Nonlinear Codes, T-designs and Perfect Codes

Piyush Agarwal

27th October 2021

This report is written as part of the seminar in the course Coding Theory (MA5105) taken over the autumn semester 2021. Prof. Sudhir Ghorpade was the course instructor.
The motivation of this study was to explore non-linear codes and their relation with perfect codes.

1 Hadamard Codes

1.1 Plotkin Bound

For a (n, M, d) code $\mathscr{C}$ over $\mathbb{F}_2$ for which $n < 2d$ we have:

$$M \leq 2\Big\lfloor \frac{d}{2d-n} \Big\rfloor$$

Let $A(n,d) = max\{|C| : C-(n,d)code\}$ then we have:

$$A(n,d) \leq 2A(n-1,d)$$

Proof for the above statement:

Let C be s.t. $|C| = A(n,d)$. Each codeword $c \in C$ begins with a 0 or 1. Then $C = C_1 \cup C_2$ where $C_1 = \{c = (c_1,..,c_n) \in C | c_1 = 0\}$ and $C_2 = \{c = (c_1,,..,c_n) \in C | c_1 = 1\}$. Note that C_1, C_2 are $(n-1,d)$ codes. Hence, we have $A(n,d) = |C_1| + |C_2| \leq 2A(n-1,d)$

Then we have for $A(2d,d) \leq 2A(2d-1,d) \leq 4d$
Note that the second ineq. is via Plotkin bound

We'll also see that if Hadamard matrices of all possible orders exist, codes can be constructed which achieve equality (showing that the bound is tight).

1.2 Hadamard Matrices

A Hadamard matrix H of order n is a $n \times n$ matrix with all entries 1 or -1 s.t. $HH^T = nI$

For example $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

Necessary Condition for existence of Hadamard Matrices: Hadamard matrix of order $n \geq 3$ exists only if n is divisible by 4.

Proof: Let H be a Hadamard matrix of order n. Any permutation of columns of H is also a Hadamard Matrix. Also, H can be normalized by multiplying by -1 to each column so that first row is $[1, 1, .., 1]$ Now, first three rows of H can be considered as:

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
1 1 1 1..-1-1-1-1.. 1 1 1 1..-1-1-1-1

Let size of batches be n_1, n_2, n_3, n_4. By using orthogonality of rows we have:
$n_1 + n_2 - n_3 - n_4 = 0$
$n_1 - n_2 + n_3 - n_4 = 0$
$n_1 - n_2 - n_3 + n_4 = 0$
This gives $n_1 = n_2 = n_3 = n_4$

1.3 Construction of Hadamard Matrices

There are two common construction of Hadamard Matrices:

Let H_n be a Hadamard matrix of order n then $H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$

Checking $\begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \begin{bmatrix} H_n^T & H_n^T \\ H_n^T & -H_n^T \end{bmatrix} = \begin{bmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{bmatrix}$

These are Sylvester Matrices.
The second construction is known as Paley Construction and uses the Legendre Symbol.
Let p be a prime and χ denote the Legendre Symbol. Then

- $\chi(i) = 0$ if $i \equiv 0 \pmod{p}$
- $\chi(i) = 1$ if a (s.t. $i \equiv a \pmod{p}$) is a square in $\mathbb{F}_p$
- $\chi(i) = -1$ if a (s.t. $i \equiv a \pmod{p}$) is not a square in $\mathbb{F}_p$

Paley Construction gives Hadamard Matrices of order $n = p+1, p$ is a prime.

On Route to Hadamard Matrix, we construct the Jacobsthal matrix $Q = [q_{ij}]$ where $q_{ij} = \chi(j-i)$. Note that Q is a skew symmetric matrix as -1 is not a quadratic residue for $p = 4k-1$, $q_{ji} = \chi(i-j) = \chi(-1)\chi(j-i) = -q_{ij}$

Now $QQ^T = pI - J$ and $QJ = JQ = 0$ where J is the all 1s $p \times p$ matrix. $QQ^T = [\bar{q}_{ij}] = \sum_k q_{ik}q_{jk} \quad \bar{q}_{ii} = \sum_k q_{ik}^2 = \sum_k \chi^2(k-i) = p-1$

for $i \neq j$, $\bar{q}_{ij} = \sum_k q_{ik}q_{jk} = \sum_k \chi(k-i)\chi(k-i+i-j) = \sum_b \chi(b)\chi(b+c) = -1$

Showing $\sum_b \chi(b)\chi(b+c) = -1$ Claim: When $b \neq 0$ $\exists! z \in \mathbb{F}_p$ such that $b+c \equiv bz$ (mod p). Since $b \in \mathbb{F}_p$, $gcd(b,p) = 1$, so $\exists\, x, y \in \mathbb{Z}$ such that $xb + yp = 1$. Then $(xc+x+1)b + (y+yc)p = b+c$ and so $(xc+x+1)b \equiv b+c$ (mod p). Hence existence is guaranteed. We also show uniqueness, if $b_1 + c \equiv b_1 z$(mod p) and $b_2 + c \equiv b_2 z$(mod p) for some fixed $z \in \mathbb{F}_p/\{1\}$ then $b_1 = b_2$ (mod p). Hence $\sum_b \chi(b)\chi(b+c) = \sum_{z,z\neq 1} \chi(b)\chi(bz) = \sum_{z,z\neq 1} \chi(z) = -1$

Also $\sum_i q_{ij} = \sum_i \chi(j-i) = 0\ \forall j \in [p] = \{1,2,..,p\}$ Similarly $\sum_j q_{ij} = \sum_j \chi(j-i) = 0\ \forall i \in [p] = \{1,2,..,p\}$
Hence, $QJ = JQ = 0$

Claim: $H = \begin{bmatrix} 1 & \bar{1} \\ \bar{1}^T & Q-I \end{bmatrix}$ where ($\bar{1}$ is an all $1s$ p-dim. row vector) is a Hadamard matrix of order $n = p+1$
Consider $HH^T = \begin{bmatrix} 1 & \bar{1} \\ \bar{1}^T & Q-I \end{bmatrix}\begin{bmatrix} 1 & \bar{1} \\ \bar{1}^T & Q^T-I \end{bmatrix} = \begin{bmatrix} p+1 & 0 \\ 0 & J+(Q-I)(Q^T-I) \end{bmatrix}$
$= \begin{bmatrix} p+1 & 0 \\ 0 & (p+1)I_p \end{bmatrix} = nI_n$

Hence, H is a Hadamard matrix of order n.

$$Q_7 = \begin{bmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{bmatrix} \quad H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}$$

1.4 Hadamard Codes

Let H_n be a normalized Hadamard matrix. Then by replacing 1's with 0's and -1 with 1's , we get the *binary* Hadamard matrix, A_n. Now A_n gives rise to three different types of codes:

i) $\mathscr{A}_n$: $(n-1, n, n/2)$ code obtained by removing the first column from A_n.

$$A_8 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Note that if $n = 2^r$, $\mathscr{A}_n$ is nothing but the simplex code discussed in class.
Also for $\mathscr{A}_n$, $d = n/2$ because in H_n rows are orthogonal to each other and any row matches in exactly half of the elements with the other rows.
So $d(c_1, c_2) = n/2 \quad \forall c_1, c_2 \in \mathscr{A}_n \& c_1 \neq c_2$

ii) $\mathscr{B}_n$: $(n-1, 2n, n/2-1)$ consists of $\mathscr{A}_n$ and complements of codewords in $\mathscr{A}_n$
Proof for $d = n/2 - 1$:
$\mathscr{B}_n = \{\bar{0}\} \cup \mathscr{A}_n/\{\bar{0}\} \cup$ Comp($\mathscr{A}_n/\{\bar{0}\}$) $\cup \{\bar{1}\}$, $\bar{0}, \bar{1}$ denote n-1 dimensional vectors. for any $c_1, c_2 \in \mathscr{A}_n/\{0\} \cup$ Comp($\mathscr{A}_n/\{0\}$) , $d(c_1, c_2) = n/2$
But $\forall c \in \mathscr{A}_n/\{0\} \cup$ Comp($\mathscr{A}_n/\{0\}$), $d(c, \bar{1}) = n - 1 - n/2 = n/2 - 1$
Hence $d(\mathscr{B}_n) = n/2 - 1$

iii)$\mathscr{C}_n$: $(n, 2n, n/2)$ consists of all rows of A_n and its complements, Note that showing $d(\mathscr{C}_n) = n/2$ is rather easy.

1.5 Levenshtein's Theorem

Two basic constructions required for Levenshtein's Theorem
Codewords in $\mathscr{A}_n$ which begin with 0 form a $(n-2, n/2, n/2)\mathscr{A}'_n$ code. Note that each column in A_n has $n/2$ 1's and 0's

Let C_1 be a (n_1, M_1, d_1) code and C_2 be a (n_2, M_2, d_2) code, paste a copies of C_1 and b copies of C_2 side by side, deleting additional rows of either C_1 or C_2. Note that if $M_1 > M_2$, last $M_1 - M_2$ rows of C_1 are deleted. Then the resulting code is a $(an_1 + bn_2, min(M_1, M_2), d \geq ad_1 + bd_2)$ code

Levenshtein's Theorem
Provided Hadamard Matrices exist, equality holds for the Plotkin Bound. So if d is even, $A(n, d) = 2\left\lfloor \frac{d}{2d-n} \right\rfloor$ and $A(2d, d) = 4d$

$\mathscr{C}_{2d}$ is a $(2d, 4d, d)$ code and hence satisfies, $A(2d, d) = 4d$
For $A(n, d) = 2\lfloor \frac{d}{2d-n} \rfloor$, a $(n, 2\lfloor \frac{d}{2d-n} \rfloor, d)$ code shall be constructed.

Let $k = \lfloor \frac{d}{2d-n} \rfloor$ and define $a = d(2k+1) - n(k+1) \quad ; b = kn - d(2k-1)$
Then $a = k(2d-n) - (n-d) \geq ((d/(2d-n)) - 1)(2d-n) - (n-d) \geq 0$
Also $b = kn - d(2k-1) \geq d - k(2d-n) \geq 0$
Now, if n is even, a and b both are even. if n is odd and k odd then a is even and if k even then b even. So, the following codes satisfy the first equality

if n even, $\mathscr{C} = \frac{a}{2}\mathscr{A}'_{4k} \bigoplus \frac{b}{2}\mathscr{A}'_{4k+4}$
Length $n' = \frac{a}{2}(4k-2) + \frac{b}{2}(4k+2) = k(2k+1)n - (k+1)(2k-1)n = n$
Distance: $d' \geq \frac{a}{2}2k + \frac{b}{2}(2k+2) = ak + b(k+1) = d(2k+1)k - d(2k-1)(k+1) = d$
No. of Codewords $M' = min(2k, 2k+2) = 2k = 2\lfloor \frac{d}{2d-n} \rfloor$

if k odd, $\mathscr{C} = \frac{a}{2}\mathscr{A}'_{4k} \bigoplus b\mathscr{A}_{2k+2}$
$n' = a(2k-1) + (2k+1)b = n$, $d' \geq ak + b(k+1) = d$ and $M' = 2k$

if k even, $\mathscr{C} = a\mathscr{A}_{2k} \bigoplus \frac{b}{2}\mathscr{A}'_{4k+4}$
$n' = a(2k-1) + (2k+1)b = n$, $d' \geq ak + b(k+1) = d$ and $M' = 2k$

2 T-Designs

2.1 Introduction

Definition: Let X be a v set (a set with v elements). A t-design is a collection of distinct k-subsets of X (called blocks) such that any t-subset of X occurs exactly in λ blocks. This is called a $t-(v,k,\lambda)$ design.

Examples: The set X is itself a $|X| - (|X|, |X|, 1)$ design (Trivial)
Consider 3 points in a plane forming a triangle. Seeing the line as blocks, we have a $2-(3,2,1)$ design.
Consider a set of 7 people $\{A,B,C,D,E,F,G\}$ from which 3-member committees are made. Suppose the committees are: $\{ABD, BCE, CDF, DEG, AEF, BFG, ACG\}$. Then any particular pair is in exactly 1 committee. This forms a $2-(7,3,1)$ design.

Definition: A t-design with $\lambda = 1$ is called a Steiner System and a $t-(v,k,1)$ design is denoted as $S(t,k,v)$. The above example is a $S(2,3,7)$

Theorem In a $t-(v,k,\lambda)$ design, let $A = \{P_1, P_2, .., P_t\}$ be a set of distinct points. Let λ_i be the number of distinct blocks containing A. Then λ_i is independent of the choice of points and in fact $\lambda_i = \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}} \quad 0 \leq i \leq t$
Proof is via a summation argument. Let $C = \{(S,j) \mid S$: set of t points s.t.

$A \subseteq S$, j : index of block containing S} Then

$$|C| = \sum_{|S|=t} \sum_{\substack{j \\ A \subseteq B_j}} 1 = \sum_{\substack{|S|=t \\ A \subseteq S}} \lambda = \lambda \binom{v-i}{t-i} = \sum_{\substack{j \\ A \subseteq B_j}} \binom{k-i}{t-i} = \lambda_i \binom{k-i}{t-i}$$

Hence, we have the result.
Substituting $i = 0$ above gives the total number of blocks $b = \frac{\lambda \binom{v}{t}}{\binom{k}{t}}$ and each point belongs to exactly λ_1 blocks where $bk = v\lambda_1$ (using b)

Definition In a $t-(v,k,\lambda)$ design, let $P_1, P_2, .., P_k$ be points belonging to one of the blocks. Consider the blocks which contain $P_1, P_2, .., P_j$ but not $P_{j+1}, .., P_i$ for $0 \leq j \leq i$(For $j = 0$ consider the blocks not containing $P_1, .., P_i$ and for $j = i$ consider the blocks containing $P_1, .., P_i$). If the number of such blocks is a constant and independent of the choice of points, we call it by λ_{ij}. λ_{ij} are called the block intersection numbers.

Theorem If $i \leq t$, λ_{ij} are well defined and we have $\lambda_{ij} = \lambda_j - \lambda_{i-j}$, so $\lambda_{ii} = \lambda_i$. Also λ_{ij} satisfy the Pascal Property

$$\lambda_{ij} = \lambda_{i+1,j} + \lambda_{i+1,j+1}$$

whenever they are defined. If the design is a Steiner System, we have $\lambda_{tt} = \lambda_{t+1,t+1} = .. = \lambda_{kk} = 1$ and so λ_{ij} are well defined for Steiner Systems.
Proof Let λ_{ij} be the number of blocks containing $P_1, .., P_j$ and not containing $P_{j+2}, .., P_{i+1}$. Then the blocks can be divided such that they either contain, P_{j+1} which is $\lambda_{i+1,j+1}$ number of blocks or not containing which is $\lambda_{i+1,j}$. Hence, $\lambda_{ij} = \lambda_{i+1,j+1} + \lambda_{i+1,j}$

Corollary: Given a $t-(v,k,\lambda)$ design, block intersection numbers λ_{ij}, one can construct other designs.

Suppose a point P_1 is omitted from all the blocks $\mathscr{B}$, then this results in two types of blocks, $\mathscr{B}_1$: λ_{10} number of blocks with k elements (those boxes which did not contain P_1) and
$\mathscr{B}_2$: λ_{11} number of blocks with $k-1$ elements (those boxes which contained P_1).

Theorem Blocks $\mathscr{B}_1$ form a $(t-1)-(v-1,k,\lambda_{t,t-1})$ with block intersection numbers. $\lambda'_{ij} = \lambda_{i+1,j}$. The blocks $\mathscr{B}_2$ form a $(t-1)-(v-1,k-1,\lambda)$ with block intersection numbers $\lambda'_{ij} = \lambda_{i+1,j+1}$.

Proof For $\mathscr{B}_1$ if take $(t-1)$ elements, and append P_1 to get a t element set. Then we have exactly $\lambda_{t,t-1}$ blocks which contain the $(t-1)$ elements and not P_1. They are all contained in $\mathscr{B}_1$. Similarly, consider i points $P_{k_1}, P_{j_2}, .., P_{k_i}$ and append P_1 to it. Then $\lambda'_{ij} = \lambda_{i+1,j}$. For $\mathscr{B}_2$, consider any $t-1$ set of points

and append P_1 to that set. Then the t set will occur in exactly λ blocks.

Corollary If a Steiner System $S(t,k,v)$ exists, so does a $S(t-1,k-1,v-1)$.

Given a $t-(v,k,\lambda)$ design with v points $P_1,P_2,..,P_v$ and b blocks $B_1,.,B_b$ its $b\times v$ incidence matrix A is defined as $a_{ij}=1$ if $P_j\in B_i$ 0 otherwise.
The incidence matrix helps to see relation between codes and designs clearly.

2.2 Codes and Designs

A for the 3rd example:

$$\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\1&0&1&0&0&0&1\end{bmatrix}$$

Note that each of the rows can be considered as codewords of a code C. Hence, every Steiner system forms a Non-linear code with parameters $(n=v,M=b,d\geq 2(k-t+1)$
Each codeword has a fixed weight k and any two codewords can have at most $(t-1)$ overlapping $1'$s and Hence $d\geq 2(k-(t-1))$

Conversely, given a code (n,M,d) one can also construct designs out of the constant weight codewords.

Theorem Let $\mathscr{H}_m$ be the Hamming code of order m and $\hat{\mathscr{H}_m}$ be the extended Hamming code,(obtained by adding a parity check to $\mathscr{H}_m$). Then the codewords of weight 3 in $\mathscr{H}_m$ form a Steiner System $S(2,3,2^m-1)$. The codewords of weight 4 in $\hat{\mathscr{H}_m}$ form a Steiner System $S(3,4,2^m)$.
The Perfectness of the Hamming Codes is exploited.
Proof Consider a vector v s.t. $wt(v)=2$, then $\exists!$ codeword $c\in\mathscr{H}_m$ with $wt.(c)=3$ which covers v.(this means if $v_{i_1}=v_{i_2}=1$ then $c_{i_1}=c_{i_2}=1$) This is because $\mathscr{H}_m$ is perfect.Hence, codewords of $\mathscr{H}_m$ with weight 3 form the required Steiner system. To show the latter, consider a vector v' s.t. $wt(v')=3$ with 1's at indices P_i,P_j,P_k. Then either $k<n$ or $k=n$. Suppose $k<n$, then either $v'\in\mathscr{H}_m$ (after removing the last zero) and so $(v'|1)\in\hat{\mathscr{H}_m}$ which covers v' or $\exists u\in\mathscr{H}_m$ with $wt(u)=4$ which covers v'. Then $(u|0)\in\hat{\mathscr{H}_m}$. If $k=n$ then $\exists c\in\mathscr{H}_m$ s.t. c covers the vector with 1 on indices P_i,P_j. Then $(c|1)\in\hat{\mathscr{H}_m}$

This helps us to compute the no.of codewords with weight 3 in the Hamming code. The number of codewords in $\mathscr{H}_m$ with weight 3 is equal to $\frac{\binom{2^m-1}{2}}{\binom{3}{2}}$

A more general result is: Let $\mathscr{C}$ be a perfect e-error correcting code of length n, with e odd. Let $\hat{\mathscr{C}_n}$ be obtained by adding a parity check. Then the codewords of weight $(2e+1) \in \mathscr{C}$ form a Steiner System $S(e+1, 2e+1, n)$ and codewords of weight $(2e+2) \in \hat{\mathscr{C}_n}$ form a Steiner system $S(e+2, 2e+2, n+1)$

3 Golay Codes

The extended Golay code $\mathscr{G}_{24}$ has a generator matrix as follows:

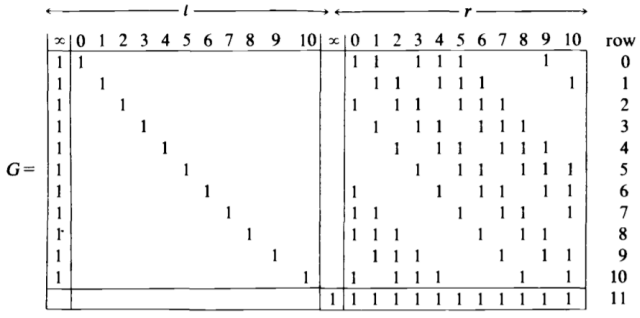


Fig. 2.13. Generator matrix for extended Golay code $\mathscr{G}_{24}$. The columns are labelled $l_\infty l_0 l_1 \cdots l_{10} r_\infty r_0 \cdots r_{10}$. The 11×11 matrix on the right is A_{11}.

Note that A_{11} mentioned is obtained from the Hadamard Matrix via Paley Construction.
For the indices mentioned in the diagram and $p = 11$, $A_{11} = [a_{ij}]$ where $a_{ij} = 1$ if $(j-i)$(mod p) $= 0$ or $(j-i)$(mod p) is a quadratic residue in $\mathbb{F}_{11}$ otherwise $a_{ij} = 0$ if $(j-i)$(mod p) is not a quadratic residue in $\mathbb{F}_{11}$

Some Properties of Golay Codes

- $\mathscr{G}_{24}$ is a $[24, 12, 8]$ linear code.
- Sum of any two rows of G has weight 8.
- $\mathscr{G}_{24}$ is self dual, $\mathscr{G}_{24} = \mathscr{G}_{24}^{\perp}$
- $\mathscr{G}_{24}$ contains the codeword **1**
- Every codeword of $\mathscr{G}_{24}$ has weight divisible by 4
  Check that every codeword in the generator matrix G of $\mathscr{G}_{24}$ has weight divisible by 4 and any codeword in $\mathscr{G}_{24}$ is either a row in G or a sum of two or more rows in G. So we need to show that sum of any two or more rows in G has weight divisible by four. This by induction reduces to showing the following:
  If $wt(x) = 4p$, $wt(y) = 4q$ and $xy = 0$ then $wt(x+y) = 4r$.
  Suppose $n_1 = |\{i : x_i = y_i = 1\}|$, $n_2 = |\{i : x_i = 1, y_i = 0\}|$, $n_3 = |\{i : y_i = 1, x_i = 0\}|$ and $n_4 = |\{i : y_i = 0 = x_i\}|$. Then from weight relations, $n_1 + n_2 = 4p$, $n_1 + n_3 = 4q$ and from $xy = 0$ $n_1 = 2z$ then $wt(x+y) = n_2 + n_3 = 4(p+q-z)$
- $\mathscr{G}_{24}$ is invariant under the following permutation. $T = (l_\infty r_\infty)(l_0 r_0)(l_1 r_{10})..(l_{10} r_1)$.
  In other words, if $\mathscr{G}_{24}$ contains a codeword $L|R$ where $L = l_\infty l_0 l_1..l_{10}$ and $R = r_\infty r_0 r_1..r_{10}$, it also contains a codeword $L'|R'$ where $L' =$

$r_\infty r_0 r_{10} r_9 .. r_1$ and $R' = l_\infty l_0 l_{10} .. l_1$
This also implies that if $\mathscr{G}_{24}$ has a codeword $L|R$ with $wt(L) = i$ and $wt(R) = j$ then there also exists $L'|R'$ s.t. $wt(L') = j$ and $wt(R') = i$

- An important result of the above property is that $\mathscr{G}_{24}$ does not contain any codeword of weight 4 and hence 20.
Suppose $\exists$ a codeword $c = (L|R) \in \mathscr{G}_{24}$ such that $wt(c) = 4$. Then either $wt(L) = 0$ or $wt(L) = 2$. (if $wt(L) = 4$ then $wt(R) = 0$ and by the above property $\exists c' = (L'|R')$ such that $wt(L') = 0$) But if $wt(L) = 0$ then $wt(R) = 12$ or 0. If $wt(L) = 2$ then c is a sum of any two rows (in the first eleven) and possibly the last row, but in any case $wt(R) = 6$. So $wt(c) = 4$ is not possible.

Definition: The (unextended) Golay code of length 23, $\mathscr{G}_{23}$ is obtained by deleting the last coordinate from every codeword of $\mathscr{G}_{24}$
$\mathscr{G}_{23}$ is a $[23, 12, 7]$ code and is a perfect triple error correcting code. Note that $1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11} = 2^{23-12}$

Ternary Golay Codes The extended ternary Golay code, denoted by $\mathscr{G}_12$ is the ternary linear code with generator $G = (I_6|B)$ where B is

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}$$

Again $\mathscr{G}_{12}$ is a self dual ternary $[12, 6, 6]$ code and the ternary Golay Code $\mathscr{G}_{11}$ is obtained by removing the last coordinate from each codeword in $\mathscr{G}_{12}$. $\mathscr{G}_{11}$ is a perfect ternary $[11, 6, 5]$ code.

4 No more Perfect Codes Exist

We prove the theorem due to Van Lint and Tietavainen.

A nontrivial perfect code over any field $\mathbf{F}_q$ must have the same parameters n, M and d as one of the Hamming or Golay codes.

Proof We assume a necessary condition for perfect codes to exist. (Lloyd's Condition)
Theorem If there exists an $(n, M, 2e + 1)$ perfect code over $\mathbb{F}_q$, then the Lloyd polynomial

$$\begin{aligned} L_e(x) &= P_0(x; n) + P_1(x; n) + .. + P_e(x; n) \\ &= P_e(x - 1; n - 1) \end{aligned}$$

$$= \sum_{j=0}^{e} (-1)^j (q-1)^{e-j} \binom{x-1}{j} \binom{n-x}{e-j}$$

has e integer zeros $\sigma_1, \sigma_2, .., \sigma_e$ satisfying $0 < \sigma_1 < \sigma_2 < .. < \sigma_2 < n$

Let $\mathscr{C}$ be a $(n, M, 2e+1)$ perfect code over $\mathbb{F}_q$ where $q = p^r$, p:prime and $\sigma_1, \sigma_2, .., \sigma_e$ are the integer zeros of $L_e(x)$.

Lemma 1 No. of codewords M is a power of q and $\sum_{j=0}^{e}(q-1)^j \binom{n}{j} = q^l$ for some integer l.
Proof The code being perfect, we have by the Hamming bound
$M \sum_{i=0}^{e}(q-1)^i \binom{n}{i} = q^n$. Now, $M = p^i$ for some integer i and so $\sum_{i=0}^{e}(q-1)^i \binom{n}{i} = p^{nr-i}$. This shows $q-1 = p^r - 1 | p^{nr-i} - 1$. Using fact that if $p^a - 1 | p^b - 1$ then $a|b$, we get $r|nr-i$ and so $r|i$, Hence M is a power of q.
Proof of the fact. Let $b = aq_0 + r_0$ then $p^b - 1 = p^{aq_0+r_0} - p^{r_0} + p^{r_0} - 1 = p^{r_0}(p^{aq_0} - 1) + (p^{r_0} - 1)$ Now $p^a - 1$ divides LHS and first term of RHS and so must also divide the second term in RHS but $r_0 < a$. Hence $r_0 = 0$

Lemma 2 $L_e(0) = q^l$; and if $\mathscr{C}$ is nontrivial, $L_e(1)$ and $L_e(2)$ are nonzero.
Proof Using $L_e(x)$ defined above, we get $L_e(0) = \sum_{j=0}^{e}(q-1)^{e-j}\binom{n}{e-j} = q^l$.
Also, $L_e(1) = (q-1)^e \binom{n-1}{e}$ and $e \leq n-1$ and so $L_e(1) \neq 0$
Finally $L_e(2) = \frac{(q-1)^{e-1}}{q}\binom{n-2}{q-1}(q(n-e-1) - n + 1)$ and this is 0 only if $q = 1 + (\frac{e}{n-e-1})$ which implies $n \leq 2e+1$ since $q \geq 2$ but this is the trivial case.

Lemma 3 $\sigma_1 + \sigma_2 + .. + \sigma_e = \frac{e(n-e)(q-1)}{q} + \frac{e(e+1)}{2}$ and $\sigma_1 .. \sigma_e = e! q^{l-e}$
Proof Using $L_e(x)$ we get the coefficients of x^e and x^{e-1}. Note that L_e is a polynomial of degree e. Coeff. of x^e comes out $\frac{(-q)^e}{e!}$ and coefficient of x^{e-1} is $\frac{(-q)^e}{e!}(\frac{e(n-e)(q-1)}{q} + \frac{e(e+1)}{2})$

We are dividing the proof into different parts. 1)$e = 1$, 2) $e = 2, q = 2$,
(3) $e = 2, q > 2$, (4) $e > 2, q > 2$, (5) $e > 2, q = 2$

Part (1) A perfect single-error-correcting code over $\mathbf{F}_q$ has the same parameters n, M and d as the Hamming code.
Proof By the sphere packing condition we have $1 + n(q-1) = q^l$ and by Lloyd's condition, $1 + (q-1)n - qx = 0$ has an integer root σ_1 and so $1 + (q-1)n - q\sigma_1 = 0$ These give $\sigma_1 = q^{l-1}$ and $n = q^l - 1/q - 1$. Also, $M = q^{n-l}$. So parameters of $\mathscr{C}$ is same as that of the Hamming Code of order l.

Part (2) There are no nontrivial binary perfect double-error-correcting code.
Proof By the Sphere packing bound we have $1 + n + \binom{n}{2} = q^l \implies (2n+1)^2 = 2^{l+3} - 7$. From Lloyd's Polynomial we have $2L_2(x) = y^2 - 2(n+1)y + 2^{l+1}$, with roots $y_1 = 2\sigma_1$ and $y_2 = 2\sigma_2$.
Note that since code is non-trivial, $y_1, y_2 \geq 4$ Also $y_1 y_2 = 2^{l+1}$ which im-

plies $y_1 = 2^a$ and $y_2 = 2^b$ such that $a + b = l + 1$ and $3 \leq a < b$. We have $2^a + 2^b = 2(n+1)$ and so $(2^a + 2^b - 1)^2 = 2^{l+3} - 7$.
Taking mod 16 both sides we have $1 \equiv -7$ (mod16) which is not possible.

Part (3) The only possible parameters for a nontrivial perfect double error-correcting code over a field $\mathbb{F}_q$, $q = p^r$, are the parameters of the ternary Golay code.
Proof The sphere packing condition gives: $1+(q-1)n+(q-1)^2\binom{n}{2} = q^l$. This gives $2(q-1)n = q-3+\sqrt{q^2-6q+1+8q^l}$.
From Lemma 3, we have $\sigma_1\sigma_2 = 2q^{l-2}$and $\sigma_1 + \sigma_2 = \frac{2(n-2)(q-1)}{q} + 3$. We can eliminate n and get $q(\sigma_1+\sigma_2) = 1+\sqrt{q^2-6q+1+8q^l}$, (1)
From Lemma 2, we have $\sigma_1, \sigma_2 > 2$ and from product of $\sigma_1\sigma_2$, $\sigma_1 = p^\lambda$ and $\sigma_2 = 2p^\mu$ with $\lambda, \mu \geq 1$ and $\lambda + \mu = r(l-2)$
Substituting σ_1, σ_2 in equation (1) and squaring and dividing by q we get
$q(p^\lambda + 2p^\mu)^2 - 2(p^\lambda + 2p^\mu) = q - 6 + 8q^{l-1}$ (2). Note that in here, all terms have a factor of p except -6. Hence p must be either 2 or 3. If p is 2 then $q-6$ must be divisible by 4 implying $q = 2$. But from **Part 2** this is not possible.
Substituting $p = 3$ and $q = 3$ in the equation (2)
$3(3^\lambda + 2(3^\mu))^2 - 2(3^\lambda + 2(3^\mu)) = -3 + 8(3^{l-1})$ We know $l \geq 3$ as $\sigma_1\sigma_2 = 2q^{l-2}$ and $\sigma_1, \sigma_2 > 1$.
Now, Expanding the above equation and dividing by 3 we get
$3^{2\lambda} + 4(3^{\lambda+\mu}) + 4(3^{2\mu}) - 2(3^{\lambda-1}) - 4(3^{\mu-1}) = -1 + 8(3^{l-2})$ Taking modulo 3 $\mu = 1$ and $\lambda = 2$ and so $l = 5$. From the sphere packing we get, $n = 11$ and hence they are the same parameters as the ternary Golay Codes.
Now if $q = 3^r$, from (2) we get $3^\lambda + 2(3^\mu) \equiv 3$(mod9). From here, $\lambda = 1$ and $\mu \geq 2$ This gives $3^{\mu+1} = q^{l-2}$ and (2) becomes $-4(3^\mu)+8(3^r) = 4(3^{r+\mu+1})-4(3^{2\mu+r})$
Note that the RHS has a power of 3 strictly greater than LHS and hence no solution exists.

Part 4 There is no nontrivial perfect e-error-correcting code over $\mathbb{F}_q, q = p^r$. if $q > 2$ and $e > 2$.

i) We first show $2\sigma_1 \leq \sigma_e$. If $s \in \mathbb{Z}^+$ and $s = p^\alpha t$ define $a_p(s) = t$. It is clear that $a_p(s_1)a_p(s_2) = a_p(s_1s_2)$ and $a_p(s) \leq s$. Using this we get that $a_p(\sigma_1)..a_p(\sigma_e) = a_p(\sigma_1..\sigma_e)$ Now using product of $\sigma_1..\sigma_e$, we have $a_p(\sigma_1..\sigma_e) \leq e!$ So either any two $a_p(\sigma_i), a_p(\sigma_j)$ are equal or each take value $1, 2, .., e$ in some order. In the first case, $\sigma_i = p^\alpha t$ and $\sigma_j = p^\beta t$. $\sigma_j > \sigma_i \implies \beta > \alpha$ and so $2\sigma_i \leq \sigma_j$. In the second case, $\exists \sigma_i, \sigma_j$ s.t. $a_p(\sigma_i) = 1$ and $a_p(\sigma_j) = 2$, and so we have $\sigma_i = p^\alpha$ and $\sigma_j = 2p^\beta$. This also leads to $2\sigma_i \leq \sigma_j$.(exchange the variables if necessary)
Hence we have $2\sigma_1 \leq 2\sigma_i \leq \sigma_j \leq \sigma_e$

ii) Next we show: $\sigma_1\sigma_e \leq \frac{8}{9}(\frac{\sigma_1+\sigma_e}{2})^2$. Given that $\frac{\sigma_e}{\sigma_1} \geq 2$, dividing by σ_1^2, we get $x \leq \frac{8}{9}((1+x)/2)^2$, $x = \sigma_e/\sigma_1$ and this is true if $x \geq 2$

iii) $\sigma_1..\sigma_e = q^{-e}e!\sum_{j=0}^{e}(q-1)^{e-j}\binom{n}{e-j} > q^{-e}(q-1)^e(n-1)..(n-e+1)$
$> q^{-e}(q-1)^e n^e(1-\frac{e(e-1)}{2n})$

Last inequality is using if $a_1, a_2, .., a_n \in \mathbb{R}_{\geq 0}$ we have $(1-a_1)..(1-a_n) \geq (1-(a_1+a_2+..+a_n))$

iv) We shall use the weighted version of Arithmetic- Geometric Inequality.

$\sigma_1..\sigma_e = (\sigma_1\sigma_e)(\sigma_2..\sigma_{e-1}) \leq \frac{8}{9}(\frac{\sigma_1+\sigma_e}{2})^2(\frac{\sigma_2+..+\sigma_{e-1}}{e-2})^2 \leq \frac{8}{9}(\frac{\sigma_1+..+\sigma_e}{e})^2$

Now using sum of σ_i's we get $\sigma_1..\sigma_e \leq \frac{8}{9}(\frac{(n-e)(q-1)}{q} + \frac{e+1}{2})^2 \leq \frac{8}{9}q^{-e}(q-1)^e n^e$

(the second inequality is by using $q > 2, e > 2$ and $\frac{e(q-1)}{q} - \frac{e}{2} > \frac{3q-8}{2q}$)

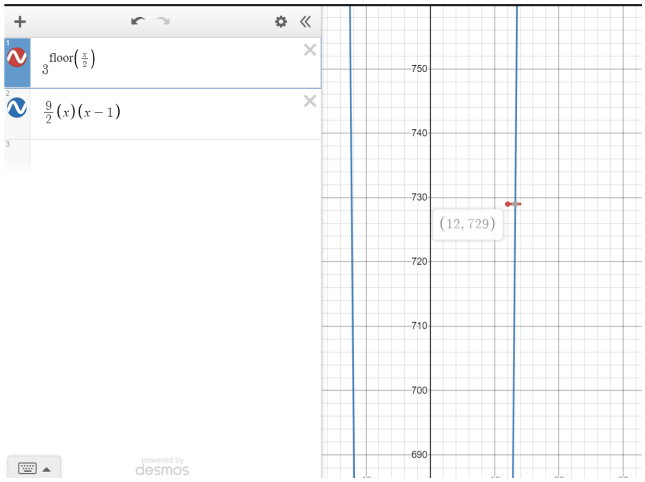
Using iii and iv we get, $n < \frac{9}{2}e(e-1)$

v) Considering non-trivial codes, by Lemma 2 we have $L_e(1)$ is non-zero. So $\prod_{i=0}^{e}(\sigma_i - 1) = \frac{e!}{q^e}L_e(1) = \frac{(q-1)^e(n-1)..(n-e)}{q^e}$ must be an integer and so $p^{re}|(n-1)(n-2)..(n-e)$. Let α be the largest power of p dividing any of $\{n-1, n-2, ..n-e\}$ then power of p dividing $(n-1)(n-2)..(n-e)$ is at most $\alpha + \lfloor\frac{e}{p}\rfloor + \lfloor\frac{e}{p^2}\rfloor + ...$ Hence $\alpha + \lfloor\frac{e}{p}\rfloor + \lfloor\frac{e}{p^2}\rfloor + .. \geq re \implies \alpha \geq re/2$
(This is because max additional number of factors due to p will be $\lfloor\frac{e}{p}\rfloor$ as if $n-i = q(p^\alpha)$ then $n-e > q(p^\alpha) + p * \lfloor\frac{e}{p}\rfloor$. Similary due to p^2, p^3 and so on.)
$q^{\lfloor\frac{e}{2}\rfloor}$ divides $n-i$ for some i and so $n \geq q^{\lfloor\frac{e}{2}\rfloor}$.

All these creates bounds on n, e:

$$3^{\lfloor\frac{e}{2}\rfloor} \leq q^{\lfloor\frac{e}{2}\rfloor} < n < \frac{9}{2}e(e-1)$$

This gives $e \leq 11$ and $n \leq 495$



If we iterate over them to find solutions of eq. in Lemma 1, there are no non-trivial perfect codes in the range.

A code snippet checking the above:

Listing 1: Code for checking

```
import math
def comb(n,r):
    prod=1
    for i in range(n,n-r,-1):
        prod=prod*i
    for j in range(1,r+1):
        prod=prod/j
    return int(prod)
def sum(n,e,q):
  sum=0
  for j in range(e+1):
    sum+=math.pow(q-1,j)*comb(n,j)
  return int(sum)
for e in range(3,12):
  for i in range(1,496):
    for q in range(3,496):
      if math.pow(q,math.floor(e/2))<i and 2*e+1<i and i!=q+1:
        ham=sum(i,e,q)
        pr=q
        for j in range(int(math.log(ham,q))+1):
          if(pr==ham):
            print((i,e,q))
            break
          else:
            pr=pr*q
```

Part 5 The only possible parameters for a nontrivial binary perfect e-error-correcting code with $e > 2$ are those of the Golay code.

Proof Consider $\prod_{i=0}^{e}(\sigma_i-2) = e!L_e(2)/2^e = (n-2)(n-3)..(n-e)(n-2e-1)/2^e$. Now since $(\sigma_i-1)(\sigma_i-2)$ is even, we have $2^{3e}|(n-1)(n-2)^2..(n-e)^2(n-2e-1)$ and by using the same idea as before $n > 2^{e/2}$. Following the same as part 4 , we can get upper bound on n.

References:
McWilliams and Sloane: "Theory of Error Correcting Codes"