WIKIPEDIA

Parity-check matrix

In coding theory, a **parity-check matrix** of a linear block code C is a matrix which describes the linear relations that the components of a codeword must satisfy. It can be used to decide whether a particular vector is a codeword and is also used in decoding algorithms.

Contents

Definition

Formally, a parity check matrix, H of a linear code C is a generator matrix of the dual code, $C^{\perp}$. This means that a codeword $\mathbf{c}$ is in C if and only if the matrix-vector product $H\mathbf{c}^{\top} = \mathbf{0}$ (some authors[1] would write this in an equivalent form, $\mathbf{c}H^{\top} = \mathbf{0}$.)

The rows of a parity check matrix are the coefficients of the parity check equations.[2] That is, they show how linear combinations of certain digits (components) of each codeword equal zero. For example, the parity check matrix

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

compactly represents the parity check equations,

$$\begin{aligned} c_3 + c_4 &= 0 \\ c_1 + c_2 &= 0 \end{aligned},$$

that must be satisfied for the vector (c_1, c_2, c_3, c_4) to be a codeword of C.

From the definition of the parity-check matrix it directly follows the minimum distance of the code is the minimum number d such that every d - 1 columns of a parity-check matrix H are linearly independent while there exist d columns of H that are linearly dependent.

Creating a parity check matrix

The parity check matrix for a given code can be derived from its generator matrix (and vice versa).[3] If the generator matrix for an $[n,k]$-code is in standard form

$$G = [I_k | P],$$

then the parity check matrix is given by

$$H = [-P^\top | I_{n-k}],$$

because

$$GH^\top = P - P = 0.$$

Negation is performed in the finite field $\mathbf{F}_q$. Note that if the characteristic of the underlying field is 2 (i.e., 1 + 1 = 0 in that field), as in binary codes, then -P = P, so the negation is unnecessary.

For example, if a binary code has the generator matrix

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right],$$

then its parity check matrix is

$$H = \left[\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

It can be verified that G is a $k \times n$ matrix, while H is a $(n-k) \times n$ matrix.

Syndromes

For any (row) vector $\mathbf{x}$ of the ambient vector space, $\mathbf{s}$ = $H\mathbf{x}^\top$ is called the syndrome of $\mathbf{x}$. The vector $\mathbf{x}$ is a codeword if and only if $\mathbf{s}$ = $\mathbf{0}$. The calculation of syndromes is the basis for the syndrome decoding algorithm.[4]

See also

- Hamming code

Notes

1. for instance, Roman 1992, p. 200
2. Roman 1992, p. 201
3. Pless 1998, p. 9
4. Pless 1998, p. 20

References

- Hill, Raymond (1986). *A first course in coding theory*. Oxford Applied Mathematics and Computing Science Series. Oxford University Press. p. 69. ISBN 0-19-853803-0.
- 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
- J.H. van Lint (1992). *Introduction to Coding Theory*. GTM. **86** (2nd ed.). Springer-Verlag. p. 34. ISBN 3-540-54894-7.