MTH2002
Coding Theory

Semester A, 2024/25

Yuri Santos Rego

University of Lincoln

Week 3, Lecture 1

Today

Week 3: Goals

Week 3

1. Lecture 1: More geometry: solid spheres and symmetries.
2. Lecture 2: (Re)design strategies.

Last time

Recalling: Geometry of codes

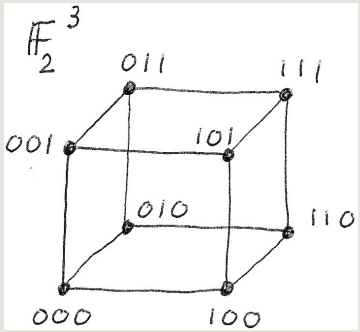
Definition 23 (Solid spheres)

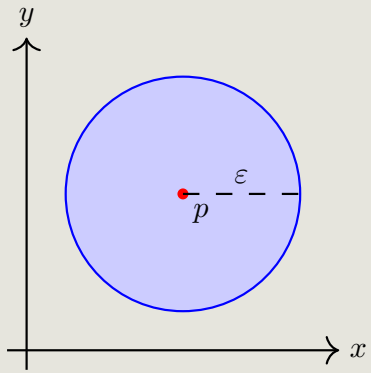
Given a metric space X with distance function d and a positive real number $\varepsilon \in \mathbb{R}_{>0}$, the solid sphere (or ball) or radius ε and centre $p \in X$ is the set defined by

$$S_\varepsilon(p) = \{x \in X \mid d(p, x) \leq \varepsilon\}.$$

In case X is *finite*, the volume of the (solid) sphere $S_\varepsilon(p)$, is its number of elements $\mathrm{vol}(S_\varepsilon(p)) := \#S_\varepsilon(p)$.

Examples





Recalling: The Distance Theorem

Distance Theorem (22)

Let C be a code with minimal distance $d_{\min}(C)$. Then the following statements hold:

1. If $t \in \mathbb{N}$ and $d_{\min}(C) \geq t+1$, then C detects t errors.
2. If $k \in \mathbb{N}$ and $d_{\min}(C) \geq 2k+1$, then C corrects k errors.

Corollary (27) to the Distance Theorem

Let C be a code and write $\mathbf{d}$ for $d_{\min}(C)$. Then C can detect up to $d-1$ errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$ denotes the integer part function: $\lfloor r \rfloor = \max\{z \in \mathbb{Z} \mid z \leq r\}$.

Recalling: Parameters

Definition 30 (Parameters of a code)

Let n, M, d and q be natural numbers. A code C called an $(n, M, d)_q$-code when

- the underlying alphabet used for C has q symbols,
- each codeword in C has length n,
- C itself has M codewords in total (i.e., $M = \#C$), and
- d is its minimal distance (i.e., $d = d_{\min}(C)$).

The numbers n, M, d and q are called *parameters* of C.

Recalling: Main Problem

Main Problem of Coding Theory

Given a q-ary alphabet, a length n, and a desired minimal distance d, design an $(n, M, d)_q$-code for which its total number of codewords M **is as large as possible**.

Notation

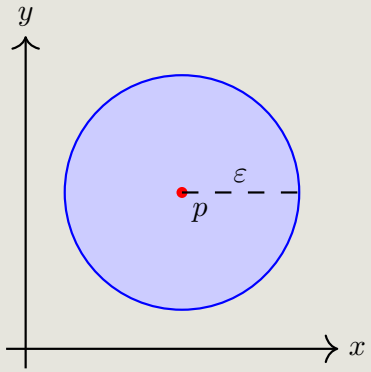
Given q, n, and d as above, we write $M_q(n, d)$ for the largest possible such M.

Written in mathematical symbols,
$M_q(n, d) := \max\{M \in \mathbb{N} \mid M = \#C \text{ for some } (n, M, d)_q\text{-code } C\}$.

More geometry: Solid spheres and symmetries

Motivating question: How 'big' are spheres?

Example: Euclidean solid spheres



The **(usual)** volume of a solid sphere $S_\varepsilon(p)$ of radius ε in n-dimensional Euclidean space $\mathbb{R}^n$ has a formula:

$$\mathrm{vol}(S_\varepsilon(p)) = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}\varepsilon^n,$$

where $\Gamma(\,)$ is a special function that goes $\Gamma(\frac{1}{2}+1) = \frac{\sqrt{\pi}}{2}$, $\Gamma(\frac{2}{2}+1) = 1$, $\Gamma(\frac{3}{2}+1) = \frac{3\sqrt{\pi}}{4}$, ... For instance, on the plane: $\mathrm{vol}(S_\varepsilon(p)) = \pi\varepsilon^2$. In three dimensions: $\mathrm{vol}(S_\varepsilon(p)) = \frac{4}{3}\pi\varepsilon^3$.

Is there a closed formula for $\mathrm{vol}(S_\varepsilon(w)) = \#S_\varepsilon(w)$ in spaces of words with the Hamming distance?

Lemma 35 (Volume of spheres in spaces of words)

Let A be a q-ary alphabet and let $n \in \mathbb{N}$. Consider the space of words A^n of length n as a metric space with the Hamming distance.

Then, given any word $w \in A^n$ and integer radius $\varepsilon \in \mathbb{N}$, the solid sphere $S_\varepsilon(w)$ has volume $\mathrm{vol}(S_\varepsilon(w)) = \#S_\varepsilon(w)$ given by the formula

$$\begin{aligned}\#S_\varepsilon(w) &= \binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{\varepsilon}(q-1)^\varepsilon \\ &= \sum_{i=0}^{\varepsilon} \binom{n}{i}(q-1)^i.\end{aligned}$$

Proof.

Goal: check that $\#S_\varepsilon(w) = \sum_{i=0}^{\varepsilon} \binom{n}{i}(q-1)^i$.

Recall: $S_\varepsilon(w) = \{x \in A^n \mid d(w,x) \leq \varepsilon\}$. So we need only count how many words are at Hamming distance i to w for each i from 0 to ε.

- A word at Hamming distance i to w differs from w in exactly i positions.
- There are $\binom{n}{i}$ ways to choose those differing positions.
- At every such position, we can use up to $q-1$ other symbols.
- Thus changing each symbol in i chosen positions can be done in $(q-1)^i$ ways.
- Altogether, we find exactly $\binom{n}{i}(q-1)^i$ words at distance exactly i from w.

Proof.

Goal: check that $\#S_\varepsilon(w) = \sum_{i=0}^{\varepsilon} \binom{n}{i}(q-1)^i$.

Recall: $S_\varepsilon(w) = \{x \in A^n \mid d(w,x) \leq \varepsilon\}$. So we need only count how many words are at Hamming distance i to w for each i from 0 to ε.

Adding everything up gives

$$\begin{aligned}\#S_\varepsilon(w) &= \binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{\varepsilon}(q-1)^\varepsilon \\ &= \sum_{i=0}^{\varepsilon} \binom{n}{i}(q-1)^i,\end{aligned}$$

as claimed. □

Corollary 36 (Spheres 'look the same' everywhere)

Let A be a q-ary alphabet and let $n \in \mathbb{N}$. Consider the space of words A^n of length n as a metric space with the Hamming distance.

Then, given any pair of words $v, w \in A^n$ and the same integer radius $\varepsilon \in \mathbb{N}$, the solid spheres $S_\varepsilon(w)$ and $S_\varepsilon(v)$ have exactly the same number of elements. In symbols,

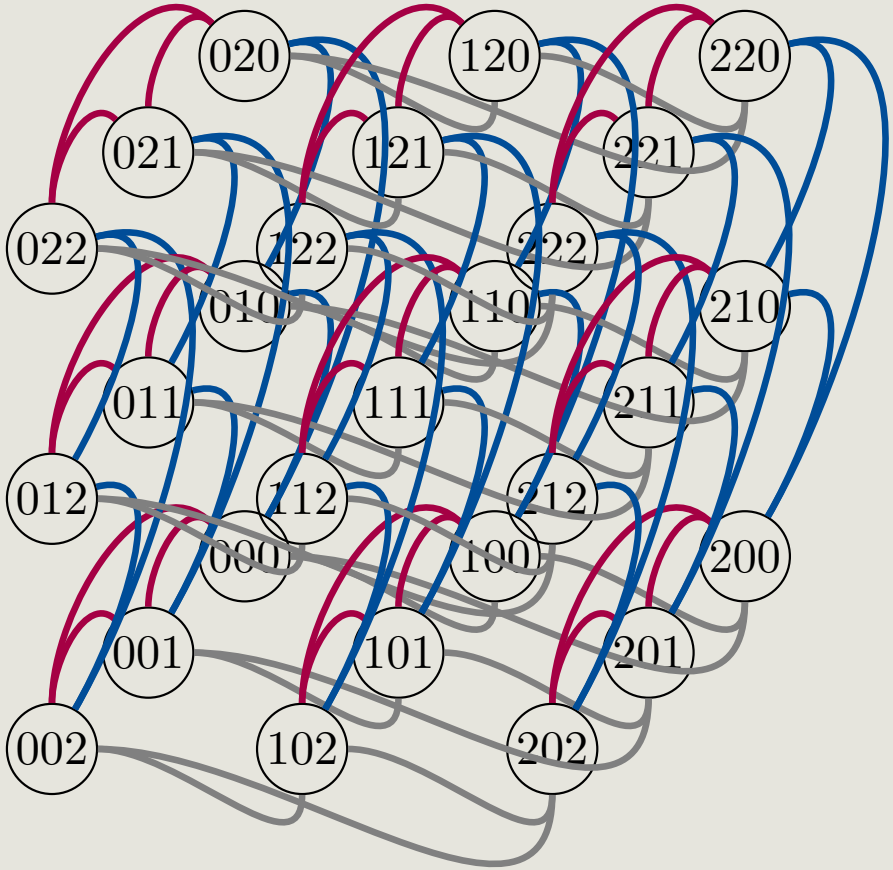
$$\operatorname{vol}(S_\varepsilon(w)) = \operatorname{vol}(S_\varepsilon(v)) \quad \forall w, v \in A^n.$$

Proof.

The formula from Lemma 35 tells us that those volumes only depend on the parameters n, q and on the radius ε, but not on the centres of the spheres. Thus the values are equal. □

Pictorial example

Identify $S_1(002)$ below within $\mathbb{F}_3^3$:



Another application of geometry to codes

Recall: The Main Problem of Coding Theory is, given parameters n (length), d (minimal distance) and q (number of symbols), to design $(n, M, d)_q$-codes where M (total number of codewords) is as large as possible. Using spheres we get the following bound for M:

Theorem 37 (Sphere Packing Bound (a.k.a. Hamming bound))

Let C be an $(n, M, d)_q$-code over a q-ary alphabet A, let $\varepsilon(d)$ be the value $\varepsilon(d) := \lfloor \frac{d-1}{2} \rfloor$, and let $c \in C$ be any codeword. Then the parameter $M = \#C$ is bounded from above as follows:

$$M \leq \frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))} = \frac{q^n}{\#S_{\varepsilon(d)}(c)},$$

where the volume $\mathrm{vol}(S_{\varepsilon(d)}(c)) = \#S_{\varepsilon(d)}(c)$ is taken in the space A^n (with the Hamming distance).

Consequence of the Sphere Packing Bound

Recall: $M_q(n,d)$ = largest possible number of codewords in a code of length n with minimal distance d and over a q-ary alphabet.
Written in mathematical symbols,
$M_q(n,d) := \max\{M \in \mathbb{N} \mid M = \#C \text{ for some } (n,M,d)_q\text{-code } C\}$.

Corollary 38

Writing $\varepsilon(d) = \lfloor \frac{d-1}{2} \rfloor$, *it holds*

$$M_q(n,d) \leq \frac{q^n}{\left(\sum_{i=0}^{\varepsilon(d)} \binom{n}{i} (q-1)^i\right)}.$$

Proof.

Follows by combining Corollary 36 and Lemma 35 with the Sphere Packing Bound Theorem. □

Proof of Sphere Packing Bound

Proof of the Sphere Backing Bound Theorem.

- Along the proof of the Distance Theorem, we have seen (cf. Lemma 25) that for $\varepsilon = \varepsilon(d) = \lfloor \frac{d-1}{2} \rfloor$ and any two codewords $v, w \in C$, the solid spheres $S_{\varepsilon(d)}(v)$ and $S_{\varepsilon(d)}(w)$ are disjoint.
- Hence, counting the elements of the union $\bigcup_{w \in C} S_{\varepsilon(d)}(w) \subseteq A^n$, we do not double count any elements of A^n. Therefore $\sum_{w \in C} \mathrm{vol}(S_{\varepsilon(d)}(w)) = \sum_{w \in C} \#S_{\varepsilon(d)}(w) \leq \#A^n = q^n$.
- By Corollary 36 and Lemma 35, the spheres $S_{\varepsilon(d)}(w)$ have the same number of elements. Thus, choosing $c \in C$, the sum above becomes $\sum_{w \in C} \#S_{\varepsilon(d)}(w) = \sum_{w \in C} \#S_{\varepsilon(d)}(c) =$ $\#S_{\varepsilon(d)}(c) \cdot \sum_{w \in C} 1 = \#S_{\varepsilon(d)}(c) \cdot \#C = M \cdot \mathrm{vol}(S_{\varepsilon(d)}(c))$. □

Applying the Sphere Packing Bound

The Sphere Packing Bound Theorem (SPBT) says: q-ary codes of given length n and desired minimal distance d cannot be 'too big'.

Example 39

Let C be a $(5, M, 3)_2$-code. So $q = 2$, $n = 5$ and $d = 3$. Thus $\varepsilon(d) = \varepsilon(3) = \lfloor \frac{3-1}{2} \rfloor = \lfloor \frac{2}{2} \rfloor = 1$. By Lemma 35, the volume of a solid sphere of radius $\varepsilon(d) = 1$ around any codeword $c \in C$ is

$$\begin{aligned} \operatorname{vol}(S_{\varepsilon(d)}(c)) &= \sum_{i=0}^{\varepsilon(d)} \binom{n}{i} (q-1)^i = \sum_{i=0}^{1} \binom{5}{i} (2-1)^i \\ &= \sum_{i=0}^{1} \binom{5}{i} \cdot 1 = \binom{5}{0} + \binom{5}{1} = 1 + 5 = 6. \end{aligned}$$

By the SPBT, $M \leq \frac{2^5}{6} = \frac{32}{6} = 6.4$, so $\#C = M \leq 6$ (because $\#C$ is an integer).

Applying the Sphere Packing Bound

The Sphere Packing Bound Theorem (SPBT) says: q-ary codes of given length n and desired minimal distance d cannot be 'too big'.

Example 39

Let C be a $(6, M, 1)_{11}$-code. So $q = 11$, $n = 6$ and $d = 1$. Thus $\varepsilon(d) = \varepsilon(1) = \lfloor \frac{1-1}{2} \rfloor = 0$. The volume of a solid sphere of radius 0 around a codeword $c \in C$ is 1 since this sphere only contains the centre.
By the SPBT, $\#C = M \leq \frac{11^6}{1} = 11^6$, which is quite big!

State of knowledge: if we try to design an $(n, M, d)_q$-code C, then C has *at most* $q^n / \mathrm{vol}(S_{\varepsilon(d)}(c))$ codewords (by the SPBT). Can C have *exactly* $\frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))}$ elements?

Question: Can an $(n, M, d)_q$-code have $\frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))}$ codewords?

Answer

Sometimes yes, but not always!

- 'Sometimes': $A = \mathbb{F}_3 = \{0, 1, 2\}$, $C = \mathbb{F}_3^2$. This is a $(2, 9, 1)_3$-code. So $\varepsilon(d) = \varepsilon(1) = \lfloor \frac{1-1}{2} \rfloor = 0$, thus $\mathrm{vol}(S_{\varepsilon(d)}(c)) = 1$ always, and $q^n = 3^2 = 9$. Hence, in this case, $\#C = M = 9$ and $\frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))} = \frac{9}{1} = 9 = M \rightsquigarrow$ equality!
- 'Not always': Consider a $(2, 5, 2)_5$-code C, so $M = 5$ and $\varepsilon(d) = \varepsilon(2) = \lfloor \frac{2-1}{2} \rfloor = 0$. The upper bound from the SPBT is $\frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))} = \frac{5^2}{1} = 25$, which is strictly larger than $\#C = M = 5 \rightsquigarrow$ strict inequality $M < \frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))}$.

SPBT & 'NICE' CODES

If the number of elements of a code **matches** the upper bound $\frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))}$ of the SPBT, this code deserves a name!

Definition 40 (Perfect codes)

An $(n, M, d)_q$-code C is said to be perfect if

$$M = \frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(c))}$$

for some codeword $c \in C$, where $\varepsilon(d) = \lfloor \frac{d-1}{2} \rfloor$.

Example 41

- The 'easy' code $C = A^n$ over the alphabet A is perfect.
- Hamming's original code (cf. Practicals, Week 2) is perfect.

Theorem 42 (Properties of perfect codes)

Let C be a perfect $(n, M, d)_q$-code over the alphabet A. Then the following hold:

1. *There exists an integer $k \geq 0$ such that $2k + 1 = d$ and so that A^n is a disjoint union of the solid spheres $S_k(w)$ with w ranging over C. In symbols, $A^n = \bigsqcup_{w \in C} S_k(c)$.*
2. *The minimal distance d cannot be even.*
3. *The code C corrects k errors.*

Proof.

Note that, once we prove part (1), the other parts follow: (1) implies (2) immediately because $d = 2k + 1$, an odd number. And (1) implies (3) by the Distance Theorem.

Proof of part (1) of Theorem 42.

Set $k = \varepsilon(d) = \lfloor \frac{d-1}{2} \rfloor$, which is a non-negative integer. As seen in the proof of the SPBT, we have

$$\bigcup_{w \in C} S_k(w) \subseteq A^n,$$

and the union on the left hand side is disjoint by Lemma 25. Now, the right hand side has q^n elements. The left hand side has exactly $\sum_{w \in C} \#S_k(w)$ elements, which is the same as $M \cdot \mathrm{vol}(S_{\varepsilon(d)}(c))$ as seen in the proof of the SPBT. But by Definition 40, $q^n = M \cdot \mathrm{vol}(S_{\varepsilon(d)}(c)) = \sum_{w \in C} \#S_k(w)$. Therefore every element of A^n must be contained in one of the solid spheres $S_k(w)$, and we are not counting elements multiple times. In other words, $\bigsqcup_{w \in C} S_k(w) = A^n$. □

Other 'geometric' aspects: Symmetries of codes

Symmetries

In maths (and sciences that use mathematics), it is quite useful to understand the symmetries of objects: among many other useful consequences, knowing the symmetries often allows us to drastically reduce the complexity of problems we are investigating.

Broad informal 'definition'

If $\mathcal{O}$ is a set that represents a mathematical object (for example, a vector space, a finite set, a polygon, a manifold, a field, ...), then the **symmetries of** $\mathcal{O}$ are a (sub)set of bijective functions from $\mathcal{O}$ to itself that preserve certain properties defining the object $\mathcal{O}$.

This set of symmetries is sometimes denoted by $\mathrm{Aut}(\mathcal{O})$.

Examples

- Year 1: If $\mathcal{O}$ is a vector space, then $\mathrm{Aut}(\mathcal{O})$ is the set of bijective linear transformations of $\mathcal{O}$.
- Year 2: If $\mathcal{O} =$ a regular square, then $\mathrm{Aut}(\mathcal{O}) = D_8$, the dihedral group of order 8.
- Now: If $\mathcal{O}$ is a metric space, then $\mathrm{Aut}(\mathcal{O})$ is the set of **isometries** of $\mathcal{O}$, i.e., those bijections that preserve distances.
- Year 3: No matter what $\mathcal{O}$ is, its symmetries $\mathrm{Aut}(\mathcal{O})$ always form a group! (The group operation is the composition of functions.)
- Year 4: If $\mathcal{O}$ is a differentiable manifold (for example $\mathbb{R}^n$), then $\mathrm{Aut}(\mathcal{O})$ is the set of **diffeomorphisms** of $\mathcal{O}$, i.e., bijective differentiable maps whose derivatives have nonzero determinant.

Here, we shall define symmetries of a code to find out about codes which 'work exactly the same'. Before, we need some terminology.

Definition 43 (Code matrix)

Given an $(n, M, d)_q$-code C, its (full) code matrix — also written C — is the $(M \times n)$-matrix created by listing all the codewords of C in rows.

Example 44

For $C_3 = \{00000, 01101, 10110, 11011\}$, the code from Example 5 (first lecture), its code matrix is the four-by-five matrix

$$C_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Definition 45 (Transformations, equivalence, and symmetries)

Given a code $C \subseteq A^n$, represented as its code matrix, a code transformation applied to C is a (finite) combination of operations of the following types:

(a) permuting the columns of the code matrix C;

(b) permuting the symbols appearing in a given column of the code matrix C.

After transforming a code $C \subseteq A^n$, we always obtain another code $C' \subseteq A^n$, and we say that the resulting code C' and the original code C are equivalent.

We call a code transformation a code symmetry (or code automorphism) if $C' = C$. (That is, if the code transformation does not result in a different code.)

Example 46

Let us transform $C_3 = \{00000, 01101, 10110, 11011\}$:

$$C_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Example 46

Let us transform $C_3 = \{00000, 01101, 10110, 11011\}$:

$$C_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \xmapsto{2^{\text{nd}} \leftrightarrow 4^{\text{th}} \text{ columns}} C_3' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Step 1. First swap the second and fourth columns.

Example 46

Let us transform $C_3 = \{00000, 01101, 10110, 11011\}$:

$$C_3' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{\text{swap 0 by 1 in } 2^{\text{nd}} \text{ column}} C_3'' = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Step 2. Permute (i.e., swap) 0 and 1 in second column.

Example 46

Let us transform $C_3 = \{00000, 01101, 10110, 11011\}$:

$$C_3'' = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{\text{swap 0 by 1 in } 4^{\text{th}} \text{ column}} C_3''' = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Step 3. Permute (i.e., swap) 0 and 1 in fourth column.

The codes $C_3 = \{00000, 01101, 10110, 11011\}$ and $C_3''' = \{01010, 10001, 01101, 10110\}$ are equivalent.

Example 47 (Code symmetry)

Again consider $C_3 = \{00000, 01101, 10110, 11011\}$:

$$C_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

If we now swap the first and fourth columns, and then swap the second and fifth columns, the resulting code will again be C_3 (exactly the same code matrix). This transformation is thus a symmetry.

Properties of code transformations

Theorem 48 (Number of equivalent codes)

Given an $(n, M, d)_q$-code C, the number of distinct codes equivalent to C is equal to $\frac{n! \cdot (q!)^n}{s(C)}$, where $s(C)$ denotes the total number of code symmetries of C.

Proof idea (easier in Year 3 after Group Theory)

- The number of permutations (bijections) of a set with n elements is $n!$, which is the number of elements of the *symmetric group* S_n on n letters.
- Thus there are $n!$ permutations of the n columns of C (transformations of type (a)), and $q!$ permutations of the symbols of the underlying alphabet of C.

Theorem 48 (Number of equivalent codes)

Given an $(n, M, d)_q$-code C, the number of distinct codes equivalent to C is equal to $\frac{n! \cdot (q!)^n}{s(C)}$, where $s(C)$ denotes the total number of code symmetries of C.

Proof idea (easier in Year 3 after Group Theory)

- For each column we can apply those $q!$ permutations of symbols, hence we can get $(q!)^n$ transformations of type (b).
- The final number of transformations of C has to be divided by $s(C)$ since symmetries do not change the code. □

Definition 49 (Isometries)

Given metric spaces X and Y with distance functions d_X and d_Y, respectively, an isometry between X and Y is a bijective function $T : X \to Y$ which preserves distances — that is,

$$d_Y(T(a), T(b)) = d_X(a, b) \quad \text{for all } a, b \in X.$$

Example 50

Given an angle $\theta \in [0, 2\pi)$, a rotation in $\mathbb{R}^2$ about θ is an isometry from $\mathbb{R}^2$ to itself (with respect to the usual Euclidean distance).

[Trivia/reminder: in matrix form, the rotation above is given by $\binom{x}{y} \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \binom{x}{y}$.]

Properties of code transformations

Proposition 51

Let $T : C \to C'$ be a code transformation between two codes. Then T is an isometry (with respect to the Hamming distance).

Proof.

We need only argue that code transformations of types (a) and (b) do not change the Hamming distance.

A transformation of type (a) permutes columns (say i-th and j-th columns) of C. Thus they change the i-th and j-th entry of all its codewords simultaneously. Hence, given a pair of codewords $c_1, c_2 \in C$, the number of differences between their entries before or after the transformation remains the same.

Proposition 51

Let $T : C \to C'$ be a code transformation between two codes. Then T is an isometry (with respect to the Hamming distance).

Proof.

A transformation of type (b) permutes simultaneously permutes a fixed entry of all codewords of C. Thus, this rearrangement of entries maintains differences or equalities between a pair of codewords in the corresponding position. Therefore the number of differences between their entries before or after the transformation is the same. □

Corollary 52

If $T : C \to C$ is a code symmetry, then $T \in \mathrm{Isom}(C)$ — the group of all isometries of C.

Corollary 53 (Equivalence preserves parameters)

If C and C' are equivalent codes, then their parameters are the same.
That is, if C is an $(n_1, M_1, d_1)_{q_1}$-code and if C' is an $(n_2, M_2, d_2)_{q_2}$-code, then $n_1 = n_2$, $M_1 = M_2$, $d_1 = d_2$ and $q_1 = q_2$.

Proof.

Code transformations clearly do not change the length of codes nor their number of elements nor their number of symbols. And by Proposition 51 they also do not affect the Hamming distance, hence also the minimal distance is preserved. □

Example 54

Consider the binary repetition code $C = \{000, 111\}$ of length 3,

$$C = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

There are 3! ways of permuting the columns of C, but none of which results in a new code. Besides these swaps, the code transformation that simultaneously swaps 0 by 1 in all columns of C also yields the same code (viewed as a set).
Thus C has $3! \cdot 2$ symmetries. By Theorem 48, C has $\frac{n!(q!)^n}{3!2} = \frac{3!2^3}{3!2} = 2^2 = 4$ equivalent codes. These are easy to find:

$$C = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

We see they all are $(3, 2, 3)_2$-codes, as predicted by Corollary 53.

Properties of code transformations

Recall: $\mathbb{F}_q = \{0, 1, 2, \ldots, q-1\}$.

Lemma 55 (Linear codes contain the zero vector)

Any code $C \subseteq \mathbb{F}_q^n$ is equivalent to a code containing the **zero codeword** $\underline{\mathbf{0}} = 0\,0\ldots0 \in \mathbb{F}_q^n$.

Proof.

Let $c = c_1\, c_2 \ldots c_n$ be the codeword on the top row of the code matrix of C. For every $i = 1, 2, \ldots, n$, choose a bijection $\sigma_i : \mathbb{F}_q \to \mathbb{F}_q$ that sends c_i to 0. Applying to the i-th column of C the code transformation of type (b) corresponding to the permutation σ_i changes the i-th entry of c into zero. Doing those n transformations successively for each $i = 1, 2, \ldots, n$ eventually turns c into $\underline{\mathbf{0}}$. □

Recall: $\mathbb{F}_q = \{0, 1, 2, \ldots, q-1\}$.

Corollary 56 (SPBT over $\mathbb{F}_q$)

If C is an $(n, M, d)_q$ code over the alphabet $\mathbb{F}_q$, then

$$M \leq \frac{q^n}{\mathrm{vol}(S_{\varepsilon(d)}(\underline{\mathbf{0}}))}.$$

Proof.

Combine the SPBT with Lemma 55 and Corollary 53. □

Next lecture

Next time...

- Strategies to (re)design codes;
- Modular arithmetic.

I wish you a great week!