Hamming bound

In mathematics and computer science, in the field of coding theory, the **Hamming bound** is a limit on the parameters of an arbitrary block code: it is also known as the **sphere-packing bound** or the **volume bound** from an interpretation in terms of packing balls in the Hamming metric into the space of all possible words. It gives an important limitation on the efficiency with which any error-correcting code can utilize the space in which its code words are embedded. A code which attains the Hamming bound is said to be a **perfect code**.

1 Background on error-correcting codes

An original message and an encoded version are both composed in an alphabet of *q* letters. Each code word contains *n* letters. The original message (of length *m*) is shorter than *n* letters. The message is converted into an *n*-letter codeword by an encoding algorithm, transmitted over a noisy channel, and finally decoded by the receiver. The decoding process interprets a garbled codeword, referred to as simply a *word*, as the valid codeword "nearest" the *n*-letter received string.

Mathematically, there are exactly q^m possible messages of length *m*, and each message can be regarded as a vector of length *m*. The encoding scheme converts an *m*-dimensional vector into an *n*-dimensional vector. Exactly q^m valid codewords are possible, but any one of q^n garbled codewords (words) can be received, because the noisy channel might distort one or more of the *n* letters while the codeword is being transmitted.

2 Statement of the bound

Let $A_q(n,d)$ denote the maximum possible size of a q -ary block code C of length n and minimum Hamming distance d (a q -ary block code of length n is a subset of the strings of $\mathcal{A}_q^n$, where the alphabet set $\mathcal{A}_q$ has q elements).

Then, the Hamming bound is:

$$A_q(n,d) \leq \frac{q^n}{\sum_{k=0}^{t} \binom{n}{k}(q-1)^k}$$

where

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

3 Proof

By definition of d , if at most $t = \left\lfloor \frac{1}{2}(d-1) \right\rfloor$ errors are made during transmission of a codeword then minimum distance decoding will decode it correctly (i.e., it decodes the received word as the codeword that was sent). Thus the code is said to be capable of correcting t errors.

For a given codeword $c \in C$, consider the ball of radius t around c . Every pair of balls (Hamming spheres) are non-intersecting by the *t*-error-correcting property, and each ball contains (in other words, the volume of the ball) *m* words. Since we may allow (or choose) up to t of the n components of a word to deviate (from the value of the corresponding component of the ball's centre, which is a codeword) to one of $(q-1)$ possible other values (recall, the code is q-ary: it takes values in $\mathcal{A}_q^n$), we can define:

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

Since $A_q(n,d)$ is the maximum total number of codewords in C , and thus the greatest number of balls, and no two balls have a word in common, by taking the union of the words in balls centered at codewords we observe that the resulting set of words, each counted precisely once, is a subset of $\mathcal{A}_q^n$ (where $|\mathcal{A}_q^n| = q^n$ words) and deduce:

$$A_q(n,d) \times m = A_q(n,d) \times \sum_{k=0}^{t} \binom{n}{k}(q-1)^k \leq q^n.$$

Whence:

$$A_q(n,d) \leq \frac{q^n}{\sum_{k=0}^{t} \binom{n}{k}(q-1)^k}.$$

4 Covering radius and packing radius

Main article: Covering radius

For an $A_q(n,d)$ code *C* (a subset of $\mathcal{A}_q^n$), the *covering radius* of *C* is the smallest value of *r* such that every element of $\mathcal{A}_q^n$ is contained in at least one ball of radius *r* centered at each codeword of *C*. The *packing radius* of *C* is the largest value of *s* such that the set of balls of radius *s* centered at each codeword of *C* are mutually disjoint.

From the proof of the Hamming bound, it can be seen that for $t = \left\lfloor \frac{1}{2}(d-1) \right\rfloor$, we have:

$$s \le t \text{ and } t \le r.$$

Therefore, $s \le r$ and if equality holds then $s = r = t$. The case of equality means that the Hamming bound is attained.

5 Perfect codes

Codes that attain the Hamming bound are called **perfect codes**. Examples include codes that have only one codeword, and codes that are the whole of $\mathcal{A}_q^n$. Another example is given by the *repeat codes*, where each symbol of the message is repeated an odd fixed number of times to obtain a codeword where $q = 2$. All of these examples are often called the *trivial* perfect codes. In 1973, it was proved that any non-trivial perfect code over a prime-power alphabet has the parameters of a Hamming code or a Golay code.[1]

A perfect code may be interpreted as one in which the balls of Hamming radius *t* centered on codewords exactly fill out the space (*t* is the covering radius = packing radius). A **quasi-perfect code** is one in which the balls of Hamming radius *t* centered on codewords are disjoint and the balls of radius *t*+1 cover the space, possibly with some overlaps.[2] Another way to say this is that a code is *quasi-perfect* if its covering radius is one greater than its packing radius.[3]

6 See also

- Griesmer bound
- Singleton bound
- Gilbert-Varshamov bound
- Plotkin bound
- Johnson bound
- Rate-distortion theory

7 Notes

[1] Hill (1988) p. 102

[2] McWilliams and Sloane, p. 19

[3] Roman 1992, pg. 140

8 References

- Raymond Hill (1988). *A First Course In Coding Theory*. Oxford University Press. ISBN 0-19-853803-0.
- F.J. MacWilliams; N.J.A. Sloane (1977). *The Theory of Error-Correcting Codes*. North-Holland. ISBN 0-444-85193-3.
- Vera Pless (1982). *Introduction to the Theory of Error-Correcting Codes*. John Wiley & Sons. ISBN 0-471-08684-3.
- Roman, Steven (1992), *Coding and Information Theory*, GTM, **134**, New York: Springer-Verlag, ISBN 0-387-97812-7
- J.H. van Lint (1992). *Introduction to Coding Theory*. GTM. **86** (2nd ed.). Springer-Verlag. ISBN 3-540-54894-7.
- J.H. van Lint (1975). “A survey of perfect codes”. *Rocky Mountain Journal of Mathematics*. **5** (2): 199–224. doi:10.1216/RMJ-1975-5-2-199.
- P. J. Cameron; J. A. Thas; S. E. Payne (1976). “Polarities of generalized hexagons and perfect codes”. **5**: 525–528. doi:10.1007/BF00150782.

9 Text and image sources, contributors, and licenses

9.1 Text

- **Hamming bound** *Source:* https://en.wikipedia.org/wiki/Hamming_bound?oldid=713575236 *Contributors:* The Anome, Michael Hardy, Ixfd64, Charles Matthews, Bearcat, Giftlite, Mpeisenbr, Diego Moya, Culix, Pierremenard, BD2412, Reetep, Malcolma, SmackBot, Oli Filth, CmdrObot, Thijs!bot, Hermel, Drizzd~enwiki, Vanish2, David Eppstein, Jamelan, Sharov, Wdwd, Mild Bill Hiccup, Addbot, Luckas-bot, Kilom691, Piano non troppo, Citation bot, VanceIII, Citation bot 1, GoingBatty, Wcherowi, Rezabot, Schjora, Monkbot and Anonymous: 16

9.2 Images

9.3 Content license