}) \le |S \cap L_1| \le \tfrac{1}{2}\,(m + m^{3/4}) < m\ .$$

If this happens and if $S \cap L_1$ produces a good event with the sequence of hyperplanes $L_2, L_3, \ldots$, then S produces a good event with the sequence of hyperplanes $L_1, L_2, \ldots$. Thus,

$$p(m) \ge (1 - m^{-1/2})\ q(\tfrac{1}{2}\,(m + m^{3/4}))\ . \qquad (*)$$

Next, we show that (*) implies that $p(m)$ is bounded away from zero. First, since $m \ge 2$ implies $\frac{1}{2}\,(m + m^{3/4}) < m$, we have $p(m) \ge (1 - m^{-1/2})p(m')$ for some $m' < m$. Iterating this until $m' = 1$,

$$p(m) \ge \prod_{l=2}^{l=m} (1 - l^{-1/2})\ .$$

This serves to show that for each $s \ge 1$, $q(s) > 0$. Now let $\alpha = 3/2$. For any t larger than some t_0,

$$\tfrac{1}{2}\,(\alpha^t + (\alpha^t)^{3/4}) < \alpha^{t-1}\ .$$

For $t > t_0$, if $\alpha^t < m < \alpha^{t+1}$, by (*) we have,

$$p(m) \ge (1 - \alpha^{-t/2})q(\alpha^t) \quad \text{and that}$$

$$q(\alpha^{t+1}) \ge (1 - \alpha^{-t/2})q(\alpha^t)\ . \qquad (**)$$

Let $\beta = \alpha^{-1/2}$, so that iterating (**), we obtain,

$$q(\alpha^{t+l}) \ge ((1 - \beta^t)(1 - \beta^{t+1}) \cdots)q(\alpha^t)\ .$$

Since the infinite product converges to a positive limit, there is a $c > 0$ such that $q(s) \ge c$ for all $s \ge 1$ and therefore $p(m) \ge c$ for $m \ge 1$.

Knowing there is a $c > 0$ such that $p(m) \ge c$ allows us to say that if S is the set of points covered an odd number of times and $|S| > 1$, then the procedure correctly halts with probability at least c. Recall that our condition for a good event included not only that $|S \cap B_k| = 1$ for some k, but that $|S \cap B_i|$ is strictly decreasing for $i < k$. This implies that the dimensions of the B_i are strictly decreasing. Since B_0 has dimension n, the dimension can only decrease for n steps, so $k \le n$ and the procedure exits correctly.

Hence, the procedure completes successfully with probability at least c. Since each application of the procedure erroneously returns the statement ‘‘even cover’’ with probability no more than $1 - c$, independent application of the procedure j times will erroneously miss finding an oddly covered point with probability at most $(1 - c)^j$. For sufficiently large j, this error probability is less than 1/4. The entire algorithm, with j repetitions, is still $O(an^3)$ operations. ∎

Corollary 4.5.3. There is a probabilistic algorithm using $O(an^3)$ operations to solve systems of equations on $\mathbf{x} \in K_2^n$, $n \ge 1$, consisting of n or less $GF(2)$-linear equations and a single equation of the form $f(\mathbf{x}) = 1$ where f is given explicitly as a $GF(2)$-polynomial with $a \ge 1$ monomial terms.

Proof. The solution set of the linear part is some affine space, say A. An arbitrary monomial of f is the characteristic function of some cube, say Q. A solution to the entire system is a point oddly covered by the a affine spaces of the form $A \cap Q$. Solutions can therefore be found by using Theorem 2 to test if the sets $A \cap Q$ together with all of K_2^n form an odd cover. ∎

Suppose we are given a system with several polynomial constraints, $f_1(\mathbf{x}) = 1, \ldots, f_k(\mathbf{x}) = 1$. These are equivalent to the single constraint $f_1(\mathbf{x}) \cdots f_k(\mathbf{x}) = 1$ which may be expanded as a single polynomial and made an instance of the corollary. In principle then, it can be said that for any fixed k the system can be probabilistically solved in polynomial time. However, the number of terms in the expanded polynomial may be so large that it is practical only for small values of k.

If there are only a few solutions to the system in the corollary these solutions can all be found. Once one evenly covered point (solution) is found, an affine space consisting only of that point can be added to the collection of sets. This effectively ‘‘marks out’’ that solution and when the algorithm is rerun, only *new* solutions to the original system can be found. This marking out process can be repeated until all solutions have been located with a high degree of certainty.

Further results can be obtained using the lemma. If $|S|$ is large, the lemma states that nearly every hyperplane approximately bisects S. This means that the number of solutions to the system can be estimated to arbitrarily small relative error. First, one cuts S down to size using k randomly chosen hyperplanes. Then the size of the remaining set can be found by listing its m elements, as in the previous paragraph. The size of the original set can then be estimated to be $2^k m$. By making k small the relative error can be made small, at the expense of much more work on the second step.

We do not know of any *deterministic* polynomial time algorithms for verifying odd covers or of a method of *exactly* enumerating the number of evenly covered points.

4.6. Covering Spheres by Combinatorial Sets

As mentioned in section 1.6, a problem of interest to electrical engineers is to cover a given set $S \subseteq K_2^n$ by a minimal number of subcubes. For some sets the minimal number can be found, but the covering is not very interesting. For example, if all connected components of S have only one point, then all nonempty subcubes of S are singletons and the minimal cover has $|S|$ elements. This happens whenever S is a sphere. The purpose of this section is to show that by relaxing the problem to covering combinatorial sets, something nontrivial can be done for spheres and perhaps other sets.

A possible application is to algebraic coding theory, where we have the problem of determining if a given $GF(2)$-affine space, A, intersects the sphere, S, of radius k about 0. The idea is to cover the sphere with a collection C_i, $i = 1, 2, \ldots, m$, of $GF(2)$-affine subsets of the sphere, with m a small as possible. The intersections $C_i \cap A$ can be rapidly found using Gaussian elimination. If any of these intersections is nonempty, a point in $S \cap A$ has been found and if all $C_i \cap A$ are empty, $S \cap A$ is also.

As stated so far, the problem would be to cover the sphere by a minimal number of $GF(2)$-affine spaces. We do not have an exact solution to this problem, but we will show that the $GF(2)$-affine spaces can be constrained to be combinatorial sets without drastically increasing the number of subsets required to cover the sphere.

First, we may assume that if we are attempting to cover a sphere of radius k in K_2^n, $2k \le n$. This is because the sphere of radius k about $\mathbf{0}$ is identical to the sphere of radius $n - k$ about $\mathbf{1}$. Assuming $2k \le n$, let

$$M = \{\mathbf{x} \mid x_1 \ne x_2, x_3 \ne x_4, \ldots, x_{2k-1} \ne x_{2k}, x_{2k+1} = 0, \ldots, x_n = 0\} .$$

Thus, M is a combinatorial set. Alternatively, we may write, $M = \{01, 10\}^k \times \{0\}^{n-2k}$. From this it is seen that every member of M has weight k and $|M| = 2^k$. The next result shows that even if we allow any $GF(2)$-affine space, no larger subsets of the sphere can be found. The result is a modification of [43,Proposition 1] suggested by R. McEliece (personal communication).

Proposition 4.6.1. There does not exist a $(k+1)$-dimensional $GF(2)$-affine subset of a sphere of radius k in K_2^n, $0 \le k \le n$.

Proof. It can be assumed that the sphere is about $\mathbf{0}$. Assume H is a $(k+1)$-dimensional $GF(2)$-affine space containing only points of weight k. Express H as $L \oplus \mathbf{c}$, where L is a $GF(2)$-linear space. There is a $(k+1) \times n$ 0-1 matrix G whose row space over $GF(2)$ is L. Since G has row rank $k+1$, there is a nonsingular $(k+1) \times (k+1)$ submatrix of G. By permuting the columns, we may assume this is the submatrix of the leftmost $k+1$ columns. Since this submatrix is nonsingular, some $GF(2)$-linear combination of the $(k+1)$-rows equals $(\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_{k+1})$. But, this would mean that there is a vector in $L \oplus \mathbf{c} = H$ which begins with $k+1$ 1's, and surely this vector cannot have weight k. ⁝

Of course, more than one large subset of the sphere is required to cover it, in any but the trivial cases. Define an *M-set*, to be the result of applying any coordinate permutation to the set M given above. Each M-set is a combinatorial subset of the sphere and has 2^k elements. In graph theory terms each M-set can be identified with a k-matching on a complete graph with n nodes. These nodes can be labeled $x_1, \ldots, x_n$ and if the edge between x_i and x_j is in the matching, $x_i \ne x_j$ is included in the defining combinatorial system for the M-set. For nodes x_i not in any edge of the matching, the equation $x_i = 0$ is included.

Definition. For nonnegative integers k and $n \ge 2k$, let $\mathrm{sm}(n, k)$ be the minimum number of M-sets of cardinality 2^k required to cover the radius k sphere about $\mathbf{0}$ in K_2^n.

It is easy to see that $\mathrm{sm}(n, k)$ is well defined, because every point of weight k is in some M-set.

Proposition 4.6.2. $\mathrm{sm}(n, k) \ge 2^{-k}\binom{n}{k}$, for $n \ge 2k$.

Proof. The sphere has $\binom{n}{k}$ points to be covered and each M-set covers 2^k of them. ∎

Proposition 1 shows that the bound of Proposition 2 still would apply if any $GF(2)$-affine subspaces of the sphere could be used. The next result shows that keeping with M-sets $\mathrm{sm}(n, k)$, is not very much more than the lower bound just established.

Theorem 4.6.3. $\mathrm{sm}(n, k) \le \left\lceil 2^{-k}\binom{n}{k} \ln\binom{n}{k} \right\rceil$, for $n \ge 2k > 0$.

Proof. We have used "ln" to denote the natural logarithm. The proof is a standard probabilistic method. Let $l = \left\lceil 2^{-k}\binom{n}{k} \ln\binom{n}{k} \right\rceil$ and it will be shown that if l M-sets are randomly selected (with repetition), then there is some nonzero probability that they completely cover the sphere, S, of radius k about $\mathbf{0}$.

First, for any $\mathbf{s} \in S$, let $p(\mathbf{s})$ be the probability that one random M-set will contain $\mathbf{s}$. By symmetry, it is clearly true that $p(\mathbf{s})$ does not depend on $\mathbf{s}$. Also, the sum of $p(\mathbf{s})$ over all elements of S is the expected value of the cardinality of an M-set. But, all these M-sets have 2^k elements. Thus, $p(\mathbf{s}) = p = 2^k\binom{n}{k}^{-1}$.

Now, if l M-sets are randomly selected, the probability that some particular point $\mathbf{s}$ of S is not covered is $(1-p)^l$. Therefore, the expected number of points not covered by l random M-sets is $\binom{n}{k}(1-p)^l$. Note $l \ge p^{-1}\log\binom{n}{k}$, so

$$\binom{n}{k}(1-p)^l \le \binom{n}{k}\left((1-p)^{p^{-1}}\right)^{\log\binom{n}{k}} < \binom{n}{k}e^{-\log\binom{n}{k}} = 1\,.$$

Since the expected number of uncovered points is less than 1, there must be a nonzero probability of leaving 0 points uncovered. ∎

Proposition 2 and Theorem 3 do not quite determine $\mathrm{sm}(n, k)$. We do not know the precise value of $\mathrm{sm}(n, k)$, except for certain small values of k. Perhaps most challenging is the problem of finding $\mathrm{sm}(2n, n)$. This is equivalent to the following purely graph theoretic problem.

Unsolved Problem. What is the smallest number of perfect matchings of K_{2n} such that for every induced copy of K_n in K_{2n}, at least one of these perfect matchings is edge disjoint from it?

References

1. R. W. Hamming, “ERROR DETECTING AND ERROR CORRECTING CODES,” *Bell System Tech. J.,* 29, pp. 147-160 (1950).
2. T. M. Thompson, *FROM ERROR-CORRECTING CODES THROUGH SPHERE PACKINGS TO SIMPLE GROUPS,* Carus Monograph 21, The Mathematical Association of America (1983).
3. J. A. Bondy and U. S. R. Murty, *GRAPH THEORY WITH APPLICATIONS,* North-Holland (1976).
4. R. E. Tarjan, *DATA STRUCTURES AND NETWORK ALGORITHMS,* 44, SIAM, CBMS-NSF, Philadelphia (1983).
5. D. Slepian, “ON THE NUMBER OF SYMMETRY TYPES OF BOOLEAN FUNCTIONS OF N VARIABLES,” *Canad. J. Math,* 5, pp. 185-193 (1953).
6. S. W. Golomb, “MATHEMATICAL THEORY OF DISCRETE CLASSIFICATION” in *Information Theory, Proceedings of the Fourth London Symposium,* ed. C. Cherry, London (1960).
7. R. L. Graham, “ON ISOMETRIC EMBEDDINGS OF GRAPHS” in *Progress in Graph Theory,* ed. Bondy and Murty, pp. 307-322, Academic Press Canada.
8. D. Z. Djoković, “DISTANCE-PRESERVING SUBGRAPHS OF HYPERCUBES,” *J. Comb. Thry B,* 14, pp. 263-267 (1973).
9. M. R. Garey and R.L. Graham, “ON CUBICAL GRAPHS,” *J. Comb. Thry B,* 18, pp. 84-95 (1975).
10. M. R. Garey and D. S. Johnson, *COMPUTERS AND INTRACTABILITY,* W. H. Freeman, New York (1979).
11. R. Ahlswede and G. O. H. Katona, “CONTRIBUTIONS TO THE GEOMETRY OF HAMMING SPACES,” *Disc. Math.,* 17, pp. 1-22 (1977).
12. L. H. Harper, “OPTIMAL ASSIGNMENTS OF NUMBERS TO VERTICES,” *J. SIAM,* 12, pp. 131-135 (March 1964).
13. John H. Lindsey II, “ASSIGNMENT OF NUMBERS TO VERTICES,” *Am. Math. Monthly,* 71, pp. 508-516 (May 1964).
14. A. J. Bernstein, “MAXIMALLY CONNECTED ARRAYS ON THE N-CUBE,” *SIAM J. Appl. Math.,* 15, pp. 1485-1489 (Nov. 1967).
15. I. Flores, “REFLECTED NUMBER SYSTEMS,” *IRE Transactions on Electronic Computers,* EC-5, pp. 79-82 (June 1956).
16. Teuvo Kohonen, *DIGITAL CIRCUITS AND DEVICES,* Prentice-Hall, Englewood Cliffs, N.J. (1972).
17. A. K. Chandra and G. Maskowsky, “ON THE NUMBER OF PRIME IMPLICANTS,” *Disc. Math.,* 24, pp. 7-11 (1978).
18. Michael L. Dertouzos, *THRESHOLD LOGIC: A SYNTHESIS APPROACH,* MIT press, Cambridge, Massachusetts.
19. S. T. Hu, *THRESHOLD LOGIC,* Univ. of Calif. Press (1965).
20. S. Muroga, *THRESHOLD LOGIC AND ITS APPLICATIONS,* Wiley-Interscience, New York (1971).
21. R. O. Winder, *THRESHOLD LOGIC* (1962). PhD Thesis Princeton Dept. of Math.
22. Ching Lai Sheng, *THRESHOLD LOGIC,* Academic Press (1969).
23. S. Even, A. Itai, and A. Shamir, “ON THE COMPLEXITY OF TIMETABLE AND MULTICOMMODITY FLOW PROBLEMS,” *SIAM J. Comp. Science,* 5, 4, pp. 691-702 (Dec. 1976).
24. B. Aspvall, M. F. Plass, and R. E. Tarjan, “A LINEAR-TIME ALGORITHM FOR TESTING THE TRUTH OF CERTAIN QUANTIFIED BOOLEAN FORMULAS,” *Inf. Proc. Let.,* 8 (1979).
25. S. Burris and H. P. Sankappanavar, *A COURSE IN UNIVERSAL ALGEBRA,* Springer-Verlag (1981).
26. Nathan Linial, “HARD ENUMERATION PROBLEMS IN GEOMETRY AND COMBINATORICS,” *SIAM Alg. Disc. Meth.,* 7, pp. 331-335 (April 1986).

27. H. J. Bandelt, “RETRACTS OF HYPERCUBES,” *J. Graph Thry.,* 8, pp. 501-510 (1984).

28. Martyn Mulder, “N-CUBES AND MEDIAN GRAPHS,” *J. Graph Thry.,* 4, pp. 107-110 (1980).

29. W. T. Trotter, “GRAPHS AND PARTIALLY ORDERED SETS” in *Graph Theory 2,* Academic Press, London (1983).

30. D. H. Wiedemann, “PROBLEM E-2846,” *Amer. Math. Monthly,* p. 577 (Aug. 1980).

31. Kathy W. Hoke, *VALID NUMBERINGS OF THE D-CUBE,* PhD Thesis U. North Carolina, Chapel Hill (1985).

32. Vasek Chvátal, *LINEAR PROGRAMMING,* W. H. Freeman, New York (1983).

33. N. Jacobson, *BASIC ALGEBRA 1,* W. H. Freeman.

34. G. Ringel, “UBER DREI KOMBINATORISCHE PROBLEME AM N-DIMENSIONALEN WURFEL UND WURFELGITTER,” *Abh. Math. Sem. Univ. Ham.,* 20, pp. 10-19 (1955).

35. J. Aubert and B. Schneider, “DECOMPOSITION DE LA SOMME CARTESIENNE D’UN CYCLE ET DE L’UNION DE DEUX CYCLES HAMILTONIENS EN CYCLES HAMILTONIENS,” *Discrete Math.,* 38, pp. 7-12 (1982).

36. Brian Alspach, *personal communication.*

37. A. Kotzig, *EVERY CARTESIAN PRODUCT OF TWO CIRCUITS IS DECOMPOSABLE INTO TWO HAMILTONIAN CIRCUITS* (1973). Center de Recherche Mathematiques, Montreal.

38. B. R. Myers, “HAMILTONIAN FACTORIZATION OF THE PRODUCT OF A COMPLETE GRAPH WITH ITSELF,” *Networks,* 2, pp. 1-9 (1972).

39. F. Harary, *GRAPH THEORY,* Addison-Wesley (1969).

40. Ian F. Blake and Ronald C. Mullin, *AN INTRODUCTION TO ALGEBRAIC AND COMBINATORIAL CODING THEORY,* Academic Press (1976).

41. L. E. Baum and L. P. Neuwirth, “DECOMPOSITIONS OF VECTOR SPACES OVER GF(2) INTO DISJOINT EQUIDIMENSIONAL AFFINE SPACES,” *J. Comb. Thry A,* 18, pp. 88-100 (1975).

42. Sheldon B. Akers, Jr., “ON A THEORY OF BOOLEAN FUNCTIONS,” *J. Soc. Indust. Appl. Math.,* 7, 4, pp. 487-498 (Dec. 1959).

43. Doug Wiedemann, “SOLVING SPARSE LINEAR EQUATIONS OVER FINITE FIELDS,” *IEEE Trans. Infor. Thry.,* IT-32, pp. 54-62 (Jan. 1986).