WIKIPEDIA

Linear code

In coding theory, a **linear code** is an error-correcting code for which any linear combination of codewords is also a codeword. Linear codes are traditionally partitioned into block codes and convolutional codes, although turbo codes can be seen as a hybrid of these two types.[1] Linear codes allow for more efficient encoding and decoding algorithms than other codes (cf. syndrome decoding).

Linear codes are used in forward error correction and are applied in methods for transmitting symbols (e.g., bits) on a communications channel so that, if errors occur in the communication, some errors can be corrected or detected by the recipient of a message block. The codewords in a linear block code are blocks of symbols that are encoded using more symbols than the original value to be sent.[2] A linear code of length *n* transmits blocks containing *n* symbols. For example, the [7,4,3] Hamming code is a linear binary code which represents 4-bit messages using 7-bit codewords. Two distinct codewords differ in at least three bits. As a consequence, up to two errors per codeword can be detected while a single error can be corrected.[3] This code contains 2^4=16 codewords.

Contents

Definition and parameters

A **linear code** of length *n* and rank *k* is a linear subspace *C* with dimension *k* of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with *q* elements. Such a code is called a *q*-ary code. If *q* = 2 or *q* = 3, the code is described as a **binary code**, or a **ternary code** respectively. The vectors in *C* are called *codewords*. The **size** of a code is the number of codewords and equals q^k.

The **weight** of a codeword is the number of its elements that are nonzero and the **distance** between two codewords is the Hamming distance between them, that is, the number of elements in which they differ. The distance *d* of the linear code is the minimum weight of its nonzero codewords, or equivalently, the minimum distance between distinct codewords. A linear code of length *n*, dimension *k*, and distance *d* is called an [*n*,*k*,*d*] code.

We want to give $\mathbb{F}_q^n$ the standard basis because each coordinate represents a "bit" that is transmitted across a "noisy channel" with some small probability of transmission error (a binary symmetric channel). If some other basis is used then this model cannot be used and the Hamming metric does not measure the number of errors in transmission, as we want it to.

Generator and check matrices

As a linear subspace of $\mathbb{F}_q^n$, the entire code *C* (which may be very large) may be represented as the span of a minimal set of codewords (known as a basis in linear algebra). These basis codewords are often collated in the rows of a matrix G known as a **generating matrix** for the code *C*. When G has the block matrix form $\boldsymbol{G} = [I_k|P]$, where I_k denotes the $k \times k$ identity matrix and P is some $k \times (n-k)$ matrix, then we say G is in **standard form**.

A matrix *H* representing a linear function $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ whose kernel is *C* is called a **check matrix** of *C* (or sometimes a parity check matrix). Equivalently, *H* is a matrix whose null space is *C*. If *C* is a code with a generating matrix *G* in standard form, $\boldsymbol{G} = [I_k|P]$, then $\boldsymbol{H} = [-P^T|I_{n-k}]$ is a check matrix for C. The code generated by *H* is called the **dual code** of C. It can be verified that G is a $k \times n$ matrix, while H is a $(n-k) \times n$ matrix.

Linearity guarantees that the minimum Hamming distance *d* between a codeword c_0 and any of the other codewords $c \neq c_0$ is independent of c_0. This follows from the property that the difference $c - c_0$ of two codewords in *C* is also a codeword (i.e., an element of the subspace *C*), and the property that $d(c, c_0) = d(c - c_0, 0)$. These properties imply that

$$\min_{c \in C,\ c \neq c_0} d(c, c_0) = \min_{c \in C, c \neq c_0} d(c - c_0, 0) = \min_{c \in C, c \neq 0} d(c, 0) = d.$$

In other words, in order to find out the minimum distance between the codewords of a linear code, one would only need to look at the non-zero codewords. The non-zero codeword with the smallest weight has then the minimum distance to the zero codeword, and hence determines the minimum distance of the code.

The distance *d* of a linear code *C* also equals the minimum number of linearly dependent columns of the check matrix *H*.

Proof: Because $\boldsymbol{H} \cdot \boldsymbol{c}^T = \boldsymbol{0}$, which is equivalent to $\sum_{i=1}^{n} (c_i \cdot \boldsymbol{H_i}) = \boldsymbol{0}$, where $\boldsymbol{H_i}$ is the i^{th} column of $\boldsymbol{H}$. Remove those items with $c_i = 0$, those $\boldsymbol{H_i}$ with $c_i \neq 0$ are linearly dependent. Therefore, d is at least the minimum number of linearly dependent columns. On another hand, consider the minimum set of linearly dependent columns $\{\boldsymbol{H_j} | j \in S\}$ where S is the column index set. $\sum_{i=1}^{n} (c_i \cdot \boldsymbol{H_i}) = \sum_{j \in S} (c_j \cdot \boldsymbol{H_j}) + \sum_{j \notin S} (c_j \cdot \boldsymbol{H_j}) = \boldsymbol{0}$. Now consider the vector $\boldsymbol{c'}$ such that $c_j^{'} = 0$ if $j \notin S$. Note $\boldsymbol{c'} \in C$ because $\boldsymbol{H} \cdot \boldsymbol{c'}^T = \boldsymbol{0}$. Therefore, we have $d \leq wt(\boldsymbol{c'})$, which is the minimum number of linearly dependent columns in $\boldsymbol{H}$. The claimed property is therefore proved.

Example: Hamming codes

As the first class of linear codes developed for error correction purpose, *Hamming codes* have been widely used in digital communication systems. For any positive integer $r \geq 2$, there exists a $[2^r - 1, 2^r - r - 1, 3]_2$ Hamming code. Since $d = 3$, this Hamming code can correct a 1-bit error.

Example : The linear block code with the following generator matrix and parity check matrix is a $[7, 4, 3]_2$ Hamming code.

$$\boldsymbol{G} = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,1 \\ 0\,0\,0\,1\,1\,0\,1 \end{pmatrix}, \boldsymbol{H} = \begin{pmatrix} 1\,0\,1\,1\,1\,0\,0 \\ 1\,1\,1\,0\,0\,1\,0 \\ 0\,1\,1\,1\,0\,0\,1 \end{pmatrix}$$

Example: Hadamard codes

Hadamard code is a $[2^r, r, 2^{r-1}]_2$ linear code and is capable of correcting many errors. Hadamard code could be constructed column by column : the i^{th} column is the bits of the binary representation of integer i, as shown in the following example. Hadamard code has minimum distance 2^{r-1} and therefore can correct $2^{r-2} - 1$ errors.

Example: The linear block code with the following generator matrix is a $[8, 3, 4]_2$ Hadamard code: $\boldsymbol{G}_{Had} = \begin{pmatrix} 0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,0\,1\,1\,0\,0\,1\,1 \\ 0\,1\,0\,1\,0\,1\,0\,1 \end{pmatrix}$.

Hadamard code is a special case of Reed–Muller code. If we take the first column (the all-zero column) out from $\boldsymbol{G}_{Had}$, we get $[7, 3, 4]_2$ *simplex code*, which is the *dual code* of Hamming code.

Nearest neighbor algorithm

The parameter d is closely related to the error correcting ability of the code. The following construction/algorithm illustrates this (called the nearest neighbor decoding algorithm):

Input: A "received vector" v in $\mathbb{F}_q^n$.

Output: A codeword w in C closest to v if any.

- Starting with t=0 repeat the following two steps.
- Enumerate the elements of the ball of (Hamming) radius t around the received word v, denoted B_t(v).
  - For each w in B_t(v), check if w in C. If so, return w as the solution!
- Increment t. Fail when t > (d - 1)/2 so enumeration is complete and no solution has been found.

Note: "fail" is not returned unless $t > (d - 1)/2$. We say that a linear C is t-error correcting if there is at most one codeword in B_t(v), for each v in $\mathbb{F}_q^n$.

Popular notation

Codes in general are often denoted by the letter *C*, and a code of length *n* and of rank *k* (i.e., having *k* code words in its basis and *k* rows in its *generating matrix*) is generally referred to as an (*n*, *k*) code. Linear block codes are frequently denoted as [*n*, *k*, *d*] codes, where *d* refers to the code's minimum Hamming distance between any two code words.

(The [*n*, *k*, *d*] notation should not be confused with the (*n*, *M*, *d*) notation used to denote a *non-linear* code of length *n*, size *M* (i.e., having *M* code words), and minimum Hamming distance *d*.)

Singleton bound

Lemma (Singleton bound): Every linear [n,k,d] code C satisfies $k + d \leq n + 1$.

A code C whose parameters satisfy k+d=n+1 is called **maximum distance separable** or **MDS**. Such codes, when they exist, are in some sense best possible.

If C_1 and C_2 are two codes of length n and if there is a permutation p in the symmetric group S_n for which $(c_1,...,c_n)$ in C_1 if and only if $(c_{p(1)},...,c_{p(n)})$ in C_2, then we say C_1 and C_2 are **permutation equivalent**. In more generality, if there is an $n \times n$ monomial matrix $M\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ which sends C_1 isomorphically to C_2 then we say C_1 and C_2 are **equivalent**.

Lemma: Any linear code is permutation equivalent to a code which is in standard form.

Examples

Some examples of linear codes include:

- Repetition codes
- Parity codes
- Cyclic codes
- Hamming codes
- Golay code, both the binary and ternary versions
- Polynomial codes, of which BCH codes are an example
- Reed–Solomon codes
- Reed–Muller codes
- Goppa codes
- Low-density parity-check codes
- Expander codes
- Multidimensional parity-check codes

Generalization

Hamming spaces over non-field alphabets have also been considered, especially over finite rings (most notably over $\mathbf{Z}_4$) giving rise to modules instead of vector spaces and ring-linear codes (identified with submodules) instead of linear codes. The typical metric used in this case the Lee distance. There exist a Gray isometry between $\mathbb{Z}_2^{2m}$ (i.e. GF(2^{2m})) with the Hamming distance and $\mathbb{Z}_4^m$ (also denoted as GR(4,m)) with the Lee distance; its main attraction is that it establishes a correspondence between some "good" codes that are not linear over $\mathbb{Z}_2^{2m}$ as images of ring-linear codes from $\mathbb{Z}_4^m$.[4][5][6]

More recently, some authors have referred to such codes over rings simply as linear codes as well.[7]

See also

- Decoding methods

References

1. William E. Ryan and Shu Lin (2009). *Channel Codes: Classical and Modern*. Cambridge University Press. p. 4. ISBN 978-0-521-84868-8.
2. MacKay, David, J.C. (2003). *Information Theory, Inference, and Learning Algorithms* (http://www.inference.phy.cam.ac.uk/itprnn/book.pdf) (PDF). Cambridge University Press. p. 9. ISBN 9780521642989. "In a *linear* block code, the extra $N - K$ bits are linear functions of the original K bits; these extra bits are called *parity-check bits*"
3. Thomas M. Cover and Joy A. Thomas (1991). *Elements of Information Theory*. John Wiley & Sons, Inc. pp. 210–211. ISBN 0-471-06259-6.

4. Marcus Greferath (2009). "An Introduction to Ring-Linear Coding Theory". In Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, Carlo Traverso (eds.). *Gröbner Bases, Coding, and Cryptography*. Springer Science & Business Media. ISBN 978-3-540-93806-4.
5. http://www.encyclopediaofmath.org/index.php/Kerdock_and_Preparata_codes
6. J.H. van Lint (1999). *Introduction to Coding Theory* (3rd ed.). Springer. Chapter 8: Codes over $\mathbb{Z}_4$. ISBN 978-3-540-64133-9.
7. S.T. Dougherty, J.-L. Kim, P. Sole (2015). "Open Problems in Coding Theory". In Steven Dougherty, Alberto Facchini, Andre Gerard Leroy, Edmund Puczylowski, Patrick Sole (eds.). *Noncommutative Rings and Their Applications* (https://books.google.com/books?id=psrXBgAAQBAJ&pg=PA80). American Mathematical Soc. p. 80. ISBN 978-1-4704-1032-2.

- J. F. Humphreys; M. Y. Prest (2004). *Numbers, Groups and Codes* (2nd ed.). Cambridge University Press. ISBN 978-0-511-19420-7. Chapter 5 contains a more gentle introduction (than this article) to the subject of linear codes.

External links

- *q*-ary code generator program (http://jason.mchu.com/QCode/index.html)
- Code Tables: Bounds on the parameters of various types of codes (http://www.codetables.de/), *IAKS, Fakultät für Informatik, Universität Karlsruhe (TH)]*. Online, up to date table of the optimal binary codes, includes non-binary codes.
- The database of Z4 codes (http://z4codes.info/) Online, up to date database of optimal Z4 codes.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Linear_code&oldid=871316981"

This page was last edited on 2018-11-30, at 15:00:54.