no arrowhead is used:

x ----- xa

for if $a = a^{-1}$, then multiplying by a is the same as multiplying by a^{-1}.

The Cayley diagram of a group contains the same information as the group's table. For instance, to find the product $(ab)(ab^2)$ in the figure on page 51, we start at ab and follow the path corresponding to ab^2 (multiplying by a, then by b, then again by b), which is

●-----●—→—●—→—●

This path leads to b; hence $(ab)(ab^2) = b$.

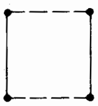
As another example, the inverse of ab^2 is the path which leads from ab^2 back to e. We note instantly that this is ba.

A point-and-arrow diagram is the Cayley diagram of a group iff it has the following two properties: (a) For each point x and generator a, there is exactly one a-arrow starting at x, and exactly one a-arrow ending at x; furthermore, at most one arrow goes from x to another point y. (b) If two different paths starting at x lead to the same destination, then these two paths, starting at any point y, lead to the same destination.

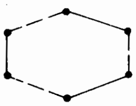
Cayley diagrams are a useful way of finding new groups.

Write the table of the groups having the following Cayley diagrams: (REMARK: You may take any point to represent e, because there is perfect symmetry in a Cayley diagram. Choose e, then label the diagram and proceed.)

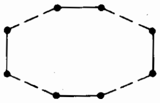
1



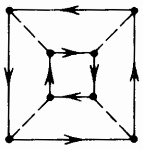
2



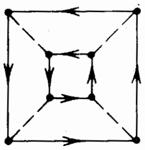
3



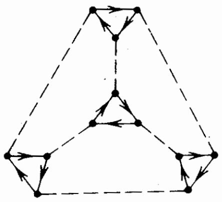
4



5



6



H. Coding Theory: Generator Matrix and Parity-Check Matrix of a Code

For the reader who does not know the subject, linear algebra will be developed in Chapter 28. However, some rudiments of vector and matrix multiplication will be needed in this exercise; they are given here:

A *vector* with n components is a sequence of n numbers: $(a_1, a_2, \ldots, a_n)$. The *dot product* of two vectors with n components, say the vectors $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$, is defined by

$$\mathbf{a} \cdot \mathbf{b} = (a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

that is, you multiply corresponding components and add. For example,

$$(1, 4, -2, 3) \cdot (6, 2, 4, -2) = 1(6) + 4(2) + (-2)4 + 3(-2) = 0$$

When $\mathbf{a} \cdot \mathbf{b} = 0$, as in the last example, we say that $\mathbf{a}$ and $\mathbf{b}$ are *orthogonal*.

A *matrix* is a rectangular array of numbers. An "m by n matrix" ($m \times n$ matrix) has m rows and n columns. For example,

$$\mathbf{B} = \begin{pmatrix} 1 & 2 & -2 & 3 \\ 4 & 1 & 1 & -3 \\ 7 & 2 & 5 & -1 \end{pmatrix}$$

is a 3×4 matrix: It has three rows and four columns. Notice that each row of $\mathbf{B}$ is a vector with four components, and each column of $\mathbf{B}$ is a vector with three components.

If $\mathbf{A}$ is any $m \times n$ matrix, let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ be the *columns* of $\mathbf{A}$. (Each column of $\mathbf{A}$ is a vector with m components.) If $\mathbf{x}$ is any vector with m components, $\mathbf{xA}$ denotes the vector

$$\mathbf{xA} = (\mathbf{x} \cdot \mathbf{a}_1, \mathbf{x} \cdot \mathbf{a}_2, \ldots, \mathbf{x} \cdot \mathbf{a}_n)$$

That is, the components of $\mathbf{xA}$ are obtained by dot multiplying $\mathbf{x}$ by the successive columns of $\mathbf{A}$. For example, if $\mathbf{B}$ is the matrix of the previous paragraph and $\mathbf{x} = (3, 1, -2)$, then the components of $\mathbf{xB}$ are

$$(3, 1, -2) \cdot (1, 4, 7) = -7$$
$$(3, 1, -2) \cdot (2, 1, 2) = 3$$
$$(3, 1, -2) \cdot (-2, 1, 5) = -15$$
$$(3, 1, -2) \cdot (3, -3, -1) = 8$$

that is, $\mathbf{xB} = (-7, 3, -15, 8)$.

If $\mathbf{A}$ is an $m \times n$ matrix, let $\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \ldots, \mathbf{a}^{(m)}$ be the *rows* of A. If $\mathbf{y}$ is any vector with n components, $\mathbf{Ay}$ denotes the vector

$$\mathbf{Ay} = (\mathbf{y} \cdot \mathbf{a}^{(1)}, \mathbf{y} \cdot \mathbf{a}^{(2)}, \ldots, \mathbf{y} \cdot \mathbf{a}^{(m)})$$

That is, the components of $\mathbf{Ay}$ are obtained by dot multiplying $\mathbf{y}$ with the successive *rows* of $\mathbf{A}$. (Clearly, $\mathbf{Ay}$ is not the same as $\mathbf{yA}$.) From linear algebra, $\mathbf{A}(\mathbf{x} + \mathbf{y}) = \mathbf{Ax} + \mathbf{Ay}$ and $(\mathbf{A} + \mathbf{B})\mathbf{x} = \mathbf{Ax} + \mathbf{Bx}$.

We shall now continue the discussion of codes begun in Exercises F and G of Chapter 3. Recall that $\mathbb{B}^n$ is the set of all vectors of length n whose entries are 0s and 1s. In Exercise F, page 32, it was shown that $\mathbb{B}^n$ is a group. A *code* is defined to be any subset C of $\mathbb{B}^n$. A code is called a *group code* if C is a *subgroup* of $\mathbb{B}^n$. The codes described in Chapter 3, as well as all those to be mentioned in this exercise, are group codes.

An $m \times n$ matrix $\mathbf{G}$ is a *generator matrix* for the code C if C is the group generated by the rows of $\mathbf{G}$. For example, if C_1 is the code given on page 34, its generator matrix is

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

You may check that all eight codewords of C_1 are sums of the rows of $\mathbf{G}_1$.

Recall that every codeword consists of information digits and parity-check digits. In the code C_1 the first three digits of every codeword are information digits, and make up the *message*; the last two digits are parity-check digits. *Encoding* a message is the process of adding the parity-check digits to the end of the message. If $\mathbf{x}$ is a message, then $E(\mathbf{x})$ denotes the encoded word. For example, recall that in C_1 the parity-check equations are $a_4 = a_1 + a_3$ and $a_5 = a_1 + a_2 + a_3$. Thus, a three-digit message $a_1a_2a_3$ is encoded as follows:

$$E(a_1, a_2, a_3) = (a_1, a_2, a_3, a_1 + a_3, a_1 + a_2 + a_3)$$

The two digits added at the end of a word are those dictated by the parity check equations. You may verify that

$$E(a_1, a_2, a_3) = (a_1, a_2, a_3)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \text{[Dot multiply } (a_1, a_2, a_3) \text{ by the successive columns of } \mathbf{G}_1\text{.]}$$

$$= (a_1, a_2, a_3, a_1 + a_3, a_1 + a_2 + a_3)$$

This is true in all cases: If $\mathbf{G}$ is the generator matrix of a code and $\mathbf{x}$ is a message, then $E(\mathbf{x})$ is equal to the product $\mathbf{xG}$. Thus, encoding using the generator matrix is very easy: you simply multiply the message $\mathbf{x}$ by the generator matrix $\mathbf{G}$.

Now, the parity-check equations of C_1 (namely, $a_4 = a_1 + a_3$ and $a_5 = a_1 + a_2 + a_3$) can be written in the form

$$a_1 + a_3 + a_4 = 0 \qquad \text{and} \qquad a_1 + a_2 + a_3 + a_5 = 0$$

which is equivalent to

$$(a_1, a_2, a_3, a_4, a_5) \cdot (1, 0, 1, 1, 0) = 0$$

and

$$(a_1, a_2, a_3, a_4, a_5) \cdot (1, 1, 1, 0, 1) = 0$$

The last two equations show that a word $a_1a_2a_3a_4a_5$ is a codeword (that is, satisfies the parity-check equations) if and only if $(a_1, a_2, a_3, a_4, a_5)$ is orthogonal to both rows of the matrix:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$\mathbf{H}$ is called the *parity-check matrix* of the code C_1. This conclusion may be stated as a theorem:

Theorem 1 *Let* $\mathbf{H}$ *be the parity-check matrix of a code* C *in* $\mathbb{B}^n$. *A word* $\mathbf{x}$ *in* $\mathbb{B}^n$ *is a codeword if and only if* $\mathbf{Hx} = 0$.

(Remember that **Hx** is obtained by dot multiplying **x** by the rows of **H**.)

1 Find the generator matrix $\mathbf{G}_2$ and the parity-check matrix $\mathbf{H}_2$ of the code C_2 described in Exercise G2 of Chapter 3.

2 Let C_3 be the following code in $\mathbb{B}^7$: the first four positions are information positions, and the parity-check equations are $a_5 = a_2 + a_3 + a_4$, $a_6 = a_1 + a_3 + a_4$, and $a_7 = a_1 + a_2 + a_4$. (C_3 is called the *Hamming code*.) Find the generator matrix $\mathbf{G}_3$ and parity-check matrix $\mathbf{H}_3$ of C_3.

The *weight* of a word **x** is the number of 1s in the word and is denoted by $w(\mathbf{x})$. For example, $w(11011) = 4$. The *minimum weight* of a code C is the weight of the nonzero codeword of smallest weight in the code. (See the definitions of "distance" and "minimum distance" on page 34.) Prove the following:

# **3** $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$.

4 $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, where **0** is the word whose digits are all 0s.

5 The minimum distance of a group code C is equal to the minimum weight of C.

6 (*a*) If **x** and **y** have even weight, so does $\mathbf{x} + \mathbf{y}$.

(*b*) If **x** and **y** have odd weight, $\mathbf{x} + \mathbf{y}$ has even weight.

(*c*) If **x** has odd and **y** has even weight, then $\mathbf{x} + \mathbf{y}$ has odd weight.

7 In any group code, either all the words have even weight, or half the words have even weight and half the words have odd weight. (Use part 6 in your proof.)

8 $\mathbf{H}(\mathbf{x} + \mathbf{y}) = 0$ if and only if $\mathbf{Hx} = \mathbf{Hy}$, where **H** denotes the parity-check matrix of a code in $\mathbb{B}^n$ and **x** and **y** are any two words in $\mathbb{B}^n$).