Orthogonal Arrays & Codes
Orthogonal Arrays - Redux

An **orthogonal array of strength** $t$, a $t$-$(v,k,\lambda)$-OA, is a $\lambda v^t \times k$ array of $v$ symbols, such that in any $t$ columns of the array every one of the possible $v^t$ $t$-tuples of symbols occurs in exactly $\lambda$ rows.

We have previously defined an OA of strength 2.

If all the rows of the OA are distinct we call it **simple**.

If the symbol set is a finite field $GF(q)$, the rows of an OA can be viewed as vectors of a vector space $V$ over $GF(q)$. If the rows form a subspace of $V$ the OA is said to be **linear**. [Linear OA's are simple.]
Constructions

**Theorem:** If there exists a Hadamard matrix of order $4m$, then there exists a $2-(2,4m-1,m)$-OA.

**Pf:** Let $H$ be a standardized Hadamard matrix of order $4m$. Remove the first row and take the transpose to obtain a $4m$ by $4m-1$ array, which is a $2-(2,4m-1,m)$-OA.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
<td>b</td>
<td>a</td>
<td>a</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
<td>a</td>
<td>b</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
<td>b</td>
<td>a</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>a</td>
<td>b</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>b</td>
<td>a</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

$2-(2,7,2)$-OA constructed from an order 8 Hadamard matrix
Linear Constructions

**Theorem:** Let $M$ be an $m \times n$ matrix over $\mathbb{F}_q$ with the property that every $t$ columns of $M$ are linearly independent. If $D$ is the $q^m \times n$ matrix whose rows consist of all the linear combinations of rows of $M$, then $(\mathbb{F}_q, D)$ is a linear $t$-$(q,n,\lambda)$-OA where $\lambda = q^{m-t}$.

**Pf:** Choose $t$ columns of $D$, say $c_1, ..., c_t$ and an arbitrary $t$-tuple from $\mathbb{F}_q$, $(y_1, ..., y_t)$.

A row of $D$ is given by $rM$, where $r = (r_1, ..., r_m)$ in $\mathbb{F}_q^m$. Let $C = (c_1, ..., c_t)$ be the $m \times t$ matrix consisting of the columns of $M$ which correspond to the chosen columns of $D$. The linear system $rC = (y_1, ..., y_t)$ has a solution space of dimension $m-t$ since the columns of $C$ are linearly independent. So there are $q^{m-t}$ solutions for $r$. 
Examples

**Corollary**: If $m \geq 2$ and $q$ a prime power, then there exists a $2-(q, (q^m-1)/(q-1), q^{m-2})$-OA.

**Pf**: There are $(q^m-1)/(q-1)$ points in $\text{PG}(m-1,q)$. Homogeneous coordinates of different points, thought of as vectors of length $m$ over $\mathbb{F}_q$, are linearly independent. Take one representative for each point as columns of a matrix $M$ and apply the theorem.

Note: With $m = 2$ we obtain a $2-(q,q+1,1)$-OA constructed from the points of $\text{PG}(1,q)$ [a projective line], but this OA is equivalent to $q-1$ MOLS($q$) which are equivalent to an AG(2,$q$) that uniquely extends to a PG(2,$q$).
Examples

**Corollary:** For a prime power $q$ and any integer $t \geq 2$, there exists a $t$-$(q,q,1)$-OA.

**Pf:** In $\text{PG}(t-1,q)$ the set of $q$ points with homogeneous coordinates $(1,x,x^2,\ldots,x^{t-1})$ for $x$ in $\mathbb{F}_q$ lie on a *normal rational curve*. Form a matrix $M$ with these vectors as coordinates. The submatrix formed by picking any $t$ columns of $M$ is a square Vandermonde matrix with non-zero determinant since no two columns are equal. Thus any set of $t$ columns of $M$ are linearly independent and we can apply the theorem.
Quadratic Constructions

**Theorem:** Let $q$ be an odd prime power and define the functions $f_{a,b} : \mathbb{F}_q \rightarrow \mathbb{F}_q$ by

$$f_{a,b}(x) = (x+a)^2 + b.$$ 

The $q^2 \times q$ array $D$ whose rows are indexed by ordered pairs $(a,b)$ in $\mathbb{F}_q^2$ and columns by elements of $\mathbb{F}_q$ and whose entry in the $(c,d)$ row and $j$ column is $f_{c,d}(j)$ is a $2-(q,q,1)$-OA.

**Pf:** Given two columns $x_1$ and $x_2$ ($x_1 \neq x_2$) and a fixed ordered pair $(y_1,y_2)$, we need to find a unique $(a,b)$ so that

$$(x_1 + a)^2 + b = y_1$$ and $$(x_2 + a)^2 + b = y_2.$$
Quadratic Constructions

**Theorem**: Let $q$ be an odd prime power and define the functions $f_{a,b} : \mathbb{F}_q \rightarrow \mathbb{F}_q$ by

$$f_{a,b}(x) = (x+a)^2 + b.$$ 

The $q^2 \times q$ array $D$ whose rows are indexed by ordered pairs $(a,b)$ in $\mathbb{F}_q^2$ and columns by elements of $\mathbb{F}_q$ and whose entry in the $(c,d)$ row and $j$ column is $f_{c,d}(j)$ is a $2-(q,q,1)$-OA.

**Pf**: By subtracting the two equations:

$$x_1^2 - x_2^2 + 2a(x_1 - x_2) = y_1 - y_2$$

which can then be solved for $a$. The value for $b$ is then uniquely determined.
Gilbert-Varshamov Bound

**Theorem:** For positive integers $m$, $t$ and $n$ with $2 \leq t \leq m$, if

$$\sum_{i=0}^{t-1} \binom{n-1}{i}(q-1)^i < q^m,$$

then there exists a linear $t$-$(q, n, q^{m-t})$-OA.

**Pf:** Let $M_{m,m}$ be the $mxm$ identity matrix. Any $t$ columns of $M_{m,m}$ are linearly independent. Let $M_{m,j}$ be an $m \times j$ matrix with entries from $\mathbb{F}_q$ such that any $t$ columns are linearly independent. The number of linear combinations of at most $t-1$ columns of $M_{m,j}$ is

$$\sum_{i=0}^{t-1} \binom{j}{i}(q-1)^i.$$
Gilbert-Varshamov Bound

**Theorem:** For positive integers m, t and n with \(2 \leq t \leq m\), if

\[
\sum_{i=0}^{t-1} \binom{n-1}{i} (q-1)^i < q^m ,
\]

then there exists a linear t-(q, n, q^{m-t})-OA.

**Pf:** There are \(q^m\) possible column vectors of length m. So there will be a column vector which is not one of these linear combinations only if

\[
\sum_{i=0}^{t-1} \binom{j}{i} (q-1)^i < q^m .
\]

We can use this column to create \(M_{m,j+1}\) which still has the same property. The assumption assures us that we can repeatedly do this for \(j = m, m+1, \ldots, n-1\). The matrix \(M_{m,n}\) can then be used to obtain the desired OA.
Codes

A code is a set of “things” constructed from some alphabet which are transmitted in place of “messages”. The things are called **codewords** and the reason for replacing the messages by codewords is to gain an ability to detect and/or correct errors made in the transmission. We make some assumptions about our code.

First of all we shall restrict our horizons and only consider block codes, so all codewords will have the same length. There are other types of codes, with variable length codewords, which are used in practice, but their underlying theory is quite different from that of the block codes.
Assumptions

Our second assumption is that the symbols used in our codewords will come from a finite alphabet $\Sigma$. Typically, $\Sigma$ will just consist of the integers $\{0,1,\ldots,k-1\}$ when we want our alphabet to have size $k$, but there will be other alphabets used in our work. Note that unless otherwise specified, these numbers are only being used as symbols – they have no arithmetic properties.
A code with codewords of length $n$, based on an alphabet $\Sigma$ of size $k$, is then just a subset of $\Sigma^n = \Sigma \times \Sigma \times \ldots \times \Sigma$, that is the set of $n$-tuples with entries from $\Sigma$. Since the actual alphabet is important (only its size) we will denote this “space” by

$$V(n,k) := \Sigma^n$$

The elements of $V(n,k)$ are called words.
Special Settings

In those situations where we wish to use algebraic properties of the alphabet, we modify the notation by replacing the parameter \( k \) by the name of the algebraic structure we are using. Thus,

\[ V(n, \mathbb{Z}_4) \]

indicates that the \( n \)-tuples are made up from the elements of \( \mathbb{Z}_4 \) and that we can add \( n \)-tuples componentwise using the operations of \( \mathbb{Z}_4 \) (namely, adding mod 4). [Technically, this space is known as a \( \mathbb{Z}_4 \)-module since the alphabet is a ring.]
Settings

The most important setting occurs when the alphabet is a finite field. To indicate this setting we will use the notation $V[n,q]$ implying that the alphabet is the finite field with $q$ elements ($q$ must be a prime or power of a prime). In this case, $V[n,q]$ is a vector space (with scalars from the finite field).

Many of the codes, especially those that have been useful in computer science, have the vector space setting $V[n,2]$. These are often called binary codes since the alphabet is the binary field consisting of only two elements. Codes in $V[n,3]$ are called ternary codes, and, in general, codes in $V[n,q]$ are called $q$-ary codes.
The **Hamming distance** between two words in $V(n,k)$ is the number of places in which they differ.

So, for example, the words $(0,0,1,1,1,0)$ and $(1,0,1,1,0,0)$ would have a Hamming distance of 2, since they differ only in the 1$^{st}$ and 5$^{th}$ positions. In $V(4,4)$, the words $(0,1,2,3)$ and $(1,1,2,2)$ also have distance 2.

This Hamming distance is a **metric** on $V(n,k)$, i.e., if $d(x,y)$ denotes the Hamming distance between words $x$ and $y$, then $d$ satisfies:

1) $d(x,x) = 0$
2) $d(x,y) = d(y,x)$, and
3) $d(x,y) + d(y,z) \geq d(x,z)$. (triangle inequality)
Hamming Distance

The first two of these properties are obvious, but the triangle inequality requires a little argument (this is a homework problem).

Since we will only deal with the Hamming distance (there are other metrics used in Coding Theory), we will generally omit the Hamming modifier and talk about the distance between words.
Minimum Distance

The *minimum distance* of a code $C$ is the smallest distance between any pair of distinct codewords in $C$. It is the minimum distance of a code that measures a code's error correcting capabilities. If the minimum distance of a code $C$ is $2e + 1$, then $C$ is a $2e$-error detecting code since $2e$ or fewer errors in a codeword will not get to another codeword and is an $e$-error correcting code, since if $e$ or fewer errors are made in a codeword, the resulting word is closer to the original codeword than it is to any other codeword and so can be correctly decoded (*maximum-likelihood decoding*).

In the 5-repeat code of $V(5,4)$ ([codewords: 00000, 11111, 22222, and 33333]) the minimum distance is 5. The code detects 4 or fewer errors and corrects 2 or fewer errors.
Weight of a Word

We always assume that 0 is one of the symbols in our alphabet.

The weight of a word is the number of non-zero components in the word. Alternatively, the weight is the distance of the word from the zero word.

In \( V(6,6) \) the word \((0,1,3,0,1,5)\) has weight 4.

When we are working with an alphabet in which one can add and subtract then there is a relationship between distance and weight,

\[ d(x,y) = wt(x - y), \]

since whenever a component of \( x \) and \( y \) differ, the corresponding component of \( x - y \) will not be 0.
Let $C$ be a $q$-ary code in $V(n,k)$. If $C$ has $M$ codewords and minimum distance $d$, we sometimes refer to it as an $(n,M,d,q)$-code.

For fixed $n$, the parameters $M$ and $d$ work against one another - the bigger $M$, the smaller $d$ and vice versa. This is unfortunate since for practical reasons we desire a large number of codewords with high error correcting capability (large $M$ and large $d$). The search for “good” codes always involves some compromise between these parameters.
Linear Codes

In the V[n,q] setting (which is a vector space) a code is just a subset of vectors. However, we can obtain “better” (meaning more easily analyzed) codes if they form a subspace of the vector space. These codes are called **linear codes** and form a well studied class of codes.

Note that for linear codes we have the property that the minimum distance between distinct code words is the same as the minimum weight of a non-zero code word.
Codes and Orthogonal Arrays

**Theorem:** Let $C \subseteq (F_q)^n$ be a linear code of dimension $m$. $(F_q, C)$ is an $(n, q^m, d, q)$-code if and only if $C^\perp$ is a (linear) $(d-1)-(q, n, \lambda)$-OA where $\lambda = q^{n-m-d+1}$.

**Proof:** If $C$ is a linear $(n, q^m, d, q)$-code, then $C^\perp$ is a s/space of dimension $n - m$. Let $D$ be a basis for this s/space and write the vectors of $D$ as an $n-m \times m$ matrix. Suppose that there are $e \leq d-1$ linearly dependent columns of $D$. WLOG we may assume that these are the first $e$ columns, $c_1, \ldots, c_e$ and we have:

$$\sum_{i=1}^{e} \alpha_i c_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$ 

Define $x = (\alpha_1, \ldots, \alpha_e, 0, \ldots, 0)$, and since $x \cdot r = 0$ for each row of $D$, we have $x$ in $C \rightarrow\leftarrow$ since $wt(x) < d$. 

Theorem: Let $C \subseteq (F_q)^n$ be a linear code of dimension $m$. $(F_q, C)$ is an $(n, q^m, d, q)$-code if and only if $C^\perp$ is a (linear) $(d-1)-(q, n, \lambda)$-OA where $\lambda = q^{n-m-d+1}$.

Proof: (cont) Now suppose that $C^\perp$ is a linear $(d-1)-(q, n, \lambda)$-OA where $\lambda = q^{n-m-d+1}$. This implies that $C^\perp$ has dimension $n-m$ and so $C$ has dimension $m$. [The OA has $\lambda q^{d-1} = q^{n-m}$ rows.]

Suppose that $C$ does not have minimum distance $d$. Then there exists a vector $x$ with $0 < \text{wt}(x) \leq d-1$. WLOG suppose that the nonzero entries of $x$ occur in the first $e$ coordinates with $e = \text{wt}(x)$. Now since $x \in C$, $x \cdot y = 0$ for every row $y$ of $C^\perp$ which implies that the first $e$ columns of $C^\perp$ are linearly dependent which contradicts the fact that $C^\perp$ has strength $d-1$. 
Singleton Bound

**Theorem:** If $C$ is an $(n,M,d,q)$-code, then $M \leq q^{n-d+1}$.

**Proof:** Suppose $M > q^{n-d+1}$. Consider the first $n-d+1$ coordinates of the code words. There are only $q^{n-d+1}$ distinct vectors of length $n-d+1$, so by the Pigeon-Hole Principle, there are at least two code words, $x$ and $y$ which are identical in the first $n-d+1$ positions. The distance between these vectors, $d(x,y) \leq n - (n-d+1) = d - 1$, contradicting the minimum distance of the code.

A code which achieves the Singleton Bound is called a **Maximum Distance Separable (MDS)** code.
MDS Codes

**Theorem**: An MDS code is equivalent to a $(n-d+1)-(q,n,1)$-OA.

Proof: Suppose that $D$ is a $t-(q,n,1)$-OA. Construct a code $C$ by taking the $q^t$ rows of $D$ as codewords. If $d(C) \leq n-t$ then there exist code words $x$ and $y$ which agree in at least $t$ columns. Within $t$ of these columns the rows of $x$ and $y$ are the same, contradicting $\lambda = 1$. Apply this when $t = n-d+1$ to get an MDS $(n,M,d,q)$-code.

Conversely, assume $C$ is an MDS code. Construct array $D$ by using the codewords of $C$ as rows. $D$ is an $M \times n$ array. Restrict $D$ to any $n-d+1$ of its columns. The $q^{n-d+1}$ $(n-d+1)$-tuples which are the rows of this restriction are all different (else two code words would be closer than $d$ apart), so each appears exactly once.
Example

A previous corollary produced \(t-(q,q,1)-\text{OA's}\) from normal rational curves when \(t \geq 2\) and \(q\) a prime power. We can now combine these with the previous result to obtain:

**Corollary:** If \(t \geq 2\) and \(q\) a prime power then there exists an MDS \((q, q^t, q-t+1, q)\)-code.

The codes obtained from this corollary are known as **Reed-Solomon codes**.

A very recent result due to Simeon Ball shows that if \(q\) is a prime (not a power of a prime) then all MDS codes come from this example using normal rational curves.
Covering Radius

Since $V(n,k)$ has a metric defined on it, it makes sense to talk about spheres centered at a word with a given radius. Thus,

$$S_r(x) = \{ y \in V(n,k) \mid d(x,y) \leq r \}$$

is the sphere of radius $r$ centered at $x$.

The covering radius of a code $C$ is the smallest radius $s$ so that

$$V(n,k) \subseteq \bigcup_{x \in C} S_s(x)$$
i.e., every word of the space is contained in some (at least one) sphere of radius $s$ centered at a codeword.
Packing Radius

The **packing radius** of a code $C$ is the largest radius $t$ so that the spheres of radius $t$ centered at the code words are disjoint.

$$S_t(x) \cap S_t(y) = \emptyset \quad \forall x \neq y \in C$$

Clearly, $t \leq s$. When $t = s$, we say that $C$ is a *perfect code*. While perfect codes are very efficient codes, they are very rare – most codes are not perfect.
Covering and Packing

Covering Radius

Packing Radius
Example

Consider the 5-repeat code in V(5,3). There are just 3 codewords, 00000, 11111, and 22222. A word such as 01221 is at distance 4 from 00000, and distance 3 from both 11111 and 22222. The distance of a word x from a code word is just $5 - (\# \text{ symbols in common with the codeword})$. Since there are just 3 symbols and 5 positions, every word must have at least one repeated symbol, and so distance at most 3 from some codeword. Spheres of radius 3 around the codewords will therefore contain all of V(5,3). This means that $s \leq 3$. The example of 01221 shows that if $s = 2$ this word would not be contained in any sphere, thus the covering radius $s = 3$. This same example shows that spheres of radius 3 are not disjoint, so $t < 3$. Two spheres of radius 2 must be disjoint, since a word in both would have 3 symbols in common with both codewords $\rightarrow \leftarrow$. So, the packing radius $t = 2$. 
Sphere Packing Bound

We can count the number of words in a sphere of radius $e$ in $V(n,q)$ and obtain:

$$|S_e(x)| = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$ 

To count the number of words at distance $i$ from the word $x$, we first select which $i$ positions will be different and then in each of these positions we select an element of the alphabet different from the one in that position in $x$ (there are $q-1$ choices per position).

If $C$ is an $(n,M,d,q)$-code in $V(n,q)$ and the spheres of radius $e$ centered at the codewords are disjoint, we obtain the sphere packing bound – since $V(n,q)$ contains $q^n$ words:

$$M \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n$$
Hamming Codes

A code which meets the sphere packing bound is called a perfect code. There are very few perfect codes, but there is an infinite family of perfect codes with distance 3 called the Hamming codes.

**Theorem:** Let $s \geq 2$ be an integer and $q$ a prime power. Then there is a Hamming $(n, q^m, 3, q)$-code in which $n = (q^s - 1)/(q-1)$ and $m = n - s$.

**Pf:** We have constructed a linear 2-$(q, (q^s - 1)/(q-1), q^s - 2)$-OA from a PG$(s-1, q)$. Consider the code $C$ which is the orthogonal complement of this OA. $C$ has distance 3, and we have $q^m = q^n/(\lambda q^2) = q^{n-s}$. 
Hamming Codes

**Theorem**: Let $s \geq 2$ be an integer and $q$ a prime power. Then there is a Hamming $(n,q^m,3,q)$-code in which $n = (q^s-1)/(q-1)$ and $m = n - s$.

**Pf**: To show that this code is perfect we calculate:

$$
\sum_{i=0}^{1} \binom{n}{i} (q-1)^i = 1 + n(q-1) = q^s,
$$

so,

$$
q^m \sum_{i=0}^{1} \binom{n}{i} (q-1)^i = q^{m+s} = q^n.
$$
Shortened Codes

There are several ways to construct new codes from old ones and we shall look at some of these.

Shortening a Code

If $C$ is an $(n,M,d,q)$-code then define

$$C_x = \{(y_1,\ldots,y_n) \mid y_1 = x\}$$

and

$$\text{short}(C,x) = \{(y_2,\ldots,y_n) \mid (y_1,\ldots,y_n) \in C_x\}.$$  

**Theorem:** There is an $x$ so that $\text{short}(C,x)$ is an $(n-1,M',d,q)$-code with $M' \geq M/q$.

**Proof:** $\text{short}(C,x)$ is an $(n-1, |C_x|, d, q)$-code. There are $q$ sets $C_x$ which are disjoint and partition the code. The average size of a $C_x$ is $M/q$, so there must be a $z$ with $C_z$ of size at least this big.
Pasting Codes Together

**Theorem:** If there is an \((n_1,M_1,d_1,q)\)-code \(C\) and an \((n_2,M_2,d_2,q)\)-code \(D\) with \(M_1 \leq M_2\), then for any positive integers \(u\) and \(v\) there exists a \((un_1+vn_2, M_1, ud_1+vd_2,q)\)-code.

**Proof:** List the elements of \(C\) as \(x_1,x_2,\ldots,x_{M_1}\) and the elements of \(D\) as \(y_1,y_2,\ldots,y_{M_2}\). For each \(i\) with \(1 \leq i \leq M_1\), concatenate \(u\) copies of \(x_i\) and \(v\) copies of \(y_i\) to get codewords of length \(un_1+vn_2\). If we arrange the lists so that \(d(x_1,x_2) = d_1\) and \(d(y_1,y_2) = d_2\), then the minimum distance in the new code will be \(ud_1+vd_2\).
Theorem [(u, u+v)-construction]: Let $C_i$ be an $[n,M_i,d_i,2]$-code for $i = 1,2$. Then the code $C$ defined by,
$$C = \{(u, u+v): u \in C_1, v \in C_2\}$$
is a $[2n, M_1M_2, \min(2d_1, d_2),2]$ code.

*Pf:* It is clear that $C$ is a $[2n, M, d, 2]$ code for some $M$ and $d$, which we now determine.

Consider the map from $C_1 \times C_2 \rightarrow C$ given by $(c_1, c_2) \rightarrow (c_1, c_1 + c_2)$. This is easily seen to be a bijection, so the size of $C$ is the same as that of $C_1 \times C_2$, which is $M_1M_2$. 
Theorem [(u, u+v)-construction]: Let $C_i$ be an $[n,M_i,d_i,2]$- code for $i = 1,2$. Then the code $C$ defined by, $C = \{(u, u+v): u \in C_1, v \in C_2\}$ is a $[2n, M_1M_2, \min(2d_1, d_2),2]$ code.

$Pf$ (cont): Consider a non-zero code word $(c_1, c_1+c_2)$ of $C$. If $c_2 = 0$ then $c_1 \neq 0$ and
\[ \text{wt}((c_1, c_1+c_2)) = \text{wt}((c_1, c_1)) = 2 \text{ wt}(c_1) \geq 2d_1 \geq \min(2d_1, d_2). \]
On the other hand, if $c_2 \neq 0$, then
\[ \text{wt}((c_1, c_1+c_2)) = \text{wt}(c_1) + \text{wt}(c_1+c_2) \geq \text{wt}(c_1) + (\text{wt}(c_2) - \text{wt}(c_1)) \]
\[ \geq \text{wt}(c_2) \geq \min(2d_1,d_2). \text{ Thus, } d \geq \min(2d_1,d_2). \]

If $x \in C_1$ has wt $d_1$, and $y \in C_2$ has wt $d_2$, then
\[ (x,x) \in C \text{ has wt } 2d_1 \text{ and } (0,y) \in C \text{ has wt } d_2 \]
so, $d \leq \min(2d_1, d_2)$, and so we have equality.
Plotkin Bound

**Theorem:** If $C$ is an $(n, M, d, 2)$-code with $d > \frac{1}{2}n$, then

$$M \leq \frac{2d}{2d-n}.$$  

Proof: Let the codewords of $C$ be denoted by $x_i$, $1 \leq i \leq M$. Let $S$ denote the sum of all distances between ordered elements of $C$, that is:

$$S = \sum_{i=1}^{M} \sum_{j=1}^{M} d(x_i, x_j).$$

Of the $M^2$ terms, $M(M-1)$ are at least $d$ and $M$ are 0, so $S \geq M(M-1)d$.

Now consider any of the $n$ coordinate positions. For any two code words, there is a contribution of 2 to $S$ iff the code words differ in this position. If $t_p$ is the number of 1's in position $p$, then $2t_p(M-t_p)$ is the contribution from this position.
Plotkin Bound

**Theorem:** If $C$ is an $(n,M,d,2)$-code with $d > \frac{1}{2}n$, then

$$M \leq \frac{2d}{2d-n}.$$ 

**Proof (cont):** Summing over the $n$ positions gives:

$$S = \sum_{p=1}^{n} 2t_p\left(M - t_p\right).$$

If $t_p$ were a real variable, the largest value of $S$ would be obtained when $t_p = M/2$ and we get that $S \leq \frac{1}{2}nM^2$.

Combining with the earlier inequality gives

$$M(M-1)d \leq \frac{1}{2}nM^2 \rightarrow M(2d-n) \leq 2d.$$ 

Since $2d > n$, we obtain:

$$M \leq \frac{2d}{2d-n}.$$
Hadamard Codes

A code which meets the Plotkin bound is known as an Hadamard code.

**Lemma:** If there is an Hadamard matrix of order $n$ then there exists an $(n-1,n,\frac{1}{2}n,2)$-code and an $(n-2,\frac{1}{2}n,\frac{1}{2}n,2)$-code.

**Proof:** Take an Hadamard matrix of order $n$, standardize it and remove the first column. By taking the rows as codewords we have an $(n-1,n,\frac{1}{2}n,2)$-code. Now shorten this code to obtain an $(n-2,\frac{1}{2}n,\frac{1}{2}n,2)$-code.
Levenshtein's Theorem

**Theorem**: Suppose that \(n\) and \(d\) are even positive integers such that \(2d > n\). Define

\[ k = \left\lfloor \frac{d}{2d - n} \right\rfloor, \]

and suppose that Hadamard matrices of order \(4k\) and \(4k+4\) exist, then there exists an \((n, 2k, d, 2)\)-Hadamard code.

**Proof**: Define

\[ u = \frac{1}{2}[d(2k+1) - n(k+1)] \text{ and } v = \frac{1}{2}[nk - d(2k-1)]. \]

Now \(u\) and \(v\) are integers since \(n\) and \(d\) are even. From the definition of \(k\) we have that:

\[ \frac{d}{2d - n} - 1 < k \leq \frac{d}{2d - n}. \]
Levenshtein's Theorem

**Theorem:** Suppose that $n$ and $d$ are even positive integers such that $2d > n$. Define

$$k = \left\lfloor \frac{d}{2d-n} \right\rfloor,$$

and suppose that Hadamard matrices of order $4k$ and $4k+4$ exist, then there exists an $(n,2k,d,2)$- Hadamard code.

**Proof:** Now $u > 0$ if and only if $d(2k+1) - n(k+1) > 0$, but

$$d(2k+1) - n(k+1) = k(2d-n) + d - n > \left( \frac{d}{2d-n} - 1 \right) (2d-n) + d - n = d - (2d-n) + d - n = 0;$$

Also, $v \geq 0$ if and only if $nk - d(2k-1) \geq 0$, and we have

$$nk - d(2k-1) = d - k(2d-n) \geq d - \left( \frac{d}{2d-n} \right) (2d-n) = d - d = 0.$$
Levenshtein's Theorem

**Theorem:** Suppose that $n$ and $d$ are even positive integers such that $2d > n$. Define

$$k = \left\lfloor \frac{d}{2d-n} \right\rfloor,$$

and suppose that Hadamard matrices of order $4k$ and $4k+4$ exist, then there exists an $(n,2k,d,2)$-Hadamard code.

**Proof (cont):** Let $C$ be a $(4k-2,2k,2k,2)$-code and $D$ a $(4k+2,2k+2,2k+2,2)$-code constructed from Hadamard matrices of orders $4k$ and $4k+4$ respectively as in the last lemma. Paste $u$ copies of $C$ and $v$ copies of $D$ together to get a $(u(4k-2)+v(4k+2), 2k, u(2k) + v(2k+2), 2)$-code. However, $u(4k-2)+v(4k+2) = \frac{1}{2}[d(2k+1) - n(k+1)](4k-2) + \frac{1}{2}[nk - d(2k-1)](4k+2) = n$, and $u(2k) + v(2k+2) = \frac{1}{2}[d(2k+1) - n(k+1)](2k) + \frac{1}{2}[nk - d(2k-1)](2k+2) = d$.\[\]