Equiseparations

Matthew Belcher, Stephen Hicks, and Meera Sitharam
mbelcher@cise.ufl.edu shicks@ufl.edu sitharam@cise.ufl.edu
CISE Department
University of Florida
Gainesville FL 32611-6120

Abstract- We define and investigate new geometric structures called equiseparations. These arise from the problem of finding a lower bound on the size of the threshold circuit needed to compute a certain function in the complexity class NP. We introduce the equiseparation problem and discuss its various formulations. We also explore several methods for finding a lower bound on the number of points in which it is possible to place in an equiseparation in d-dimension. Techniques used include Hadamard matrices, Grassman-Cayley algebras, and projective geometry.

1 Introduction

This paper defines and studies new geometric structures called equiseparations, which arise from the problem of finding a lower bound on the size of the threshold circuit needed to compute a certain function in the complexity class NP. This class contains the notorious Travelling Salesperson problem. Results in [1] and [2] show that our equiseparation question, if answered, will establish that an explicit NP problem has superpolynomial time complexity when the model of computation is restricted to a certain kind of neural network called threshold circuits. Restricting the model of computation is one direction taken by researchers in the process of settling the famous P vs. NP problem, i.e in distinguishing the complexity class of polynomially computable problems from the class NP. See [4] for a comprehensive background and treatment of these complexity classes and their relationships. A similar problem related to probabilistic communication complexity appeared in [7].

1.1 Problem Definition

Definition: Let $E = (P, H)$, where P is a set of points and H is a set of hyperplanes in the vector space $\mathbb{R}^d$, with $|P| = n \neq 0$, $|H| = m \neq 0$. Then, E is an (n, m)-*equiseparation* if for any pair of points $x, y \in P$, x and y have exactly half the hyperplanes between them. Figure 1 shows two (4,4)-equiseparations in 2D. (Note: The problem could instead require x and y to have greater than or equal to half the hyperplanes between them, since we can always add hyperplanes that do not separate any points.)

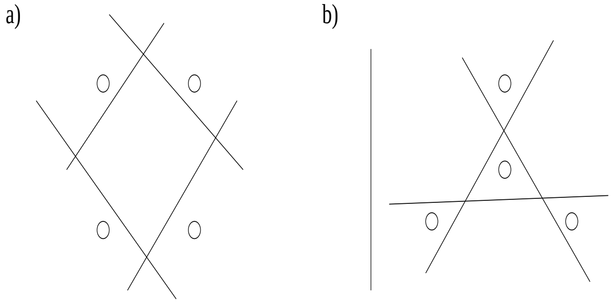

Figure 1: Two examples of equiseparations in 2D

Problem: Given d dimensions, what is the maximum number of points, n, which form an equiseparation in $\mathbb{R}^d$? Alternatively, given n, one can ask, what is the lowest dimension, d, in which one can find an equiseparation of n points? In this paper, we use both formulations.

Alon, Frankl, and Rödl [7] considered the similar problem of finding the smallest dimension d in which one can realize all possible separations of n points. Our problem is more difficult, since we want to know find the lowest dimension for a particular separation, whereas [7] does not consider any specific separation.

2 Initial Results and Tools

The following are preliminary observations about equiseparations. First, since we are trying to show that equiseparations do *not* exist in low dimensions, it is useful for us to consider a special case of the equiseparation question in which all the hyperplanes in the equiseparation pass through the origin. The following proposition, which follows from projective geometry, allows us to do so.

Proposition 1: An (n, m)-equiseparation exists in d dimensions if and only if there is an (n, m)-equiseparation in $d + 1$ dimensions with all hyperplanes passing through the origin. (Thus, we can force hyperplanes to pass through the origin when it is convenient for us to do so.)

Proof: ($\Rightarrow$) Assume we have an (n, m)-equiseparation E in a d-dimensional space A with arbitrary hyperplanes, not necessarily passing through the origin. We then consider a $(d+1)$-dimensional space B containing A. (The origin in A is not necessarily the origin in B) A will then be a hyperplane in B. Now, let x,$y \in A$ be arbitrary points separated by an arbitrary hyperplane h. Then, we can find a hyperplane H in B through the origin that intersects A on h. H then also separates x and y. We can then define a new equiseparation E' containing the points from E and the hyperplanes through the origin found by intersecting A on the hyperplanes from E. Thus, E' is an (n, m)-equiseparation in B, a $d+1$-dimensional space, with all hyperplanes passing through the origin.

($\Leftarrow$) Suppose E' is an (n, m)-equiseparation with hyperplanes passing through the origin in B, a $d+1$-dimensional space. Then, assuming that all the points in the equiseparation are in one half-space, we can examine the intersection of the hyperplanes in E' with the hyperplane A that defines the half-space. Each intersection will be a hyperplane in the d-dimensional space of A. Similarly, we can project the points onto the hyperplane. Now, let x and y be arbitrary points in B. Suppose x and y are separated by some hyperplane. Then when projected onto A, they will be separated by the d-dimensional hyperplane that is formed by the intersection of the hyperplane and A. Thus, the points are still separated by exactly half the hyperplanes. Since x and y were arbitrary, this is true for all points in E'. Thus, we have a new equiseparation with arbitrary hyperplanes in d-dimension. ■

In an equiseparation, we do not need to concern ourselves with the actual coordinates of points and hyperplanes. All that matters is the relationship between them. Therefore, we use a notation from the study of oriented matroids that reflects this fact [5]. For each hyperplane, we can define a positive side and a negative side. Also, we can order the hyperplanes arbitrarily. Then, we can define each point as a sign vector, where the i^{th} term of the sign vector is 1 if the point is on the positive side of the i^{th} hyperplane and -1 if the point is on the negative side. Similarly, by ordering the points, each hyperplane can be represented as a sign vector where the i^{th} term in the vector is 1 if the i^{th} point is on the positive side of the hyperplane, and -1 if it is on the negative side. Then an equiseparation exists if and only if the set of sign vectors of the points is *pairwise orthogonal*, since, from the definition of inner product, this means that the points are on opposite sides of exactly half the hyperplanes. This naturally leads to the following matrix.

Definition: The *equiseparation matrix* X has entries $X_{ij} = 1$ if the i^{th} point is on the positive side of the j^{th} hyperplane, and -1 otherwise. If the points and hyperplanes represented by X are all in d-dimension, then we say the equiseparation matrix X is *realized* in d dimensions.

To demonstrate the utility of these observations, we will show how this definition facilitates the proof of the following.

Proposition 2: Without loss, we can assume $|H| \geq |P|$.

Proof: Suppose $|H| < |P|$. Then, we know from linear algebra that the rows of the equiseparation matrix cannot be independent, since there are more rows than columns. Therefore, the rows cannot be orthogonal. Thus, we contradict our earlier result leading to the definition of the equiseparation matrix, so $|H| \geq |P|$. ■

Finally, we know that there are different sets of hyperplanes that create the same equiseparation matrix with a given set of points, so we need a notation that expresses the separating property of the hyperplanes, while disregarding geometric properties such as distance and orientation. To this end, we label each of these types of hyperplanes by the points in the smallest partition it creates. For example, the hyperplane that separates the point A, B, and C from the rest of the points is labelled t_{ABC}. The number of hyperplanes of that type in the equiseparation is denoted $|t_{ABC}|$.

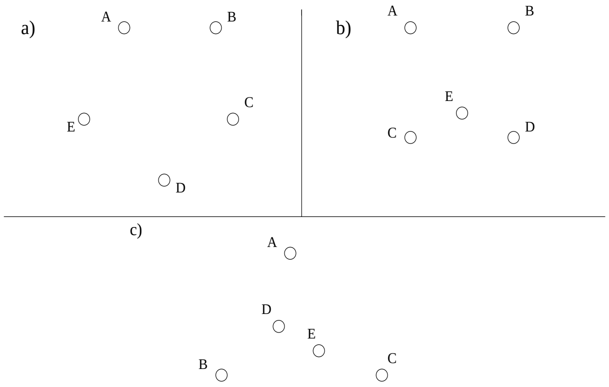

Figure 2: Unique 5 point configurations in 2D

3 Low-dimensional Results

We will now attempt to answer the two equiseparation questions for low dimensions. First, we will see that the maximum number of points for an equiseparation in 2D is 4. Then we will see that the smallest dimension in which one can place 6 points is 3. First, however, we prove a short lemma that is useful in the proofs, and also serves to demonstrate the proof method we use.

Lemma 3: No equiseparation is possible with 3 co-linear points in 2D.

Proof: Suppose A,B, and C are co-linear points. Then there are three possible hyperplane types, t_A, t_C, and t_{ABC}. Now, since points A and B must be separated by exactly half the hyperplanes, and the hyperplanes of type t_A are the only type that can separate them, $|t_A| = |H|/2$. Similarly, $|t_C| = |H|/2$. Now, by examining points A and C, we see that $|t_A| + |t_C| = h/2$, since types t_A and t_C separate A and C. This is a contradiction, so no equiseparation of three co-linear points can exist.

3.1 Five point equiseparation is impossible in 2D

We have already seen an equiseparation of 4 points in 2D, so all that remains to show that this is the maximum number of points is to show that 5 points is impossible. Our proof method first finds all possible unique point configurations in 2D in which an equiseparation may be possible, i.e. those not barred by the above lemma, then proceeds to show why an equiseparation is not.

Proposition 4: No equiseparation is possible with 5 points in 2D.

Proof: We know from the above lemma that the convex hull of any three points in 2D must form a triangle. A fourth point can be added either within the convex hull of the initial three points or outside of it. (Placing it on the convex hull will result in three co-linear points)

In the interest of space, we will only consider case b in Fig. 2 in which four points are placed on the convex hull, and a fifth point is placed within that convex hull. The other cases are similar.

By the above lemma, if the fifth point is co-linear with two other points then an equiseparation is impossible, so it must be added off the main diagonals of the qudrilateral, forcing it to be closer to two of the exterior points than the other two. Label the points as in figure 2. Now, the only types of hyperplanes possible are t_{AC}, t_{BD}, t_{AB}, t_{CD}, t_A, t_B, t_C, t_D, t_{DE}, t_{CE}. If we assume an equiseparation exists, then we can examine any pair of points, and the sum of the number of each type of hyperplanes that separate the two points should be $|H|/2$. Also, the sum of the number of each hyperplane type that does not separate the two points must be $|H|/2$.

* A and D: From examination of these two points we get the equations

I) $|t_{AC}| + |t_{BD}| + |t_{AB}| + |t_{CD}| + |t_A| + |t_D| + |t_{DE}| = |H|/2$ and
II) $|t_B| + |t_C| + |t_{CE}| = |H|/2$

* B and C:

III) $|t_{AC}| + |t_{BD}| + |t_{AB}| + |t_{CD}| + |t_B| + |t_C| + |t_{CE}| = |H|/2$ and
IV) $|t_A| + |t_D| + |t_{DE}| = |H|/2$

Using equation IV, we can substitute $|H|/2$ back into equation I to get $|t_{AC}| + |t_{BD}| + |t_{AB}| + |t_{CD}| + |H|/2 = |H|/2$, which results in $|t_{AC}| + |t_{BD}| + |t_{AB}| + |t_{CD}| = 0$. Since there cannot be negative amounts of hyperplanes, it follows that $|t_{AC}| = |t_{BD}| = |t_{AB}| = |t_{CD}| = 0$. We can delete these types from the list of possible types of hyperplanes.

* C and E:

V) $|t_C| + |t_{DE}| = m$ and
VI) $|t_A| + |t_B| + |t_D| + |t_{CE}| = |H|/2$

* D and E:

VII) $|t_D| + |t_{CE}| = |H|/2$ and
VIII) $|t_A| + |t_B| + |t_C| + |t_{DE}| = |H|/2$

Now, from equation VII we can substitute $|H|/2$ for $|t_D|+|t_{CE}|$ in equation VI, which gives $|t_A|+|t_B|+|H|/2 = |H|/2$. Subtracting $|H|/2$ results in $|t_A| + |t_B| = 0$. Again, there cannot be negative numbers of hyperplanes, so it follows that $|t_A| = |t_B| = 0$. Since these were the only types of hyperplanes separating A and B, there cannot be any hyperplanes separating A and B. Therefore, no equiseparation can exist for this configuration of points. ■

Note: In the above, somewhat cumbersome, proof, we have shown that a certain linear Diophantine system has no positive solution. i.e. the variables $|t_{ABC}|$, etc. have no positive integer values. To our knowledge, there is no automatic way of showing the non-existence of a solution in such a system.

3.2 Six points in 3D

We now wish to find the smallest dimension in which we can place six points in an equiseparation. We saw in the previous section that it is impossible in 2D, so we move on to 3D. It turns out it is possible in 3D, as we now show.

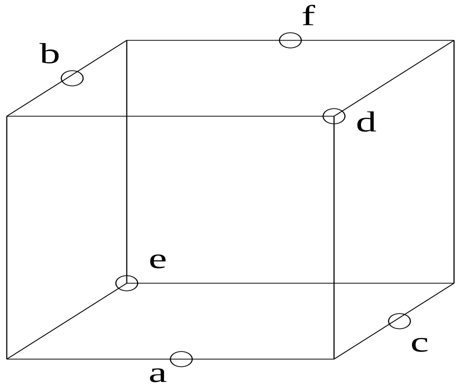

Figure 3: An equiseparation of 6 points in 3D

Proposition 5: An equiseparation of 6 points exists in 3D.

Proof: Suppose a cube as in figure 3 with one vertex at the origin. Give points $A...F$ the coordinates:

1. $A = (1/2 + \delta, 0, 0)$
2. $B = (0, 1/2 + \epsilon, 1)$
3. $C = (1, 1/2 + \epsilon, 0)$
4. $D = (1, 0, 1)$
5. $E = (0, 1, 0)$
6. $F = (1/2 + \delta, 1, 1)$.

where $0 < \delta, \epsilon < 1/2$. Now, add one of each of the following types of planes: $t_{ACE}, t_{CD}, t_{ADE}, t_{EF}, t_{ACF}, t_{AB}, t_{ADF}$. Each type's existence will now be shown.

1. t_{ACE}: Only points A,C, and E are on the $z = 0$ plane, so any plane $z = K$ where $K < 1$ will be of this type.
2. t_{CD}: Only points C and D are on the $x = 1$ plane; all other points have x-coordinate < 1, so any plane $x = K$ where $1/2 + \delta < K < 1$ will be of this type.
3. t_{ADE}: The plane $x + 2y + z = K$ is between lines BC and DE when $1 < K < 1 + 2\epsilon$. Thus, it separates the desired points.
4. t_{EF}: Only points E and F are on the $y = 1$ plane, all other points have y-coordinate < 1, so any plane $x = K$ where $1/2 + \epsilon < K < 1$ will be of this type.
5. t_{ACF}: The plane $-2x - y + k = K$ is between lines AF and DE when $-1 - 2\delta < K < -1$ and separates the desired points.
6. t_{AB}: Only points A and B have x and y coordinates both < 1. Therefore, any plane $x + y < K$ where $\delta < K < 1$.

7. t_{ADF}: The plane $x - y + z = K$ is between lines BC and AF when $1/2 - \epsilon < K < 1/2 + \delta$, and thus separates the desired points.

Thus, every pair of points has exactly 4 of the 7 planes separating them. By adding one additional plane of type t_{ABCDEF}, so that it does not separate any of the points, each pair of points will be separated by 4 of the 8 planes. Hence, an equiseparation exists.

4 Techniques for Arbitrary Dimension

Clearly, it would be very difficult to extend the proof methods used above to arbitrary dimension. We need something more powerful. This brings us then to Hadamard matrices. The definition of a Hadamard matrix and general properties about them can be found in [6]. To aid our progress, we will make one critical assumption about equiseparations. We assume that, if an equiseparation exists with 2^p points and hyperplanes passing through the origin, then there is one with hyperplanes passing through the origin whose equiseparation matrix is the Hadamard matrix H_{2^p}. This may not be true in dimensions which are not a power of 2, but for our application, we will consider only dimensions which are powers of 2, so the assumption is justified.

We now make some observations about Hadamard matrices. A Hadamard matrix can be defined recursively in the Sylvester form as follows:

$$H_{2^{p+1}} = \left[\begin{array}{cc} H_{2^p} & H_{2^p} \\ H_{2^p} & -H_{2^p} \end{array} \right]$$

It is also helpful to label the rows and columns of an H_{2^p} Hadamard matrix lexigraphically with elements of $\mathbb{F}_2{}^p$. We can then show the following lemma.

Lemma 6: The $(x, y)^{th}$ entry of H_{2^p} in Sylvester form (when x and y are expressed as elements of $\mathbb{F}_2{}^p$) is given by

$$(-1)^{\langle x,y \rangle}$$

Proof (by induction on p):

Base step: $(p = 1)$ H_{2^1} contains 1 in all entries except in $(1, 1)$, where it is -1. This is consistent with the given formula.

Inductive step: We will assume the proposition to be true for $p = k$. First, observe that the Hadamard matrix in Sylvester form is defined recursively, as above. Since we label the rows and columns in lexical order, the first half of the rows and columns will always have a 0 as the first term in their label. Thus, the first term will have no effect on the calculated inner product, so the structure for the first half of the rows and columns in $H_{2^{k+1}}$ will be the same as in H_{2^k}. In the case where the first term in the labelling vector for both the row and the column is 1, then a 1 is added to the sum of the remaining terms. Since the addition is in $\mathbb{F}_2{}^{k+1}$, the final inner product will be the opposite of the sum of the remaining terms. These remaining terms are a label in H_{2^k}, so the entry in $H_{2^{k+1}}$ as computed by the formula will be the opposite as the corresponding entry in H_{2^k}. Thus, we have the recursive definition of the Hadamard matrix. ■

This lemma gives us a formula that allows us to deal with equiseparations in an abstract way, which gives us the ability to deal with higher dimensions, and possibly induct to answer the equiseparation question for arbitrary dimension.

4.1 Demonstration of proof method using Hadamard matrices

First, some observations. Suppose we have an N-dimensional space A divided into orthants by the coordinate hyperplanes. Define the *sign vector* of an orthant to be the vector that gives the signs of the terms of any vector in that orthant. Then, if we can find a d-dimensional subspace B of A that intersects a set of orthants of A whose sign vectors are orthogonal, we can place points in those orthants on B, and each of these points will be separated by exactly half the hyperplanes, all of which pass through the origin. Thus, we have an equiseparation in d-dimensions with planes passing through the origin. The equiseparation matrix is the matrix whose rows are the sign vectors of the orthants intersected by A.

Proposition 7: The Hadamard matrix H_{2^p} cannot be realized in p dimensions with hyperplanes through the origin.

Before we prove this proposition, we will need the following useful theorem, which allows us to slightly alter the proposition into a form that is easier to prove. First some definitions.

Definition: A subspace S *intersects* an orthant x if there exists a vector $\mathbf{v} \in S$ whose signs exactly match the sign vector of x.

Definition: A subspace S *touches* an orthant x if there exists a vector $\mathbf{v} \in S$ whose signs match the sign vector of x wherever $\mathbf{v}$ is non-zero.

Duality Theorem: For all subspaces S, S intersects some orthant x if and only if $S^{\perp}$ does not touch x except at the origin.

Proof: First, the forward direction. Let S be a subspace such that S intersects x for some arbitrary orthant x. Then there exists a vector $\mathbf{v} \in S$ such that $\mathbf{v} = (v_1, ..., v_k)$ and $v_1, ..., v_k$ match the signs given by orthant x. Now, suppose by way of contradiction that $S^{\perp}$ touches x. Then there is a vector $\mathbf{r} \in S^{\perp}$ such that $\mathbf{r} = (r_1, ..., r_k)$ where $r_1, ..., r_k$ are either 0 or match the signs given by orthant x. At least one $r_i > 0$. Consider the inner product $\langle \mathbf{v}, \mathbf{r} \rangle = v_1 \times r_1 + ... + v_k \times r_k$. Wherever $r_i \neq 0$, the product $r_i \times v_i > 0$, since r_i and v_i have the same sign. Therefore, $\langle \mathbf{v}, \mathbf{r} \rangle > 0$. But this violates the assumption that S is othogonal to $S^{\perp}$, so $\mathbf{r}$ must not exist. Therefore, $S^{\perp}$ does not touch orthant x

Now the reverse direction. We will show the contrapositive, that is, show that if a subspace S does not intersect an orthant x, then $S^{\perp}$ touches x. We will do this by constructing a vector $\mathbf{y} \in S^{\perp}$ whose terms match the signs given by orthant x where $\mathbf{y}$ is non-zero. Without loss of generality, we will assume that S does not intersect the all-positive orthant and show that $S^{\perp}$ touches this orthant. First, consider the vector $\mathbf{o} = (1, 1..., 1)$. Clearly, this vector is in the all-positive orthant, and thus is not contained in S. We want to construct our $\mathbf{y}$ so that $||\mathbf{y}||_1 \leq 1$ and $|\langle \mathbf{o}, \mathbf{y} \rangle| \geq 1$. These two conditions guarantee that $\mathbf{y}$ has the signs matching orthant x. Let $\mathbf{o}^*$ be the vector with signs matching orthant x so that $||\mathbf{o} - \mathbf{o}^*||_\infty$ is minimized. Also let $\mathbf{o}|_{S^{\perp}}$ be the vector found by projecting $\mathbf{o}$ onto $S^{\perp}$. Now, let $\mathbf{y} = (\mathbf{o}|_{S^{\perp}})||\mathbf{o} - \mathbf{o}^*||/||\mathbf{o}|_{S^{\perp}}||_2^2$. To show that $||\mathbf{y}||_1 \leq 1$, notice that $||\mathbf{y}||_1 = max_{\mathbf{z} \in Span\{S \cup \mathbf{o}\}}$ of $|\langle \mathbf{z}, \mathbf{y} \rangle|/||\mathbf{z}||_\infty$.

Since $\mathbf{z} \in Span\{S \cup \mathbf{o}\}$ we can write $\mathbf{z}$ as $\mathbf{z} = k(\mathbf{o} - \mathbf{u})$ where $\mathbf{u} \in S$. By showing that $|\langle x, \mathbf{y}\rangle|/||x||_\infty \leq 1$ for all $x \in Span\{S \cup \{\mathbf{o}\}\}$ we know that it is also true for $\mathbf{z}$. By substitution, we get $k\langle \mathbf{o}|_{S^\perp} - \mathbf{u}, \mathbf{o}|_{S^\perp}\rangle / ||\mathbf{o}|_{S^\perp}||_2{}^2 * ||\mathbf{o} - \mathbf{o}^*||_\infty / k||\mathbf{o} - \mathbf{u}||_\infty$.
Since $\mathbf{o} - \mathbf{o}^*$ in the numerator is the closest vector to $\mathbf{o}$ with respect to the infinity norm, we know that $||\mathbf{o} - \mathbf{o}^*||_\infty$ is smaller than the terms in the denominator, therefore, this expression is always less than or equal to 1, so $||\mathbf{y}||_1 \leq 1$.

We now need only show that $|\langle \mathbf{o}, \mathbf{y}\rangle| \geq 1$. This follows almost immediately once we realize that $\mathbf{o} = \mathbf{o}|_{S^\perp} + \mathbf{o}|_S$. The expression reduces to $\langle \mathbf{o}|_{S^\perp}, \mathbf{o}|_{S^\perp}\rangle = ||\mathbf{o}|_{S^\perp}||_2{}^2$, which must be greater than 1. ■

We are now ready to prove proposition 7.

Proof of Proposition 7: Suppose we have a 2^p-dimensional space T. Then, if we can find a p-dimensional subspace S, which we will represent by its basis B of p rows of length 2^p, that intersects the orthants given by the rows of H_{2^p}, we will have found an equiseparation of 2^p points in p-dimensions. Since we want to show this is not true, we will prove that for all subspaces S of T, S does not intersect at least one H_{2^p} orthant of T.

By the duality theorem, this is equivalent to showing that $S^\perp$ touches at least one H_{2^p} orthant of T. Since our basis consists of 2^p columns of length p, we know from linear algebra that any $p+1$ columns must be linearly dependent. Therefore, we can find a vector $\mathbf{x}$ orthogonal to B by setting the entries of $\mathbf{x}$ to zero everywhere except where it corresponds to the $p+1$ linearly dependent columns. Since the $p+1$ vectors are linearly dependent, we can always find some entries for which $B\mathbf{x} = 0$. This is true for every possible basis.

Now, all that remains is to show that any vector $\mathbf{x}$ chosen in this way always touches one orthant of H_{2^p}. We will choose the column labeled 0 in $\mathbb{F}_2^p$ and p other columns whose labels are independent in $\mathbb{F}_2^p$. Since these columns are independent, the matrix formed by the intersection of these columns with the rows of H_{2^p}, will, in its rows, acheive every possible partition of 1 and -1. Thus, given any vector $\mathbf{x}$, it must match the signs of one of these rows, since every possible partition of signs is represented in one of the rows. Therefore, every subspace has a space orthogonal to it that touches at least on H_{2^p} orthant, and by the duality theorem, does not intersect one H_{2^p} orthant. ■

Proposition 8: The Hadamard matrix H_{2^p} can be realized in $3/4 \times 2^p$ dimensions.

Proof: This is equivalent to the statement that $\exists$ a subspace S, again represented by its basis, of dimension $3/4 \times 2^p$ that intersects every H_{2^p} orthant of some 2^p-dimensional space. To show this, construct B as orthonormal to a $2^p/4$-dimensional subspace with basis Q_p which we will construct inductively on p as follows.
Base case: We will start with $p = 2$. Then the dimension of Q_2 is 1. Since we only need to show that we can realize H_{2^p}, we can choose any vector we wish for the basis of Q. In this proof, we will choose the vector $(1, 1, 1, -1)$. Since we want the subspace orthonormal to Q to intersect every H_{2^2} orthant, we need to show that, for every row in H_{2^2}, we can find a vector orthogonal to Q that has the same sign in every entry. The vector $(1, 1, 1, 3)$ is orthogonal and has the same signs as the first row of H_{2^2}. The vectors $(1, -3, 1, -2)$, $(1, 1, -3, -1)$, and $(3, -1, -1, 1)$ are also orthogonal to Q, and have the same signs as the second, third, and fourth rows of H_{2^2}. Thus, we know the subspace B orthogonal to Q contains these vectors, and thus intersects every H_{2^2} orthant of S and has dimension $3/4 \times 2^2 = 3$. Thus, our proposition holds in the base case.

Inductive Hypothesis: $\exists$ a subspace Q_p such that $\forall$ rows $r \in H_{2^p}$, $\exists$ a vector $x_{r,p}$ with $Q_p\mathbf{x_{r,p}} = 0$ and $x_{r,p}$ has the same sign as r.

Inductive step: We will assume the proposition is true for p, and show it for $p+1$. First, let our subspace Q_{p+1} have the following matrix as its basis.

$$Q_{p+1} = \begin{bmatrix} Q_p & 0 \\ 0 & Q_p \end{bmatrix}$$

Now, if we also take each vector $x_{r,p}$ from the earlier step and use the new vectors $x_{r,p+1}$ and $x_{r+2^p,p+1}$ defined by $x_{r,p+1} = (x_{r,p}\ x_{r,p})$ and $x_{r+2^p,p+1} = (x_{r,p}\ {-x_{r,p}})$, then we see that the new vectors are orthogonal to Q_{p+1}. Also, due to the recursive structure of the H_{2^p} Hadamard matrix discussed earlier, vectors of the form $(x_{r,p}\ x_{r,p})$ will match the signs of the top half of the rows of the Hadamard matrix, while vectors of the form $(x_{r,p}\ {-x_{r,p}})$ will match the signs of the bottom half of the rows. So, we have a subspace B of dimension $3/4 \times 2^{p+1}$ that intersects the $H_{2^{p+1}}$ orthants of S. It follows from the induction that this is true for all p. ■

4.2 Conjectures for a Tighter Lower Bound

The conjecture presented in this section, if proven true, will show a much tighter lower bound on the dimension needed to have an equiseparation of 2^p points. This lower bound is superpolynomial, which is our desired result.

Conjecture 9: H_{2^p} cannot be realized in 2^{p-1} dimension with planes passing through the origin.

We will reformulate this problem as in the previous two proofs. It then becomes the following.

Conjecture 10: Any subspace $S \subset \mathbb{R}^{2^p}$ of dimension 2^{p-1} does not intersect at least one H_{2^p} orthant.

We can use the duality theorem to get the following conjecture.

Conjecture 11: Any subspace $S \subset \mathbb{R}^{2^p}$ of dimension 2^{p-1} touches at least one H_{2^p} orthant.

Assumption: For simplicity, we make the assumption that every subspace S is spanned by vectors in $\{1, -1\}^{2^p}$.

Intended proof of Conjecture 11: By induction.
Induction step A:
Given any matrix B ($2^{p-1} \times 2^p$) with (-1,1) entries representing the basis of S, $\exists \mathbf{v} \in S^\perp, B\mathbf{v} = 0$ and there exists a row $\mathbf{r}$ of H_{2^p} such that $\forall i, sign(\mathbf{r}_i) = sign(\mathbf{v}_i)$ wherever $\mathbf{v}_i \neq 0$.

Induction step B:
Given any matrix B ($2^{p-1} \times 2^{p+1}$) with (-1,1) entries, then $\exists$ a ($2^p \times 2^p$) submatrix of H_{2^p} denoted $M_{R,C}$ given by the intersection of rows in R and columns in C such that $\forall i \in R, \exists \mathbf{v}$ such that $B\mathbf{v} = 0$ wherever $i \in C$.

4.2.1 Results towards induction step B

Definition: Let S be a subspace of $\mathbb{F}_2{}^p$ of order m. A subset $S' = x_1, ..., x_m$ of $\mathbb{F}_2{}^p$ is a *subspace-like* set derived from S if $x_1 \in S^{\perp}$, $x_i \notin S^{\perp}$ for $i \in 2, 3, ..., m$, and $x_i + x_j \notin S^{\perp}$, $\forall i, j$, $i \neq j$. [3]

Proposition 12: $\forall$ subsets $S \subset R$, where R is the row set of a Hadamard matrix H and $|S| = |R|/2$, and $\forall$ $D \subset C$, where C is the column set of H, $|D| = |C|/2$, and D is a subspace-like set derived from S, we have the following:
1. $M_{S,D}$ is the Hadamard matrix $H_{2^{p-1}}$
2. $M_{S,D} = M_{S,\bar{D}}$
3. $M_{\bar{S},D}$ is an orthogonal matrix.
4. $M_{\bar{S},D} = -M_{\bar{S},\bar{D}}$

Proof: Before we show this, we first need a quick lemma.

Lemma 13: If T is a subspace-like set derived from subspace $S \subseteq \mathbb{F}_2{}^p$, then $\bar{T}$ is also a subspace-like set derived from S.

Proof: Since dim(S) = $p-1$, dim($S^{\perp}$) = 1. Therefore, $S^{\perp}$ contains only the zero vector and one other vector. Since T is a subspace like set derived from S, it must contain exactly one of these vectors.

Notice that $\bar{T}$ is the coset of T, $T + y$, where y is the non-zero vector in $S^{\perp}$. Clearly, $\bar{T}$ contains only one vector in $S^{\perp}$. Now, consider two vectors in $\bar{T}$, x_1 and x_2. Then we can rewrite x_1 and x_2 as $y_1 + y$ and $y_2 + y$, where y_1 and y_2 are in T.The y's cancel, so $x_1 + x_2 = y_1 + y_2$, and since $y_1 + y_2 \notin S^{\perp}$, neither is $x_1 + x_2$. Thus $\bar{T}$ is a subspace-like set derived from S. ■

Proof of Prop. 12:

1. This is shown in [3], Theorem 9.

2. This follows from 1 and Lemma 13. Since $\bar{D}$ is a subspace-like set derived from S, Theorem 9 also applies. Since both $M_{S,D}$ and $M_{S,\bar{D}}$ are $H_{2^{p-1}}$, they are equal.

3. Observe that $\bar{S}$ is a coset of S, $S + y$, where $y \notin S$. Since $M_{S,D}$ is an orthogonal matrix, and we know that adding some vector (in this case y) to every vector in one of the intersecting sets that form a submatrix does not change its orthogonality, it follows that $M_{\bar{S},D}$ is orthogonal.

4. We need to show that $\forall s_i \in \bar{S}(-1)^{\langle s_i, y\rangle} = -(-1)^{\langle s_i, z\rangle}$ where $y \in D$ and $z \in \bar{D}$. Since $\bar{S}$ is a coset of S, $\forall s_i \in \bar{R}$, $\exists s \notin R$ such that $s_i = s_i{}' + s$ where $s_i{}' \in R$. Also, $\forall d_i \in \bar{D}$, $\exists d \in S^{\perp}$ such that $d_i = d_i{}' + d$ where $d_i{}' \in D$. Therefore, we need only show that $\forall s_i{}' \in S(-1)^{\langle s_i{}' + s, d_i{}'\rangle} = -(-1)^{\langle s_i{}' + s, d_i{}' + d\rangle}$ where $d_i{}' \in D$. The right hand side of this equation can be rewritten as $-(-1)^{\langle s_i{}' + s, d_i{}'\rangle} \times (-1)^{\langle s_i{}' + s, d\rangle}$. It follows that $(-1)^{\langle s_i{}' + s, d\rangle} = -1$, which implies that $\langle s_i{}' + s, d\rangle = 1$, which leads to $\langle s_i{}', d\rangle + \langle s, d\rangle = 1$. But since $d \in S^{\perp}$, we know that $\langle s_i{}', d\rangle = 0$, so $\langle s, d\rangle = 1$.

Examine the set $\{d\}^{\perp}$. Since d is an independent element, the dim($\{d\}$) $= 1$. Therefore, dim($\{d\}^{\perp}$) = dim($\mathbb{F}_2{}^p$) -1. But this is the same as dim(R), and since $d \in R^{\perp}$, $R \subseteq \{d\}^{\perp}$. Therefore $R = \{d\}^{\perp}$. So, $s \notin \{d\}^{\perp}$. Therefore $\langle s, d\rangle = 1$. Thus, $\forall s_i \in \bar{S}(-1)^{\langle s_i, y\rangle} = -(-1)^{\langle s_i, z\rangle}$ where $y \in D$ and $z \in \bar{D}$ which implies that $M_{\bar{S},D} = -M_{\bar{S},\bar{D}}$. ■

5 A MATLAB Experiment

In an attempt to find a counterexample to conjecture 11, we used the linear algebra software, MATLAB©. The linear program we used is as follows.

Linear Program: For each row $\mathbf{r} \in H_{2^p}$, maximize $< \mathbf{x}, \mathbf{r} >$ subject to $B\mathbf{x} = 0$, $x_i r_i > 0$ and $x_i \leq 1$.

This determines all orthants of H_{2^p} that touch $S^{\perp}$. In addition, it finds the vector in $S^{\perp}$ that touches the orthant the "best" (that is, $\mathbf{v}$ has the least number of zeros possible). This can be helpful in looking for the worst cases for B. If we can show that a matrix of a particular form causes the least number of orthants to touch, or causes the "worst" touches, and then show that it still touches some orthant, then it may lead to a proof.

We determined several results from MATLAB. First, we constructed random boolean matrices B of sizes from 4×8 to 16×32. Using the preceeding linear program on large sets of random 8×16 test-matrices, we found that the least number of the sixteen orthants that were ever touched was 6. In addition, when the touches were only on a low number of dimensions, there were always large numbers of orthants touched. After many tests with larger matrices, we have not yet found a counterexample to our conjecture.

Finally, we note that when B has certain properties, such as being a subset of the rows of H_{2^p}, or not depending at all on a particular row of H_{2^p}, we see some trivial, yet moderately interesting results. Thus, our next approach was to look at the vectors in B in the orthonormal Hadamard basis, consisting of normalized vectors from the Hadamard matrix. Denote the Hadamard basis of S by $[S]_H$. Now let $C = [S]_H$. If every row of C has exactly two non-zero entries, then Conjecture 2 is satisfied. That is, when we can express each vector in the basis of S as a linear combination of a pair of rows of H_{2^p}, then there is a vector in $S^{\perp}$ that touches H_{2^p}. First we consider a few lemmata. Formally,

Theorem 14: Let B be a $2^{p-1} \times 2^p$ matrix such that the rows of B, $\mathbf{b^j} = a^j \mathbf{r^j} + a^{j'} \mathbf{r^{j'}}$ for $\mathbf{r^j}, \mathbf{r^{j'}} \in H_{2^p}$. Then $\exists \mathbf{x} : B\mathbf{x} = 0$ and $\mathbf{x}$ touches H_{2^p}.

Lemma 15: If B' is any $2^{p-1} \times 2^p$ matrix representing a subspace of $\mathbb{R}^{2^p}$ and each row of B is an arbitrary linear combination of two rows of H_{2^p}, and B is any $2^{p-1} \times 2^p$ matrix with each row $\mathbf{b^i} = \frac{1}{2}(1 + \delta^i)\mathbf{r^i} + \frac{1}{2}(1 - \delta^i)\mathbf{r^{i'}}$ where all the $\mathbf{r^j}$ and $\mathbf{r^{k'}}$ are distinct rows of H_{2^p}, then if there exists $\mathbf{x}$ touching H_{2^p} for any B then there exists $\mathbf{x}'$ touching H_{2^p} for any B'.

Proof: Express the rows of B' as $\mathbf{b^{i'}} = a^i \mathbf{r_i} + a^{i'} \mathbf{r'_i}$. Then we can let $\delta^i = \frac{a^i - a^{i'}}{a^i + a^{i'}}$. Because the subspace spanned by B' is invariant under scalar multiplication of the rows of B', we can multiply each row by $\frac{1}{a^i + a^{i'}}$ and we see that B and B' are now in the same form. We can justify the requirement that the rows from H_{2^p} be unique in B with the following. Suppose a row is used twice in B'. Since there are only 2^{p-1} vectors in the basis of B' and two rows per vector, there are exactly 2^p vectors to choose and 2^p rows to choose from. If one row is chosen twice then another row, $\mathbf{r}$ must not be chosen at all. Then we have $[B\mathbf{r}] = 0$ already so any choice of $\mathbf{x}$ will suffice. ■

So now we can prove a more specific case with the help of two definitions.

Definition: Let $\mathbf{x} \in \{\pm 1, \pm\delta^i\}^{2^p}$, with $1 \neq \delta^i > 0$. Define

$s(\mathbf{x}) = \mathbf{y} \in \{\pm 1\}^{2^p}$, where $y_i = -1$ if $x_i < 0$ and $y_i = 1$ if $x_i > 0$. Define $\delta(\mathbf{x}) = \mathbf{x} \in \{\pm 1\}^{2^p}$, where $z_i = 1$ if $x_i \in \{\pm 1\}$ and $z_i = -1$ if $x_i \in \{\pm \delta^i\}$.

We will now consider a particular row $\mathbf{b^j}$ of B and construct a solution $\mathbf{x}$.

Lemma 16: Let B be a $2^{p-1} \times 2^p$ matrix composed of row-vectors $\mathbf{b^j} = \frac{1}{2}(1+\delta^j)\mathbf{r^j} + \frac{1}{2}(1-\delta^j)\mathbf{r^{j}}'$ with all the $\mathbf{r^j}$ and $\mathbf{r^{k}}'$ distinct rows of H_{2^p}. Then $\exists \mathbf{x} : B\mathbf{x} = 0$ and $\mathbf{x}$ touches H_{2^p}.

Proof: Consider for some j, $s(\vec{b_j})$ and $\delta(\vec{b_j})$. Let $\mathbf{b^j} = \frac{1}{2}(1+\delta^j)\mathbf{r^j} + \frac{1}{2}(1-\delta^j)\mathbf{r^{j}}'$. Clearly, $s(\vec{b_j}) = \mathbf{r^j}$ and $\delta(\vec{b_j}) = \mathbf{r^j}\mathbf{r^{j}}'$. We are looking for $\mathbf{x}$ with $B\mathbf{x} = 0$ and $s(\mathbf{x}) \in H_{2^p}$. So let $\mathbf{x}$ such that $s(\mathbf{x}) = \mathbf{r^{j}}'$ and $\delta(\mathbf{x}) = -\mathbf{r^j}\mathbf{r^{j}}' = -\delta(\vec{b_j})$. It is clear that $\mathbf{x}$ touches H_{2^p}. So we must now show that $B\mathbf{x} = 0$, that is, each row of B is orthogonal to $\mathbf{x}$. First consider $\mathbf{b^j}$. $<\mathbf{x}, \mathbf{b^j}>= \Sigma_i x_i b_i^j$. Since $\delta(\mathbf{x}) = -\delta(\vec{b_j})$, we have $x_i b_i^j = \pm\delta^j$. Thus, $<\mathbf{x}, \mathbf{b^j}>= \delta^j \Sigma_i s(\mathbf{x})_i s(\vec{b_j})_i = \Sigma_i r_i^j r_i^{j'} =< \mathbf{r^j}, \mathbf{r^{j}}' >= 0$ because r^j and $r^{j'}$ are distinct and orthogonal. Next we consider the other case, of $\mathbf{b^k}$ when $k \neq j$. Then the sum $<\mathbf{x}, \mathbf{b^k}>= \Sigma_i x_i b_i^k$. Each term is a member of $\{\pm 1, \pm\delta^j, \pm\delta^k, \pm\delta^j\delta^k\}$. In order for this sum to be zero, we must group the terms together into four separate sums. We see that we can separate $\mathbb{F}_2^p$ into four subsets of column labels and the sum of $s(\vec{b_k})_i s(\mathbf{x})_i$ over each set of labels must be zero. So we will look at the qualifications for this partitioning. The classificaton of a column label into one set is determined by $\delta(\vec{b_k})_i$ and $\delta(\mathbf{x})_i$. Now recall that $\mathbf{r^j}$, $\mathbf{r^{j}}'$, $\mathbf{r^k}$, $\mathbf{r^{k}}'$ are all distinct by our hypothesis. Thus, the product of any two of them cannot be the all-positive row. Since $\delta(\mathbf{x}) = -\mathbf{r^j}\mathbf{r^{j}}' \neq (++\ldots+)$ and $\delta(\vec{b_k}) = \mathbf{r^k}\mathbf{r^{k}}' \neq (++\ldots+)$. Now we look at the vector we are partitioning. We are splitting up the vector that is the product of the two sign vectors, $s(\vec{b_k})s(\mathbf{x}) = \mathbf{r^k}\mathbf{r^{j}}'$. If this vector was equal to the product of the two δ vectors, then we could divide the two vectors out and see that the product of the other two, $\mathbf{r^{k}}'\mathbf{r^j} = (++\ldots+)$, which we know cannot happen since the two rows must be distinct. Thus, the row we are partitioning is *not* the product of the two rows we are using to partition it. In addition, it is *not* the all-positive row. Therefore, the sum of each partition is zero, and thus $<\mathbf{b^k}, \mathbf{x}>= 0$. Therefore, $\mathbf{x}$ satisfies the proposition. ■

Theorem 14 follows directly from lemmata 15 and 16.

Unfortunately, this approach is too limited and cannot be extended to a more general case. To illustrate this, we will try to extend it. First, we will consider the extent to which we need to extend this. Given a matrix B, we can look at $[B]_H$ and we have the same subspace represented in a different basis. We have proven that if we can reduce this to have exactly two non-zero entries in each row, then we have sufficiently proved what we need. But when we consider reducing this matrix with row operations, the best we can hope for is about half non-zero columns. This could possibly be extended further by considering also the row and column operations that preserve equiseparations, beyond only the standard ones. But this only allows for a few specific column transforms, so we will most likely not be able to eliminate more than one or two more columns, and not from all the rows.

So we will consider extending the proof to allow more nonzero columns. Say we allow 3 non-zero columns in each row. This causes two obvious problems with no solution in sight. First, we can no longer assume that each column has exactly one non-zero entry. This was a staple in the previous proof. Second, we need two paramaters to express a triple (x, y, z) when we disregard scalar multiplication - thus we would have more than simply a sign vector and a δ vector for each row. This would complicate the proof to the point where it would no longer work at all. Because of this, we must look for other methods of solving this problem.

5.1 Boolean Matrices and Cube Mappings

Because of the nature of the problem we are trying to solve – threshold circuits – we may add the constraint that the matrix B must contain entries from $\{-1, 1\}$. This assumption leads to several interesting results. First, we will look at a smaller case, with B a 2×4 matrix.

Let b_1^+ and b_1^- be the sets of columns for which $b_1 = +1$ and $b_1 = -1$ respectively. That is, if $i \in b_1^+$, then $B_{1i} = +1$, and similarly for b_1^-. Define b_2^+ and b_2^- the same way. When $\mathbf{b}_1 \neq \mathbf{b}_2$ we can use sets to prove that there exists $\mathbf{x}$ touching H_{2^p} with $B\mathbf{x} = 0$. Specifically, we force $\mathbf{x}$ to be all-positive and then take any $\mathbf{o} \in H_{2^p}$, then show that $[B\mathbf{o}]\mathbf{x} = 0$.

Proposition: For $p > 1$, let B be a 1×2^p matrix which contains one vector b_1 in $\{-1, 1\}^{2^p}$. Then there exists $\mathbf{o} \in H_{2^p}$ such that $[B\mathbf{o}]^\perp$ contains an all positive vector. *Proof:* Let b^1 and b^2 be defined such that $b_1 = (b^1, b^2, \ldots)$ and define $\mathbf{x} = (1, 1, 0, 0, \ldots)$. If $b^1 = b^2$, let $\mathbf{o} = (+-+-\ldots) \in H_{2^p}$. If $b^1 \neq b^2$, let $\mathbf{o} = (+++\ldots) \in H_{2^p}$. In both cases, $[B\mathbf{o}]\mathbf{x} = 0$ so the all-positive vector $\mathbf{x} \in [B\mathbf{o}]$. ■

Proposition: For $p > 2$, let B be a 2×2^p matrix which contains two vectors b_1 and b_2 in $\{-1, 1\}^{2^p}$. Then there exists $\mathbf{o} \in H_{2^p}$ such that $[B\mathbf{o}]^\perp$ contains an all positive vector. *Proof:* First we assume $\mathbf{o} = (++\ldots+)$, the all-positive orthant. We have defined b_1^+, b_1^-, b_2^+, and b_2^- and we assume that $b_1 \neq b_2$. If they were equal then we have the case of B is only one vector, which we proved above. For any $\mathbf{x} = (x^1, x^2, x^3, \ldots)$ we can conclude that $\mathbf{x} \in B^\perp$ iff

$$\forall j : \sum_{i \in b_j^+} x^i = \sum_{i \in b_j^-} x^i$$

In fact, this equation holds regardless of the number of rows in B.

For this case with two vectors, we have $\sum_{i \in b_1^+} x^i = \sum_{i \in b_1^-} x^i$ and $\sum_{i \in b_2^+} x^i = \sum_{i \in b_2^-} x^i$. I will adopt the notation $\sum S := \sum_{i \in S} x^i$. We can add and subtract the previous two equations to get $\sum b_1^+ \cap b_2^+ + \sum b_1^+ \cap b_2^+ = \sum b_1^- \cap b_2^- + \sum b_1^- \cap b_2^-$ and $\sum b_1^+ \cap b_2^- + \sum b_1^+ \cap b_2^- = \sum b_1^- \cap b_2^+ + \sum b_1^- \cap b_2^+$. We can split the unions into the sum of three intersections with $A \cup B = (A \cap \bar{B}) \cup (\bar{A} \cap B) \cup (A \cap B)$. This yields $\sum b_1^+ \cup b_2^+ = \sum b_1^- \cup b_2^-$ and $\sum b_1^+ \cup b_2^- = \sum b_1^+ \cup b_2^-$. Since these four intersections are mutually exclusive, as long as both $b_1^+ \cap b_2^+$ and $b_1^- \cap b_2^-$ are non-empty or both $b_1^+ \cap b_2^-$ and $b_1^- \cap b_2^+$ are non-empty then we can easily find a solution, such as setting $x^i = 1$ for exactly one i in each of the four (or two) intersections. Then $\mathbf{x}$ will satisfy the proposition. Otherwise, we can assume without loss that $b_1^+ \cap b_2^+ = \varnothing$ and $b_1^+ \cap b_2^- = \varnothing$. Then we can combine the two statements and get

$b_1^+ \cup (b_2^+ \cap b_2^-) = \varnothing$. Since $b_2^+ \cup b_2^- = \mathbb{F}_2^p$, we conclude that $b_1^+ = \varnothing$. So we can pick $\mathbf{o} \in H_{2^p}$ such that $\mathbf{o} \neq \mathbf{b}_1$ and $\mathbf{o} \neq \mathbf{b}_2$. This is possible for $p > 2$. Now $B' = [Bo]$ does not have an all-positive or all-negative vector. So this proof holds for B' and our proposition follows. ■

We can extend this example to larger matrices. Given a matrix B of dimensions (m, n), we can represent it as n vertices on an m-dimensional cube. Each column of the matrix gives the coordinate of a single vertex. If the convex hull of the vertices includes the origin, then there exists $\mathbf{x} \neq \mathbf{0}$ with $x_i \geq 0$ and $B\mathbf{x} = 0$. Similarly, we can apply a transformation to the cube. Given a row $\mathbf{o} \in H_{2^p}$ we can multiply B by $\mathbf{o}$. In order to see the geometric interpretation, we must develop some way of labeling the columns. Because they are useful in dealing with Hadamard matrices, it makes sense to label the rows and columns of a matrix with elements of the Galois field $\mathbb{F}_2^p$.

Using the column labels, we see that multiplying B by $\mathbf{o}$ is the same as reflecting the corresponding vertices about the origin. If ℓ is a column label and $\mathbf{o}_\ell = -1$, then we multiply the entire ℓ^{th} vertex by -1.

This leads to another result. If two columns of B are identical, then we have satisfied the conjecture. When we look at the cube, we see two points on a single vertex. For any two columns there is some row of H_{2^p} that is positive in one column and negative in the other. By applying that row to B, we reflect one of the two points at the particular vertex across the origin and the other stays still. The convex hull of these two points is a line passing though the origin.

When we consider the case of a 3×4 B matrix, we find a counter-example to the concludion of the conjecture, although the hypothesis is not satisfied. We now have four vertices on a three-dimensional cube. Consider the case when we have a vertex and the three adjacent vertices selected. If the vertex in the center is assigned the column label 00, then it is possible to apply a row of the Hadamard matrix and find a solution. However, if we assign a different colunn label to the vertex in the center, such as

$$B = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

it becomes apparent that there is no way to reflect vertices using Hadamard rows and cause the convex hull to include the origin. This shows a startling result: the order of the columns in the matrix is actually important in some cases.

Finally we will consider one more case. When B is a 4×8 boolean matrix, we can show that there exists some positive $\mathbf{x}$ and some $\mathbf{o} \in H_{2^3}$ such that $[B\mathbf{o}]\mathbf{x}$=0.

When looking at the 4×8 case it is important to see that there are exactly 16 different vectors in $\{-1, 1\}^4$ and eight of them are simply negations of the other eight. If we have a duplicated column or a column which is a negative of another, then either the convex hull already includes the origin because of these two points or we can flip one of them so that the convex hull includes the origin. So any matrix B that we have is a column permutation and negation of some of the columns of

$$B_0 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}$$

We can use this to our advantage in this proof, but in larger cases, it will no longer help, because $2^{2^{p-1}} > 2 * 2^p$ when $p > 3$.

First we introduce the following convenient terminology:

Definition: $S \subset \mathbb{F}_2^3$ is "good" iff S is a subgroup or coset with $|S| = 4$ and $S \neq \{000, 110, 011, 101\}$ and $S \neq \{111, 100, 010, 001\}$.

Now we continue the proof. Note that B_0 satisfies our hypothesis. Take any four columns whose labels form a "good" subgroup or coset. Then there is a dependence and the submatrix of H_{2^3} formed from the same four columns includes every four-element boolean vector with even number of pluses and minuses. We can verify that all the four-column dependences in B_0 are of the form $c_1 + c_2 - c_3 - c_4 = 0$, that is, two rows are positive and two are negative. So by including all even boolean vectors, we are guaranteed a solution x with $B_0 x = 0$.

Now consider permutations of the columns of B_0. We note that every subset of four column labels yields all even sign-combinations when we look at those columns of H_{2^3}. So regardless of the permutation, the columns that have "good" subgroups or cosets mapped onto them will now yield a solution. Thus, as long as there is a submatrix of B that is equal to or a neagation of a submatrix of B_0 with "good" column labels, we have a solution. In fact, we also have a solution if exactly two of the four columns are negated as well.

We finally consider negations. Consider again B_0. Suppose we negate three or less columns. There will always be a subgroup or coset in the remaining five columns. Similarly, if we negate five or more columns, then there will always be a subgroup or coset in those five that are a negation of an entire submatrix of B_0. Usually, this subgroup or coset is "good", but if it is not, then we must use an alternative method. I will outline the subgroup or coset we find, depending on how we pick the three columns to negate. In the following, let $x, y, z \in \mathbb{F}_2^3$ be linearly independent. There are three ways to pick three elements.

First, negate $\{0, x, y\}$. Then we let $S = \{z, z+x, z+y, z+x+y\}$. If S is not "good" then we let $S = \{0, x, z, x+z\}$. In either case, S is a subgroup or coset, and at least one must be good. This alternate choice demonstrates another method. We note that two elements are in the negated set and two are not. So we still need an even sign vector and thus we have invariance under equiseparations, as long as exactly two elements are negated and two are not.

Second, negate $\{x, y, z\}$. Then let $S = \{0, x+y, y+z, x+z\}$. If this S is not "good" then let $S = \{0, x, y, x+y\}$. One of these must be "good" so we again have a solution.

Finally, negate $\{x, y, x+y\}$. Then let $S = \{z, z+x, z+y, z+x+y\}$. If this choice of S is not "good" then let $S = \{y, y+x, y+z, y+x+z\}$ which is "good".

So regardless of how we negate three or less or five or more columns, we remain invariant under our equiseparation property. Now consider negatng four columns. If we negate a "good" subgroup or coset then we can just select the other four columns which are also "good". If it is subgroup or coset that is not "good" then we know already that we are negating $\{000, 011, 110, 101\}$ or its coset. We can then pick $S = \{000, 011, 001, 010\}$ which has two elements negated and two remain the same, thus yielding a solution. We now have one final case. If we negate four columns which do not form a subgroup or coset at all. There are two possible ways of doing this.

First, we negate $\{0, x, y, z\}$. Then pick $S = \{0, x, y+z, x+y+z\}$ or $S = \{0, x+y, z, x+y+z\}$. One of these subgroups must be "good" and each have exactly two elements negated.

Finally negate $\{x, y, z, x+y\}$. Then pick $S = \{0, x, z, x+z\}$ or $\{0, y, z, y+z\}$. Again, one of these subgroups must be "good" and each have exactly two elements negated.

Thus, we can start from B_0 and negate any number of columns. Then, since we have either an identical submatrix, a negated submatrix, or a "half-negated" submatrix, with "good" column labels, we can now perform any permutation of the columns to yield any 4×8 boolean matrix with columns which are distinct up to negations. As we saw before, if any pair of columns is equivilant up to negations we already had a solution, so this is sufficient to finish the proof. $\blacksquare$

This proof demonstrates a higher dimensional case with the same method, and also shows how much more complicated the proof becomes. Unfortunately, it seems that the complexity increases quite a bit with the size and quickly becomes unworkable. This leads us into our final formulation.

6 Grassmanians

The following technique may also prove useful in building an inductive proof of our conjecture. To illustrate this technique, we will examine the case where B is a 2×4 matrix. Let

$$X = \begin{pmatrix} a & b & c & d \\ e & f & g & h \end{pmatrix}$$

and let $A = af - be$, $B = ag - ce$, $C = ah - de$, $D = bg - cf$, $E = bh - df$ and $F = ch - dg$ be the determinants of the 2×2 submatrices of X. We want to show that

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \end{pmatrix} \begin{pmatrix} \lambda^1 \\ \lambda^2 \\ \lambda^3 \\ \lambda^4 \end{pmatrix} = 0$$

for λ touching H_{2^2}. We can make the assumption that one of the $\lambda^i = 0$ because in two dimensions, if the convex hull of four points covers the origin, then clearly we are able to take out one of them so that the convex hull of the remaining three still covers the origin. Following, we show that regardless of which $\lambda^i = 0$, the proof still follows:

Proposition 17: For every 2×4 matrix B, $B^\perp$ touches some row of H_{2^2}.

Proof: We can assume that one of $\lambda^i = 0$. Thus we have four cases. First, we assume $\lambda^1 = 0$, which yields $\begin{pmatrix} b & c & d \\ f & g & h \end{pmatrix} \begin{pmatrix} \lambda^2 \\ \lambda^3 \\ \lambda^4 \end{pmatrix} = 0$. Multiplying the second row by f and the first row by b and subtracting the first from the second yields $B\lambda^3 + E\lambda^4 = 0$. Similarly, we can multiply the first row by g and the second row by c and subtract to see $B\lambda^2 - C\lambda^4 = 0$. We now separate this into four more cases, depending on which row of H_{2^2} we want λ to touch. First consider the row $(++++)$. So $\lambda^2, \lambda^3, \lambda^4 \geq 0$. Thus, $BE < 0$ and $BC > 0$. Next consider the row $(+-+-)$. Then we arrive at $BE < 0$ and $BC < 0$. The other two rows yield $BE > 0, BC > 0$ or $BE > 0, BC < 0$ respectively.

We see similar results for setting $\lambda^2 = 0$, $\lambda^3 = 0$ and $\lambda^4 = 0$. For brevity, I will show a chart of the results.

Case	$(++++)$	$(+-+-)$	$(++--)$	$(+--+)$
$\lambda^1 = 0$	$BE < 0$ $BC > 0$	$BE < 0$ $BC < 0$	$BE > 0$ $BC > 0$	$BE > 0$ $BC < 0$
$\lambda^2 = 0$	$DF < 0$ $DC > 0$	$DF < 0$ $DC < 0$	$DF > 0$ $DC < 0$	$DF > 0$ $DC > 0$
$\lambda^3 = 0$	$EF < 0$ $AE > 0$	$EF < 0$ $AE < 0$	$EF > 0$ $AE < 0$	$EF > 0$ $AE > 0$
$\lambda^4 = 0$	$AB > 0$ $BD < 0$	$AB < 0$ $BD < 0$	$AB > 0$ $BD > 0$	$AB < 0$ $BD > 0$

For each case of $\lambda^i = 0$ we see that exactly one of the rows $\mathbf{r} \in H_{2^2}$ must be touched. Thus, we have proven that for every 2×2 matrix B, $B^\perp$ touches some row of H_{2^2}. $\blacksquare$

Now we will consider the implications of this proof and the possibility for generalizing and extending it. First consider the 2×4 matrix we looked at in the proof. The span of the rows of the matrix is a two-dimensional subspace (plane) in four dimensions. When we intersect that with the $z = 1$ hyperplane (or any other that doesn't pass through the origin), we now have a line in three-space, parameterized by eight parameters. Instead, look at the six determinants, $A \ldots F$. We can use these determinants to uniquely express this line in a manner independent of the coordinates or choice of basis for the three-dimensional space containing the line. These six parameters are called the Grassman-Pluecker coordinates of lines in three-space [5].

However, as seen in the previous discussion, in order for a 6-tuple of real numbers $(A \ldots F)$ to represent a line in three-space, they must satisfy $AF + BE + CD = 0$, which is consistent with the fact that lines in three-space have only five free parameters. The sets of points $(A, \ldots, F)$ in $\mathbb{R}^6$ that satisfy the above equation lie on a manifold, which is called a Grassmanian. Thus there is a bijection between points on this Grassmanian and lines in three dimensional projective space, or two dimensional subspaces of four dimensional space. For this reason, this Grassmanian is called $G_{4,2}$.

This idea extends to k dimensional subspaces S of n dimensional Euclidean space, which are represented by the rows of a $k \times n$ matrix. The $k \times k$ determinants of this matrix give a coordinate free representation of S in $\binom{n}{k}$-dimensional space. As in the 2×4

case, a point in $\binom{n}{k}$-dimensional space represents a k-dimensional subspace of R^n only if it satisfies a series of quadratic Grassman-Pluecker relations which define the Grassmanian manifold $G_{n,k}$. By duality, one can view a point on $G_{n,k}$ corresponding to a k dimensional subspace S as also representing the $(n-k)$ dimensional subpace $S^{\perp}$.

In order to show that there is no k dimensional subspace that cuts through all the $n = 2^p$ Hadamard orthants of $\mathbb{R}^n$ (i.e, orthants whose sign vectors are identical to the Hadamard rows), by duality it is sufficient to show that every $(n-k)$ dimensional subspace touches at least one Hadamard orthant. In other words, let us consider the $n = 2^p$ Hadamard regions of $G_{n,k}$ where each region contains exactly those points that correspond to $(n-k)$ dimensional (orthogonal) subspaces that touch a particular Hadamard orthant. Now the goal is to show that these 2^p Hadamard regions entirely cover $G_{n,k}$. It is not hard to see that these regions are connected and closed. The boundary structure of these regions can also be systematically classified. Due to the symmetric structure of the Hadamard orthants to show these Hadamard regions form a cover of $G_{n,k}$, it is sufficient to consider one of these regions, and show that every point on the boundary is either on the boundary or the interior of another Hadamard region.

This type of approach is used in proving the *nonrealizability* of oriented matroids [5], which is a difficult problem in general. An oriented matroid over set of size n specifies a complete set of hyperplane separations or so called Radon partitions of of n points. An oriented matroid is realizable in k dimensions if and only if a point configuration can be found in $\mathbb{R}^k$ realizing all of the given Radon partitions. In our case, our separation matrix (the 2^p Hadamard matrix) specifies only a partial set of Radon partitions. Hence we are trying to prove the nonrealizability of a *partially specified* oriented matroid, which is an even more difficult problem.

However, we can use the sophisticated tools at the junction of combinatorial and algebraic geometry that has been developed for proving nonrealizability of oriented matroids. Moreover, the highly symmetric structure of the Hadamard matrix in Sylvester form (the automorphism group of $\mathbb{Z}_2^n$) appears to make the problem tractable.

7 Conclusion

Propositions 7 and 8 in section 4 show that H_2^p cannot be realized as an equiseparation matrix in p-dimensions and can be realized in $3/4 \times 2^p$ dimensions. Additionally, we have presented a small amount of research on the current Grassmanian approach to the problem as well as a MATLAB experiment verifying our conjecture. The proof of proposition 17 can potentially be extended to the four-by-eight case and beyond. The techniques outlined in this paper are being applied to finding a tighter lower bound on the dimension required for realizing H_{2^p} as an equiseparation matrix.

Conjecture 18: $\forall k$, $\exists N$, such that $\forall n = 2^p$ and $\forall m$, there does not exist an (n, m) equiseparation in dimension $d \leq p^k$. That is, we need dimension $d > \Omega(log^k n) = \Omega(p^k)$.

If successful, we will show that NP-complete problems have super-polynomial complexity when we are restricted to a certain model of computation, namely neural nets. This will aid researchers in solving the classic P vs. NP problem by showing a distinction between the two classes of problems.

References

[1] M. Sitharam ”Approximation from Linear spaces and Complexity Applications” ECCC Report, TR96-030, Univ. of Trier (1996)

[2] P. Enflo and M. Sitharam ”Stable bases and applications to complexity” ECCC Report, TR96-049, Univ. of Trier (1996)

[3] M. Sitharam and T. Straney ”Derandomized Learning of Boolean Functions” Proceedings of Algorithmic Learning Theory (1997), Lecture notes in Artificial Intelligence, Springer-Verlag, (1997), pp. 100-115

[4] C.H. Papadimitriou ”Computational Complexity” Addison Wesley (1994)

[5] A. Björner, M. Las Vergnas, B. Strumfels, N. White, G. Ziegler: ”Oriented Matroids” Encyclopedia of Computation 5-14 Cambridge University Press (1993)

[6] S. S. Agaian: ”Hadamard matrices and their Applications” Lecture notes in mathematics; 1168 (1985)

[7] N. Alon, P. Frankl, V. Rödl ”Geometrical Realization of Set Systems and Probablistic Communication Complexity” Proc. 26th FOCS, Portland, IEEE, 277-280, (1985)