Generator matrix

For generator matrices in probability theory, see transition rate matrix.

In coding theory, a **generator matrix** is a matrix whose rows form a basis for a linear code. The codewords are all of the linear combinations of the rows of this matrix, that is, the linear code is the row space of its generator matrix.

1 Terminology

If **G** is a matrix, it generates the codewords of a linear code *C* by,

$$\mathbf{w} = \mathbf{s}\,\mathbf{G},$$

where **w** is a codeword of the linear code *C*, and **s** is any input vector. Both **w** and **s** are assumed to be row vectors.[1] A generator matrix for a linear $[n,k,d]_q$ -code has format $k \times n$, where *n* is the length of a codeword, *k* is the number of information bits (the dimension of *C* as a vector subspace), *d* is the minimum distance of the code, and *q* is size of the finite field, that is, the number of symbols in the alphabet (thus, *q* = 2 indicates a binary code, etc.). The number of redundant bits is denoted by *r* = *n* - *k*.

The *standard* form for a generator matrix is,[2]

$$G = \begin{bmatrix} I_k | P \end{bmatrix}$$

where I_k is the *k*×*k* identity matrix and P is a *k*×*r* matrix. When the generator matrix is in standard form, the code *C* is systematic in its first *k* coordinate positions.[3]

A generator matrix can be used to construct the parity check matrix for a code (and vice versa). If the generator matrix *G* is in standard form, $G = \begin{bmatrix} I_k | P \end{bmatrix}$, then the parity check matrix for *C* is[4]

$$H = \begin{bmatrix} -P^\top | I_{n-k} \end{bmatrix}$$

where $P^\top$ is the transpose of the matrix P . This is a consequence of the fact that a parity check matrix of C is a generator matrix of the dual code $C^\perp$.

2 Equivalent Codes

Codes C_1 and C_2 are *equivalent* (denoted $C_1 \sim C_2$) if one code can be obtained from the other via the following two transformations:[5]

1. arbitrarily permute the components, and
2. independently scale by a non-zero element any components.

Equivalent codes have the same minimum distance.

The generator matrices of equivalent codes can be obtained from one another via the following elementary operations:[6]

1. permute rows
2. scale rows by a nonzero scalar
3. add rows to other rows
4. permute columns, and
5. scale columns by a nonzero scalar.

Thus, we can perform Gaussian Elimination on *G*. Indeed, this allows us to assume that the generator matrix is in the standard form. More precisely, for any matrix *G* we can find a invertible matrix *U* such that $UG = \begin{bmatrix} I_k | P \end{bmatrix}$, where *G* and $\begin{bmatrix} I_k | P \end{bmatrix}$ generate equivalent codes.

3 See also

- Hamming code (7,4)

4 Notes

[1] MacKay, David, J.C. (2003). *Information Theory, Inference, and Learning Algorithms* (PDF). Cambridge University Press. p. 9. ISBN 9780521642989. Because the Hamming code is a linear code, it can be written compactly in terms of matrices as follows. The transmitted codeword **t** is obtained from the source sequence **s** by a linear operation,

$$\mathbf{t} = \mathbf{G}^\intercal \mathbf{s}$$

where **G** is the *generator matrix* of the code... I have assumed that **s** and **t** are column vectors. If instead they are row vectors, then this equation is replaced by

$$\mathbf{t} = \mathbf{sG}$$

... I find it easier to relate to the right-multiplication (...) than the left-multiplication (...). Many coding theory texts use the left-multiplying conventions (...), however. ...The rows of the generator matrix can be viewed as defining the basis vectors.

[2] Ling & Xing 2004, p. 52

[3] Roman 1992, p. 198

[4] Roman 1992, p. 200

[5] Pless 1998, p. 8

[6] Welsh 1988, pp. 54-55

5 References

- Ling, San; Xing, Chaoping (2004), *Coding Theory / A First Course*, Cambridge University Press, ISBN 0-521-52923-9
- 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
- Welsh, Dominic (1988), *Codes and Cryptography*, Oxford University Press, ISBN 0-19-853287-3

6 Further reading

- MacWilliams, F.J.; Sloane, N.J.A. (1977), *The Theory of Error-Correcting Codes*, North-Holland, ISBN 0-444-85193-3

7 External links

- Generator Matrix at MathWorld

8 Text and image sources, contributors, and licenses

8.1 Text

- **Generator matrix** *Source:* https://en.wikipedia.org/wiki/Generator_matrix?oldid=750422475 *Contributors:* Billymac00, Culix, RussBot, Gareth Jones, SmackBot, Bluebot, MaxSem, MrZap, P.L.A.R., JAnDbot, LordAnubisBOT, Peskydan, Gamall Wednesday Ida, Addbot, Luckas-bot, Cunchem, ArthurBot, John of Reading, Wcherowi, Frietjes, Theoneandonlysigma, Mark viking and Anonymous: 12

8.2 Images

8.3 Content license