Singleton bound

In coding theory, the **Singleton bound**, named after Richard Collom Singleton, is a relatively crude upper bound on the size of an arbitrary block code C with block length n , size M and minimum distance d .

1 Statement of the bound

The minimum distance of a set C of codewords of length n is defined as

$$d = \min_{\{x,y \in C : x \neq y\}} d(x, y)$$

where $d(x, y)$ is the Hamming distance between x and y . The expression $A_q(n, d)$ represents the maximum number of possible codewords in a q-ary block code of length n and minimum distance d .

Then the Singleton bound states that

$$A_q(n, d) \leq q^{n-d+1}.$$

2 Proof

First observe that the number of q -ary words of length n is q^n , since each letter in such a word may take one of q different values, independently of the remaining letters.

Now let C be an arbitrary q-ary block code of minimum distance d . Clearly, all codewords $c \in C$ are distinct. If we puncture the code by deleting the first $d - 1$ letters of each codeword, then all resulting codewords must still be pairwise different, since all of the original codewords in C have Hamming distance at least d from each other. Thus the size of the altered code is the same as the original code.

The newly obtained codewords each have length

$$n - (d - 1) = n - d + 1$$

and thus, there can be at most q^{n-d+1} of them. Since C was arbitrary, this bound must hold for the largest possible code with these parameters, thus:[1]

$$|C| \leq A_q(n, d) \leq q^{n-d+1}.$$

3 Linear codes

If C is a linear code with block length n , dimension k and minimum distance d over the finite field with q elements, then the maximum number of codewords is q^k and the Singleton bound implies:

$$q^k \leq q^{n-d+1}$$

so that

$$k \leq n - d + 1$$

which is usually written as[2]

$$d \leq n - k + 1$$

In the linear code case a different proof of the Singleton bound can be obtained by observing that rank of the parity check matrix is $n-k$.[3] Another simple proof follows from observing that the rows of any generator matrix in standard form have weight at most $n - k + 1$.

4 History

The usual citation given for this result is Singleton (1964), but according to Welsh (1988, p. 72) the result can be found in a 1953 paper of Komamiya.[4]

5 MDS codes

Linear block codes that achieve equality in the Singleton bound are called **MDS (maximum distance separable) codes**. Examples of such codes include codes that have only two codewords (the all-zero word and the all-one word, having thus minimum distance n), codes that use the whole of $(\mathbb{F}_q)^n$ (minimum distance 1), codes with a single parity symbol (minimum distance 2) and their dual codes. These are often called *trivial* MDS codes.

In the case of binary alphabets, only trivial MDS codes exist.[5][6]

Examples of non-trivial MDS codes include Reed-Solomon codes and their extended versions.[7][8]

MDS codes are an important class of block codes since, for a fixed n and k , they have the greatest error correcting and detecting capabilities. There are several ways to characterize MDS codes:[9]

Theorem: Let C be a linear [n, k, d] code over $\mathbb{F}_q$. The following are equivalent:

- C is an MDS code.
- Any k columns of a generator matrix for C are linearly independent.
- Any $n-k$ columns of a parity check matrix for C are linearly independent.
- $C^\perp$ is an MDS code.
- If $G = (I|A)$ is a generator matrix for C in standard form, then every square submatrix of A is nonsingular.
- Given any d coordinate positions, there is a (minimum weight) codeword whose support is precisely these positions.

The last of these characterizations permits, by using the MacWilliams identities, an explicit formula for the complete weight distribution of an MDS code.[10]

Theorem: Let C be a linear [n, k, d] MDS code over $\mathbb{F}_q$. If A_w denotes the number of codewords in C of weight w , then

$$A_w = \binom{n}{w}\sum_{j=0}^{w-d}(-1)^j\binom{w}{j}(q^{w-d+1-j}-1) = \binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}.$$

5.1 Arcs in projective geometry

The linear independence of the columns of a generator matrix of an MDS code permits a construction of MDS codes from objects in finite projective geometry. Let $PG(N, q)$ be the finite projective space of (geometric) dimension N over the finite field $\mathbb{F}_q$. Let $K = \{P_1, P_2, \ldots, P_m\}$ be a set of points in this projective space represented with homogeneous coordinates. Form the $(N+1) \times m$ matrix G whose columns are the homogeneous coordinates of these points. Then,[11]

Theorem: K is a (spatial) m-arc if and only if G is the generator matrix of an $[m, N+1, m-N]$ MDS code over $\mathbb{F}_q$.

6 See also

- Gilbert–Varshamov bound
- Plotkin bound
- Hamming bound
- Johnson bound
- Griesmer bound

7 Notes

[1] Ling & Xing 2004, p. 93

[2] Roman 1992, p. 175

[3] Pless 1998, p. 26

[4] Komamiya, Y. (1953), "Application of logical mathematics to information theory", *Proc. 3rd Japan. Nat. Cong. Appl. Math.*: 437

[5] Vermani 1996, Proposition 9.2

[6] Ling & Xing 2004, p. 94 Remark 5.4.7

[7] MacWilliams & Sloane 1977, Ch. 11

[8] Ling & Xing 2004, p. 94

[9] Roman 1992, p. 237, Theorem 5.3.7

[10] Roman 1992, p. 240

[11] Bruen, A.A.; Thas, J.A.; Blokhuis, A. (1988), "On M.D.S. codes, arcs in PG(n,q), with q even, and a solution of three fundamental problems of B. Segre", *Invent. Math.*, **92**: 441–459, doi:10.1007/bf01393742

8 References

- Ling, San; Xing, Chaoping (2004), *Coding Theory / A First Course*, Cambridge University Press, ISBN 0-521-52923-9
- MacWilliams, F.J.; Sloane, N.J.A. (1977), *The Theory of Error-Correcting Codes*, North-Holland, pp. 33, 37, ISBN 0-444-85193-3
- Pless, Vera (1998), *Introduction to the Theory of Error-Correcting Codes* (3rd ed.), Wiley Interscience, ISBN 0-471-19047-0
- Roman, Steven (1992), *Coding and Information Theory*, GTM, **134**, Springer-Verlag, ISBN 0-387-97812-7
- Singleton, R.C. (1964), "Maximum distance q-nary codes", *IEEE Trans. Inf. Theory*, **10** (2): 116–118, doi:10.1109/TIT.1964.1053661
- Vermani, L. R. (1996), *Elements of algebraic coding theory*, Chapman & Hall
- Welsh, Dominic (1988), *Codes and Cryptography*, Oxford University Press, ISBN 0-19-853287-3

9 Further reading

- J.H. van Lint (1992). *Introduction to Coding Theory*. GTM. **86** (2nd ed.). Springer-Verlag. p. 61. ISBN 3-540-54894-7.
- Niederreiter, Harald; Xing, Chaoping (2001). "6. Applications to algebraic coding theory". *Rational points on curves over finite fields. Theory and Applications*. London Mathematical Society Lecture Note Series. **285**. Cambridge: Cambridge University Press. ISBN 0-521-66543-4. Zbl 0971.11033.

10 Text and image sources, contributors, and licenses

10.1 Text

- **Singleton bound** *Source:* https://en.wikipedia.org/wiki/Singleton_bound?oldid=741652168 *Contributors:* Michael Hardy, Charles Matthews, Adam Bishop, DJ Clayworth, Giftlite, Pierremenard, Shreevatsa, Ruud Koot, Rjwilmsi, Reetep, SmackBot, Frap, Thijs!bot, Hermel, Vanish2, David Eppstein, Addbot, Luckas-bot, Citation bot, Xqbot, Omnipaedista, Sonofnob, VanceIII, Citation bot 1, Orenburg1, Zxl.gzhu, Wcherowi, BG19bot, Boriaj, Deltahedron, ZeeMurph and Anonymous: 19

10.2 Images

10.3 Content license