UPPER BOUND FOR $A_q(n,d)$

(MAX NUMBERS OF CODEWORDS IN q-ary codes of length n and distance d)

1. HAMMING BOUND

FOR A q-ary (n, M, d) code C with $d = 2\ell + 1$ (correcting ℓ errors) consider M balls B_ℓ of radius ℓ and centers being codewords

A volume of a ball is

$$|B_\ell| = \sum_{i=0}^{\ell} \binom{n}{i} (q-1)^i$$

EXAMPLE $q=2$, $n=5$, $\ell=1$

correction of single errors $\Rightarrow$

$d=3$

BY HAMMING BOUND:

$$A_2(5,3) \le \frac{2^5}{\sum_{i=0}^{1} \binom{5}{i}} =$$

$$= \frac{32}{6} \le 5\tfrac{2}{6}.$$

Since we constructed

$(5,4,3)$ code

we have:

$$4 \le A_2(5,3) \le 5$$

ACTUALLY $A_2(5,3)=4$

SINCE THESE BALLS CANNOT INTERSECT is C correct ℓ errors $(d = 2\ell+1)$ and $|\mathbb{Z}_q^n| = q^n$ we have

$$\boxed{M\,|B_\ell| = M \cdot \sum_{i=0}^{\ell} \binom{n}{i} (q-1)^i \le q^n}$$

or

$$\boxed{A_q(n,d) \le \frac{q^n}{\sum_{i=0}^{\ell} \binom{n}{i} (q-1)^i}}$$

HAMMING BOUND.

ISBN code

Every recent book has ISBN number $(x_1, x_2, \ldots, x_{10})$

e.x. 0-19-853804-9

for "First course in Coding Theory" by R. Hill

Set of all ISBN numbers forms ISBM code C

$C \subseteq Z_{10}^{10}$

For this code

$$x_1 + 2x_2 + 3x_3 + 4x_4 + \ldots + 10x_{10} = 0 \pmod{11}$$

C is the check sum code

or $x_{10} = \sum_{i=1}^{9} i x_i \pmod{11}$

SINCE $10 \equiv -1 \mod 11$

T. ISBN check sum code

detect any single error and any double error created by transposition of two digits

(since different digits have different weights)

If for (n, M, d) code C

with $d = 2\ell + 1$

$$M = q^n \Big/ \sum_{i=0}^{\ell} \binom{n}{i} (q-1)^i$$

then C is a <u>perfect</u> code

<u>EXAMPLE</u> 1. $q = 2$, $\ell = 1$, $n = 3$

$C = \{000, 111\}$ - <u>triplication</u> code

$d = 3$

$M = |C| = 2$

$$|B_1| = \sum_{i=0}^{1} \binom{3}{i} (2-1)^i = 1 + 3 = 4$$

$$M \cdot |B_1| = 2 \cdot 4 = 2^3 = 8.$$

C is perfect

EXAMPLE 2 BINARY REPETITION CODE

$q = 2 \qquad n = d = 2\ell + 1$

$C = \{ \underbrace{00\ldots0}_{n}, \underbrace{11\ldots1}_{n} \}, \quad |C| = 2$

SINCE $|B_\ell| = \sum_{i=0}^{\ell} \binom{2\ell+1}{i} = 2^{2\ell}$

we have that repetition codes are perfect

(but for these codes $|C| = 2$ - only two codewords)

Perfect codes exists only for very few n and d.

All binary perfect codes are known.

(IN addition to repetition codes, they include Hamming codes and Golay code which we will discuss later)

THE HAMMING BOUND IS ALSO KNOWN AS THE <u>SPHERE-PACKING BOUND</u>.

THIS BOUND is good for

$n \geq 2d+1$ or since $d = 2\ell+1$

$n \geq 4\ell+3$

PLOTKIN BOUND

(without proof)

- If $n < 2d$ and d even

$$\boxed{A_2(n,d) \le 2 \left\lfloor d/2d-n \right\rfloor}$$

- If $n < 2d+1$ and d odd

$$\boxed{A_2(n,d) \le 2 \left\lfloor {d+1}/{(2d+1-n)} \right\rfloor}$$

$\lfloor a \rfloor$ - greatest integer less or equal to a

Ex.
$\lfloor 2.7 \rfloor = 2.$