10.15 Cryptography

In this section we present a method of encoding and decoding messages. We also examine modular arithmetic and show how Gaussian elimination can sometimes be used to break an opponent's code.

Prerequisites

Matrices
Gaussian Elimination
Matrix Operations
Linear Independence
Linear Transformations (Section 4.9)

Ciphers

The study of encoding and decoding secret messages is called ***cryptography***. Although secret codes date to the earliest days of written communication, there has been a recent surge of interest in the subject because of the need to maintain the privacy of information transmitted over public lines of communication. In the language of cryptography, codes are called ***ciphers***, uncoded messages are called ***plaintext***, and coded messages are called ***ciphertext***. The process of converting from plaintext to ciphertext is called ***enciphering***, and the reverse process of converting from ciphertext to plaintext is called ***deciphering***.

The simplest ciphers, called ***substitution ciphers***, are those that replace each letter of the alphabet by a different letter. For example, in the substitution cipher

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

the plaintext letter A is replaced by D, the plaintext letter B by E, and so forth. With this cipher the plaintext message

$$ROME\ WAS\ NOT\ BUILT\ IN\ A\ DAY$$

becomes

$$URPH\ ZDV\ QRW\ EX\ LOW\ LQ\ D\ GDB$$

Hill Ciphers

A disadvantage of substitution ciphers is that they preserve the frequencies of individual letters, making it relatively easy to break the code by statistical methods. One way to overcome this problem is to divide the plaintext into groups of letters and encipher the plaintext group by group, rather than one letter at a time. A system of cryptography in which the plaintext is divided into sets of n letters, each of which is replaced by a set of n cipher letters, is called a ***polygraphic system***. In this section we will study a class of polygraphic systems based on matrix transformations. [The ciphers that we will discuss are called ***Hill ciphers*** after Lester S. Hill, who introduced them in two papers: “Cryptography in an Algebraic Alphabet,” *American Mathematical Monthly, 36* (June–July 1929), pp. 306–312; and “Concerning Certain Linear Transformation Apparatus of Cryptography,” *American Mathematical Monthly, 38* (March 1931), pp. 135–154.]

In the discussion to follow, we assume that each plaintext and ciphertext letter except Z is assigned the numerical value that specifies its position in the standard alphabet (Table 1). For reasons that will become clear later, Z is assigned a value of zero.

Table 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

In the simplest Hill ciphers, successive *pairs* of plaintext are transformed into ciphertext by the following procedure:

Step 1 Choose a 2×2 matrix with integer entries

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

to perform the encoding. Certain additional conditions on A will be imposed later.

Step 2 Group successive plaintext letters into pairs, adding an arbitrary "dummy" letter to fill out the last pair if the plaintext has an odd number of letters, and replace each plaintext letter by its numerical value.

Step 3 Successively convert each plaintext pair p_1p_2 into a column vector

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

and form the product $A\mathbf{p}$. We will call p a ***plaintext vector*** and $A\mathbf{p}$ the corresponding ***ciphertext vector***.

Step 4 Convert each ciphertext vector into its alphabetic equivalent.

EXAMPLE 1 Hill Cipher of a Message

Use the matrix

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

to obtain the Hill cipher for the plaintext message

$$I\,AM\;HIDING$$

Solution If we group the plaintext into pairs and add the dummy letter G to fill out the last pair, we obtain

$$IA \quad MH \quad ID \quad IN \quad GG$$

or, equivalently, from Table 1,

$$9\,1 \quad 13\,8 \quad 9\,4 \quad 9\,14 \quad 7\,7$$

To encipher the pair IA, we form the matrix product

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

which, from Table 1, yields the ciphertext KC.

To encipher the pair MH, we form the product

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 8 \end{bmatrix} = \begin{bmatrix} 29 \\ 24 \end{bmatrix}$$

However, there is a problem here, because the number 29 has no alphabet equivalent (Table 1). To resolve this problem, we make the following agreement:

Whenever an integer greater than 25 occurs, it will be replaced by the remainder that results when this integer is divided by 26.

Because the remainder after division by 26 is one of the integers 0, 1, 2, ..., 25, this procedure will always yield an integer with an alphabet equivalent.

Thus, in 1 we replace 29 by 3, which is the remainder after dividing 29 by 26. It now follows from Table 1 that the ciphertext for the pair *MH* is *CX*.

The computations for the remaining ciphertext vectors are

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}9\\4\end{bmatrix} = \begin{bmatrix}17\\12\end{bmatrix}$$

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}9\\14\end{bmatrix} = \begin{bmatrix}37\\42\end{bmatrix} \text{ or } \begin{bmatrix}11\\16\end{bmatrix}$$

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}\begin{bmatrix}7\\7\end{bmatrix} = \begin{bmatrix}21\\21\end{bmatrix}$$

These correspond to the ciphertext pairs *QL*, *KP*, and *UU*, respectively. In summary, the entire ciphertext message is

KC CX QL KP UU

which would usually be transmitted as a single string without spaces:

KCCXQLKPUU

Because the plaintext was grouped in pairs and enciphered by a 2×2 matrix, the Hill cipher in Example 1 is referred to as a ***Hill 2-cipher***. It is obviously also possible to group the plaintext in triples and encipher by a 3×3 matrix with integer entries; this is called a ***Hill 3-cipher***. In general, for a ***Hill n-cipher***, plaintext is grouped into sets of *n* letters and enciphered by an $n \times n$ matrix with integer entries.

Modular Arithmetic

In Example 1, integers greater than 25 were replaced by their remainders after division by 26. This technique of working with remainders is at the core of a body of mathematics called *modular arithmetic*. Because of its importance in cryptography, we will digress for a moment to touch on some of the main ideas in this area.

In modular arithmetic we are given a positive integer *m*, called the ***modulus***, and any two integers whose difference is an integer multiple of the modulus are regarded as "equal" or "equivalent" with respect to the modulus. More precisely, we make the following definition.

DEFINITION 1

If *m* is a positive integer and *a* and *b* are any integers, then we say that *a* is ***equivalent*** to *b* modulo *m*, written

$$a = b \pmod{m}$$

if $a - b$ is an integer multiple of *m*.

EXAMPLE 2 Various Equivalences

$$\begin{aligned} 7 &= 2 \pmod 5 \\ 19 &= 3 \pmod 2 \\ -1 &= 25 \pmod{26} \\ 12 &= 0 \pmod 4 \end{aligned}$$

For any modulus m it can be proved that every integer a is equivalent, modulo m, to exactly one of the integers

$$0, 1, 2, \ldots, m-1$$

We call this integer the ***residue*** of a modulo m, and we write

$$Z_m = \{0, 1, 2, \ldots, m-1\}$$

to denote the set of residues modulo m.

If a is a *nonnegative* integer, then its residue modulo m is simply the remainder that results when a is divided by m. For an arbitrary integer a, the residue can be found using the following theorem.

THEOREM 10.15.1

For any integer a and modulus m, let

$$R = \textit{remainder of } \frac{|a|}{m}$$

Then the residue r of a modulo m is given by

$$r = \begin{cases} R & \text{if } a \geq 0 \\ m - R & \text{if } a < 0 \text{ and } R \neq 0 \\ 0 & \text{if } a < 0 \text{ and } R = 0 \end{cases}$$

EXAMPLE 3 Residues mod 26

Find the residue modulo 26 of (a) 87, (b) -38, and (c) -26.

Solution

(a) Dividing $|87| = 87$ by 26 yields a remainder of $R = 9$, so $r = 9$. Thus,

$$87 = 9 \pmod{26}$$

(b) Dividing $|-38| = 38$ by 26 yields a remainder of $R = 12$, so $r = 26 - 12 = 14$. Thus,

$$-38 = 14 \pmod{26}$$

(c) Dividing $|-26| = 26$ by 26 yields a remainder of $R = 0$. Thus,

$$-26 = 0 \pmod{26}$$

In ordinary arithmetic every nonzero number a has a *reciprocal* or *multiplicative inverse*, denoted by a^{-1}, such that

$$aa^{-1} = a^{-1}a = 1$$

In modular arithmetic we have the following corresponding concept:

DEFINITION 2

If a is a number in Z_m, then a number a^{-1} in Z_m is called a ***reciprocal*** or ***multiplicative inverse*** of a modulo m if $aa^{-1} = a^{-1}a = 1 \pmod{m}$.

It can be proved that if a and m have no common prime factors, then a has a unique reciprocal modulo m; conversely, if a and m have a common prime factor, then a has no reciprocal modulo m.

EXAMPLE 4 Reciprocal of 3 mod 26 ◀

The number 3 has a reciprocal modulo 26 because 3 and 26 have no common prime factors. This reciprocal can be obtained by finding the number x in Z_{26} that satisfies the modular equation

$$3x = 1 \pmod{26}$$

Although there are general methods for solving such modular equations, it would take us too far afield to study them. However, because 26 is relatively small, this equation can be solved by trying the possible solutions, 0 to 25, one at a time. With this approach we find that $x = 9$ is the solution, because

$$3 \cdot 9 = 27 = 1 \pmod{26}$$

Thus,

$$3^{-1} = 9 \pmod{26}$$

EXAMPLE 5 A Number with No Reciprocal mod 26 ◀

The number 4 has no reciprocal modulo 26, because 4 and 26 have 2 as a common prime factor (see Exercise 8).

For future reference, in Table 2 we provide the following reciprocals modulo 26:

Table 2 Reciprocals Modulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Deciphering

Every useful cipher must have a procedure for decipherment. In the case of a Hill cipher, decipherment uses the inverse (mod 26) of the enciphering matrix. To be precise, if m is a positive integer, then a square matrix A with entries in Z_m is said to be ***invertible modulo m*** if there is a matrix B with entries in Z_m such that

$$AB = BA = I \pmod{m}$$

Suppose now that

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

is invertible modulo 26 and this matrix is used in a Hill 2-cipher. If

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \tag{1}$$

is a plaintext vector, then

$$\mathbf{c} = A\mathbf{p} \pmod{26}$$

is the corresponding ciphertext vector and

$$\mathbf{p} = A^{-1}\mathbf{c} \pmod{26}$$

Thus, each plaintext vector can be recovered from the corresponding ciphertext vector by multiplying it on the left by $A^{-1} \pmod{26}$.

In cryptography it is important to know which matrices are invertible modulo 26 and how to obtain their inverses. We now investigate these questions.

In ordinary arithmetic, a square matrix A is invertible if and only if $\det(A) \neq 0$, or, equivalently, if and only if $\det(A)$ has a reciprocal. The following theorem is the analog of this result in modular arithmetic.

THEOREM 10.15.2

A square matrix A with entries in Z_m is invertible modulo m if and only if the residue of $\det(A)$ modulo m has a reciprocal modulo m.

Because the residue of $\det(A)$ modulo m will have a reciprocal modulo m if and only if this residue and m have no common prime factors, we have the following corollary.

COROLLARY 10.15.3

A square matrix A with entries in Z_m is invertible modulo m if and only if m and the residue of $\det(A)$ modulo m have no common prime factors.

Because the only prime factors of $m = 26$ are 2 and 13, we have the following corollary, which is useful in cryptography.

COROLLARY 10.15.4

A square matrix A with entries in Z_{26} is invertible modulo 26 if and only if the residue of $\det(A)$ modulo 26 is not divisible by 2 or 13.

We leave it for you to verify that if

$$A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

has entries in Z_{26} and the residue of $\det(A)=ad-bc$ modulo 26 is not divisible by 2 or 13, then the inverse of A (mod 26) is given by

$$A^{-1}=(ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26} \tag{2}$$

where $(ad-bc)^{-1}$ is the reciprocal of the residue of $ad-bc$ (mod 26).

EXAMPLE 6 Inverse of a Matrix mod 26

Find the inverse of

$$A=\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

modulo 26.

Solution

$$\det(A)=ad-bc=5\cdot 3-6\cdot 2=3$$

so from Table 2,

$$(ad-bc)^{-1}=3^{-1}=9 \pmod{26}$$

Thus, from 2,

$$A^{-1}=9\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix}=\begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix}=\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \pmod{26}$$

As a check,

$$AA^{-1}=\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}=\begin{bmatrix} 53 & 234 \\ 26 & 105 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

Similarly, $A^{-1}A=I$.

EXAMPLE 7 Decoding a Hill 2-Cipher

Decode the following Hill 2-cipher, which was enciphered by the matrix in Example 6:

$$GTNKGKDUSK$$

Solution From Table 1 the numerical equivalent of this ciphertext is

$$7\ 20 \quad 14\ 11 \quad 7\ 11 \quad 4\ 21 \quad 19\ 11$$

To obtain the plaintext pairs, we multiply each ciphertext vector by the inverse of A (obtained in Example 6):

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}7\\ 20\end{bmatrix} = \begin{bmatrix}487\\ 436\end{bmatrix} = \begin{bmatrix}19\\ 20\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}14\\ 11\end{bmatrix} = \begin{bmatrix}278\\ 321\end{bmatrix} = \begin{bmatrix}18\\ 9\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}7\\ 11\end{bmatrix} = \begin{bmatrix}271\\ 265\end{bmatrix} = \begin{bmatrix}11\\ 5\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}4\\ 21\end{bmatrix} = \begin{bmatrix}508\\ 431\end{bmatrix} = \begin{bmatrix}14\\ 15\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}19\\ 11\end{bmatrix} = \begin{bmatrix}283\\ 361\end{bmatrix} = \begin{bmatrix}23\\ 23\end{bmatrix} \pmod{26}$$

From Table 1, the alphabet equivalents of these vectors are

$$ST \quad RI \quad KE \quad NO \quad WW$$

which yields the message

$$STRIKE\,NOW$$

Breaking a Hill Cipher

Because the purpose of enciphering messages and information is to prevent “opponents” from learning their contents, cryptographers are concerned with the *security* of their ciphers—that is, how readily they can be broken (deciphered by their opponents). We will conclude this section by discussing one technique for breaking Hill ciphers.

Suppose that you are able to obtain some corresponding plaintext and ciphertext from an opponent's message. For example, on examining some intercepted ciphertext, you may be able to deduce that the message is a letter that begins *DEAR SIR*. We will show that with a small amount of such data, it may be possible to determine the deciphering matrix of a Hill code and consequently obtain access to the rest of the message.

It is a basic result in linear algebra that a linear transformation is completely determined by its values at a basis. This principle suggests that if we have a Hill n-cipher, and if

$$\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$$

are linearly independent plaintext vectors whose corresponding ciphertext vectors

$$A\mathbf{p}_1, A\mathbf{p}_2, \ldots, A\mathbf{p}_n$$

are known, then there is enough information available to determine the matrix A and hence $A^{-1} \pmod{m}$.

The following theorem, whose proof is discussed in the exercises, provides a way to do this.

THEOREM 10.15.5 Determining the Deciphering Matrix

Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ be linearly independent plaintext vectors, and let $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ be the corresponding ciphertext vectors in a Hill n-cipher. If

$$P = \begin{bmatrix} \mathbf{p}_1^T \\ \mathbf{p}_2^T \\ \vdots \\ \mathbf{p}_n^T \end{bmatrix}$$

is the $n \times n$ matrix with row vectors $\mathbf{p}_1^T, \mathbf{p}_2^T, \ldots, \mathbf{p}_n^T$ and if

$$C = \begin{bmatrix} \mathbf{c}_1^T \\ \mathbf{c}_2^T \\ \vdots \\ \mathbf{c}_n^T \end{bmatrix}$$

is the $n \times n$ matrix with row vectors $\mathbf{c}_1^T, \mathbf{c}_2^T, \ldots, \mathbf{c}_n^T$, then the sequence of elementary row operations that reduces C to I transforms P to $(A^{-1})^T$.

This theorem tells us that to find the transpose of the deciphering matrix A^{-1}, we must find a sequence of row operations that reduces C to I and then perform this same sequence of operations on P. The following example illustrates a simple algorithm for doing this.

EXAMPLE 8 Using Theorem 10.15.5

The following Hill 2-cipher is intercepted:

$$IOSBTGX\ ESPX\ HOPDE$$

Decipher the message, given that it starts with the word *DEAR*.

Solution From Table 1, the numerical equivalent of the known plaintext is

DE	*AR*
4 5	1 18

and the numerical equivalent of the corresponding ciphertext is

IO	*SB*
9 15	19 2

so the corresponding plaintext and ciphertext vectors are

$$\mathbf{p}_1 = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \leftrightarrow \mathbf{c}_1 = \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

$$\mathbf{p}_2 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \leftrightarrow \mathbf{c}_2 = \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

We want to reduce

$$C = \begin{bmatrix} \mathbf{c}_1^T \\ \mathbf{c}_2^T \end{bmatrix} = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}$$

to I by elementary row operations and simultaneously apply these operations to

$$P = \begin{bmatrix} \mathbf{p}_1^T \\ \mathbf{p}_2^T \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix}$$

to obtain $(A^{-1})^T$ (the transpose of the deciphering matrix). This can be accomplished by adjoining *P* to the right of *C* and applying row operations to the resulting matrix $[C|P]$ until the left side is reduced to *I*. The final matrix will then have the form $[I|(A^{-1})^T]$. The computations can be carried out as follows:

$$\left[\begin{array}{cc|cc} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{array}\right]$$ ← We formed the matrix $[C|P]$.

$$\left[\begin{array}{cc|cc} 1 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right]$$ ← We multiplied the first row by $9^{-1} = 3$.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right]$$ ← We replaced 45 by its residue modulo 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{array}\right]$$ ← We added -19 times the first row to the second.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 5 & 7 & 19 \end{array}\right]$$ ← We replaced the entries in the second row by their residues modulo 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 147 & 399 \end{array}\right]$$ ← We multiplied the second row by $5^{-1} = 21$.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{array}\right]$$ ← We replaced the entries in the second row by their residues modulo 26.

$$\left[\begin{array}{cc|cc} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{array}\right]$$ ← We added -19 times the second row to the first.

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{array}\right]$$ ← We replaced the entries in the first row by their residues modulo 26.

Thus,

$$(A^{-1})^T = \begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix}$$

so the deciphering matrix is

$$A^{-1} = \begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}$$

To decipher the message, we first group the ciphertext into pairs and find the numerical equivalent of each letter:

IO	*SB*	*TG*	*XE*	*SP*	*XH*	*OP*	*DE*
9 15	19 2	20 7	24 5	19 16	24 8	15 16	4 5

Next, we multiply successive ciphertext vectors on the left by A^{-1} and find the alphabet equivalents of the resulting plaintext pairs:

$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}9\\15\end{bmatrix} = \begin{bmatrix}4\\5\end{bmatrix}\ D\ E$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}19\\2\end{bmatrix} = \begin{bmatrix}1\\18\end{bmatrix}\ A\ R$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}20\\7\end{bmatrix} = \begin{bmatrix}9\\11\end{bmatrix}\ I\ K$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}24\\5\end{bmatrix} = \begin{bmatrix}5\\19\end{bmatrix}\ E\ S \pmod{26}$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}19\\16\end{bmatrix} = \begin{bmatrix}5\\14\end{bmatrix}\ E\ N$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}24\\8\end{bmatrix} = \begin{bmatrix}4\\20\end{bmatrix}\ D\ T$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}15\\16\end{bmatrix} = \begin{bmatrix}1\\14\end{bmatrix}\ A\ N$$
$$\begin{bmatrix}1 & 17\\0 & 9\end{bmatrix}\begin{bmatrix}4\\5\end{bmatrix} = \begin{bmatrix}11\\19\end{bmatrix}\ K\ S$$

Finally, we construct the message from the plaintext pairs:

DE AR IK ES EN DT AN KS

DEAR IKE SEND TANKS

Further Readings

Readers interested in learning more about mathematical cryptography are referred to the following books, the first of which is elementary and the second more advanced.

1. Abraham Sinkov, *Elementary Cryptanalysis, a Mathematical Approach* (Mathematical Association of America, 2009).

2. Alan G. Konheim, *Cryptography, a Primer* (New York: Wiley-Interscience, 1981).

Exercise Set 10.15

1. Obtain the Hill cipher of the message

DARK NIGHT

for each of the following enciphering matrices:

(a) $\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}$

(b) $\begin{bmatrix}4 & 3\\1 & 2\end{bmatrix}$

Answer:

(a) *GIYUOKEVBH*

(b) *SFANEFZWJH*

2. In each part determine whether the matrix is invertible modulo 26. If so, find its inverse modulo 26 and check your work by verifying that $AA^{-1} = A^{-1}A = I \pmod{26}$.

(a) $A = \begin{bmatrix} 9 & 1 \\ 7 & 2 \end{bmatrix}$

(b) $A = \begin{bmatrix} 3 & 1 \\ 5 & 3 \end{bmatrix}$

(c) $A = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix}$

(d) $A = \begin{bmatrix} 2 & 1 \\ 1 & 7 \end{bmatrix}$

(e) $A = \begin{bmatrix} 3 & 1 \\ 6 & 2 \end{bmatrix}$

(f) $A = \begin{bmatrix} 1 & 8 \\ 1 & 3 \end{bmatrix}$

Answer:

(a) $A^{-1} = \begin{bmatrix} 12 & 7 \\ 23 & 15 \end{bmatrix}$

(b) Not invertible

(c) $A^{-1} = \begin{bmatrix} 1 & 19 \\ 23 & 24 \end{bmatrix}$

(d) Not invertible

(e) Not invertible

(f) $A^{-1} = \begin{bmatrix} 15 & 12 \\ 21 & 5 \end{bmatrix}$

3. Decode the message

$$SAKNOXAOJX$$

given that it is a Hill cipher with enciphering matrix

$$\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$$

Answer:

WE LOVE MATH

4. A Hill 2-cipher is intercepted that starts with the pairs

$$SL\ HK$$

Find the deciphering and enciphering matrices, given that the plaintext is known to start with the word *ARMY*.

Answer:

$$\text{Deciphering matrix} = \begin{bmatrix} 7 & 15 \\ 6 & 5 \end{bmatrix};\ \text{enciphering matrix} = \begin{bmatrix} 7 & 5 \\ 2 & 15 \end{bmatrix}$$

5. Decode the following Hill 2-cipher if the last four plaintext letters are known to be *ATOM*.

LNGIHGYBVRENJYQO

Answer:

THEY SPLIT THE ATOM

6. Decode the following Hill 3-cipher if the first nine plaintext letters are *IHAVECOME*:

HPAFQGGDUGDDHPGODYNOR

Answer:

I HAVE COME TO BURY CAESAR

7. All of the results of this section can be generalized to the case where the plaintext is a binary message; that is, it is a sequence of 0's and 1's. In this case we do all of our modular arithmetic using modulus 2 rather than modulus 26. Thus, for example, $1 + 1 = 0 \pmod 2$. Suppose we want to encrypt the message 110101111. Let us first break it into triplets to form the three vectors $\begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}$, and let us take $\begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\\1 & 1 & 1\end{bmatrix}$ as our enciphering matrix.

(a) Find the encoded message.

(b) Find the inverse modulo 2 of the enciphering matrix, and verify that it decodes your encoded message.

Answer:

(a) 010110001

(b) $\begin{bmatrix}0 & 1 & 1\\1 & 1 & 1\\1 & 0 & 1\end{bmatrix}$

8. If, in addition to the standard alphabet, a period, comma, and question mark were allowed, then 29 plaintext and ciphertext symbols would be available and all matrix arithmetic would be done modulo 29. Under what conditions would a matrix with entries in Z_{29} be invertible modulo 29?

Answer:

A is invertible modulo 29 if and only if $\det(A) \neq 0 \pmod{29}$.

9. Show that the modular equation $4x = 1 \pmod{26}$ has no solution in Z_{26} by successively substituting the values $x = 0, 1, 2, \ldots, 25$.

10. (a) Let P and C be the matrices in Theorem 10.15.5. Show that $P = C(A^{-1})^T$.

(b) To prove Theorem 10.15.5, let $E_1, E_2, \ldots, E_n$ be the elementary matrices that correspond to the row operations that reduce C to I, so

$$E_n \cdots E_2 E_1 C = I$$

Show that

$$E_n \cdots E_2 E_1 P = (A^{-1})^T$$

from which it follows that the same sequence of row operations that reduces C to I converts P to $(A^{-1})^T$.

11. (a) If A is the enciphering matrix of a Hill n-cipher, show that

$$A^{-1} = (C^{-1}P)^T \pmod{26}$$

where C and P are the matrices defined in Theorem 10.15.5.

(b) Instead of using Theorem 10.15.5 as in the text, find the deciphering matrix A^{-1} of Example 8 by using the result in part (a) and Equation 2 to compute C^{-1}. [*Note:* Although this method is practical for Hill 2-ciphers, Theorem 10.15.5 is more efficient for Hill *n*-ciphers with $n > 2$.]

Section 10.15 Technology Exercises

The following exercises are designed to be solved using a technology utility. Typically, this will be MATLAB, *Mathematica*, Maple, Derive, or Mathcad, but it may also be some other type of linear algebra software or a scientific calculator with some linear algebra capabilities. For each exercise you will need to read the relevant documentation for the particular utility you are using. The goal of these exercises is to provide you with a basic proficiency with your technology utility. Once you have mastered the techniques in these exercises, you will be able to use your technology utility to solve many of the problems in the regular exercise sets.

T1. Two integers that have no common factors (except 1) are said to be relatively prime. Given a positive integer *n*, let $S_n = \{a_1, a_2, a_3, \ldots, a_m\}$, where $a_1 < a_2 < a_3 < \ldots < a_m$, be the set of all positive integers less than *n* and relatively prime to *n*. For example, if $n = 9$, then

$$S_9 = \{a_1, a_2, a_3, \ldots, a_6\} = \{1, 2, 4, 5, 7, 8\}$$

(a) Construct a table consisting of *n* and S_n for $n = 2, 3, \ldots, 15$, and then compute

$$\sum_{k=1}^{m} a_k \quad \text{and} \quad \left(\sum_{k=1}^{m} a_k\right) \pmod{n}$$

in each case. Draw a conjecture for $n > 15$ and prove your conjecture to be true. [*Hint:* Use the fact that if *a* is relatively prime to *n*, then $n - a$ is also relatively prime to *n*.]

(b) Given a positive integer *n* and the set S_n, let P_n be the $m \times m$ matrix

$$P_n = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{m-1} & a_m \\ a_2 & a_3 & a_4 & \cdots & a_m & a_1 \\ a_3 & a_4 & a_5 & \cdots & a_1 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ a_{m-1} & a_m & a_1 & \cdots & a_{m-3} & a_{m-2} \\ a_m & a_1 & a_2 & \cdots & a_{m-2} & a_{m-1} \end{bmatrix}$$

so that, for example,

$$P_9 = \begin{bmatrix} 1 & 2 & 4 & 5 & 7 & 8 \\ 2 & 4 & 5 & 7 & 8 & 1 \\ 4 & 5 & 7 & 8 & 1 & 2 \\ 5 & 7 & 8 & 1 & 2 & 4 \\ 7 & 8 & 1 & 2 & 4 & 5 \\ 8 & 1 & 2 & 4 & 5 & 7 \end{bmatrix}$$

Use a computer to compute $\det(P_n)$ and $\det(P_n) \pmod{n}$ for $n = 2, 3, \ldots, 15$, and then use these results to construct a conjecture.

(c) Use the results of part (a) to prove your conjecture to be true. [*Hint:* Add the first $m - 1$ rows of P_n to its last row and then use Theorem 2.2.3.] What do these results imply about the inverse of $P_n \pmod{n}$?

T2. Given a positive integer *n* greater than 1, the number of positive integers less than *n* and relatively prime to *n* is called the ***Euler phi function*** of *n* and is denoted by $\varphi(n)$. For example, $\varphi(6) = 2$ since only two positive integers (1 and 5) are less than 6 and have no common factor with 6.

(a) Using a computer, for each value of $n = 2, 3, \ldots, 25$ compute and print out all positive integers that are less than *n* and relatively prime to *n*. Then use these integers to determine the values of $\varphi(n)$ for $n = 2, 3, \ldots, 25$. Can you discover a pattern in the results?

(b) It can be shown that if $\{p_1, p_2, p_3, \ldots, p_m\}$ are all the distinct prime factors of n, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

For example, since $\{2, 3\}$ are the distinct prime factors of 12, we have

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

which agrees with the fact that $\{1, 5, 7, 11\}$ are the only positive integers less than 12 and relatively prime to 12. Using a computer, print out all the prime factors of n for $n = 2, 3, \ldots, 25$. Then compute $\varphi(n)$ using the formula above and compare it to your results in part (a).

10.16 Genetics

In this section we investigate the propagation of an inherited trait in successive generations by computing powers of a matrix.

Prerequisites

Eigenvalues and Eigenvectors

Diagonalization of a Matrix

Intuitive Understanding of Limits

Inheritance Traits

In this section we examine the inheritance of traits in animals or plants. The inherited trait under consideration is assumed to be governed by a set of two genes, which we designate by A and a. Under ***autosomal inheritance*** each individual in the population of either gender possesses two of these genes, the possible pairings being designated AA, Aa, and aa. This pair of genes is called the individual's ***genotype***, and it determines how the trait controlled by the genes is manifested in the individual. For example, in snapdragons a set of two genes determines the color of the flower. Genotype AA produces red flowers, genotype Aa produces pink flowers, and genotype aa produces white flowers. In humans, eye coloration is controlled through autosomal inheritance. Genotypes AA and aa have brown eyes, and genotype Aa has blue eyes. In this case we say that gene A ***dominates*** gene a, or that gene a is ***recessive*** to gene A, because genotype Aa has the same outward trait as genotype AA.

In addition to autosomal inheritance we will also discuss ***X-linked inheritance***. In this type of inheritance, the male of the species possesses only one of the two possible genes (A or a), and the female possesses a pair of the two genes (AA, aa, or Aa). In humans, color blindness, hereditary baldness, hemophilia, and muscular dystrophy, to name a few, are traits controlled by X-linked inheritance.

Below we explain the manner in which the genes of the parents are passed on to their offspring for the two types of inheritance. We construct matrix models that give the probable genotypes of the offspring in terms of the genotypes of the parents, and we use these matrix models to follow the genotype distribution of a population through successive generations.

Autosomal Inheritance

In autosomal inheritance an individual inherits one gene from each of its parents' pairs of genes to form its own particular pair. As far as we know, it is a matter of chance which of the two genes a parent passes on to the offspring. Thus, if one parent is of genotype Aa, it is equally likely that the offspring will inherit the A

gene or the a gene from that parent. If one parent is of genotype aa and the other parent is of genotype Aa, the offspring will always receive an a gene from the aa parent and will receive either an A gene or an a gene, with equal probability, from the Aa parent. Consequently, each of the offspring has equal probability of being genotype aa or Aa. In Table 1 we list the probabilities of the possible genotypes of the offspring for all possible combinations of the genotypes of the parents.

Table 1

Genotype of Offspring	Genotypes of Parents					
	AA–AA	*AA–Aa*	*AA–aa*	*Aa–Aa*	*Aa–aa*	*aa–aa*
AA	1	$\frac{1}{2}$	0	$\frac{1}{4}$	0	0
Aa	0	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$	0
aa	0	0	0	$\frac{1}{4}$	$\frac{1}{2}$	1

EXAMPLE 1 Distribution of Genotypes in a Population

Suppose that a farmer has a large population of plants consisting of some distribution of all three possible genotypes AA, Aa, and aa. The farmer desires to undertake a breeding program in which each plant in the population is always fertilized with a plant of genotype AA and is then replaced by one of its offspring. We want to derive an expression for the distribution of the three possible genotypes in the population after any number of generations.

For $n = 0, 1, 2, \ldots$, let us set

$$\begin{aligned} a_n &= \text{fraction of plants of genotype } AA \text{ in } n \text{ th generation} \\ b_n &= \text{fraction of plants of genotype } Aa \text{ in } n \text{ th generation} \\ c_n &= \text{fraction of plants of genotype } aa \text{ in } n \text{ th generation} \end{aligned}$$

Thus a_0, b_0, and c_0 specify the initial distribution of the genotypes. We also have that

$$a_n + b_n + c_n = 1 \text{ for } n = 0, 1, 2, \ldots$$

From Table 1 we can determine the genotype distribution of each generation from the genotype distribution of the preceding generation by the following equations:

$$\begin{aligned} a_n &= a_{n-1} + \frac{1}{2}b_{n-1} \\ b_n &= c_{n-1} + \frac{1}{2}b_{n-1} \quad n = 1, 2, \ldots \\ c_n &= 0 \end{aligned} \tag{1}$$

For example, the first of these three equations states that all the offspring of a plant of genotype AA will be of genotype AA under this breeding program and that half of the offspring of a plant of genotype Aa will be of genotype AA.

Equations 1 can be written in matrix notation as

$$\mathbf{x}^{(n)} = M\mathbf{x}^{(n-1)}, \quad n = 1, 2, \ldots \tag{2}$$

where

$$\mathbf{x}^{(n)} = \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix}, \ \mathbf{x}^{(n-1)} = \begin{bmatrix} a_{n-1} \\ b_{n-1} \\ c_{n-1} \end{bmatrix}, \text{ and } M = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Note that the three columns of the matrix M are the same as the first three columns of Table 1.

From Equation 2 it follows that

$$\mathbf{x}^{(n)} = M\mathbf{x}^{(n-1)} = M^2\mathbf{x}^{(n-2)} = \cdots = M^n\mathbf{x}^{(0)} \tag{3}$$

Consequently, if we can find an explicit expression for M^n, we can use 3 to obtain an explicit expression for $\mathbf{x}^{(n)}$. To find an explicit expression for M^n, we first diagonalize M. That is, we find an invertible matrix P and a diagonal matrix D such that

$$M = PDP^{-1} \tag{4}$$

With such a diagonalization, we then have (see Exercise 1)

$$M^n = PD^nP^{-1} \text{ for } n = 1, 2, \ldots$$

where

$$D^n = \begin{bmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_k \end{bmatrix}^n = \begin{bmatrix} \lambda_1^n & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2^n & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_k^n \end{bmatrix}$$

The diagonalization of M is accomplished by finding its eigenvalues and corresponding eigenvectors. These are as follows (verify):

$$\text{Eigenvalues:} \qquad \lambda_1 = 1, \qquad \lambda_2 = \frac{1}{2}, \qquad \lambda_3 = 0$$

$$\text{Corresponding eigenvectors:} \quad \mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$$

Thus, in Equation 4 we have

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

and

$$P = [\mathbf{v}_1|\mathbf{v}_2|\mathbf{v}_3] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore,

$$\mathbf{x}^{(n)} = PD^nP^{-1}\mathbf{x}^{(0)} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \left(\frac{1}{2}\right)^n & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ b_0 \\ c_0 \end{bmatrix}$$

or

$$\mathbf{x}^{(n)} = \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix} = \begin{bmatrix} 1 & 1-\left(\frac{1}{2}\right)^n & 1-\left(\frac{1}{2}\right)^{n-1} \\ 0 & \left(\frac{1}{2}\right)^n & \left(\frac{1}{2}\right)^{n-1} \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ b_0 \\ c_0 \end{bmatrix}$$

$$= \begin{bmatrix} a_0 + b_0 + c_0 - \left(\frac{1}{2}\right)^n b_0 - \left(\frac{1}{2}\right)^{n-1} c_0 \\ \left(\frac{1}{2}\right)^n b_0 + \left(\frac{1}{2}\right)^{n-1} c_0 \\ 0 \end{bmatrix}$$

Using the fact that $a_0 + b_0 + c_0 = 1$, we thus have

$$\begin{aligned} a_n &= 1 - \left(\frac{1}{2}\right)^n b_0 - \left(\frac{1}{2}\right)^{n-1} c_0 \\ b_n &= \left(\frac{1}{2}\right)^n b_0 + \left(\frac{1}{2}\right)^{n-1} c_0 \qquad n = 1, 2, \ldots \\ c_n &= 0 \end{aligned} \tag{5}$$

These are explicit formulas for the fractions of the three genotypes in the *n*th generation of plants in terms of the initial genotype fractions.

Because $\left(\frac{1}{2}\right)^n$ tends to zero as *n* approaches infinity, it follows from these equations that

$$\begin{aligned} a_n &\to 1 \\ b_n &\to 0 \\ c_n &= 0 \end{aligned}$$

as *n* approaches infinity. That is, in the limit all plants in the population will be genotype *AA*.

EXAMPLE 2 Modifying Example 1 ◀

We can modify Example 1 so that instead of each plant being fertilized with one of genotype *AA*, each plant is fertilized with a plant of its own genotype. Using the same notation as in Example 1, we then find

$$\mathbf{x}^{(n)} = M^n \mathbf{x}^{(0)}$$

where

$$M = \begin{bmatrix} 1 & \frac{1}{4} & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{4} & 1 \end{bmatrix}$$

The columns of this new matrix *M* are the same as the columns of Table 1 corresponding to parents with genotypes *AA*–*AA*, *Aa*–*Aa*, and *aa*–*aa*.

The eigenvalues of *M* are (verify)

$$\lambda_1 = 1,\ \lambda_2 = 1,\ \lambda_3 = \frac{1}{2}$$

The eigenvalue $\lambda_1 = 1$ has multiplicity two and its corresponding eigenspace is two-dimensional. Picking two linearly independent eigenvectors $\mathbf{v}_1$ and $\mathbf{v}_2$ in that eigenspace, and a single eigenvector $\mathbf{v}_3$ for the simple eigenvalue $\lambda_3 = \frac{1}{2}$, we have (verify)

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},\ \mathbf{v}_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix},\ \mathbf{v}_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$$

The calculations for $\mathbf{x}^{(n)}$ are then

$$\begin{aligned} \mathbf{x}^{(n)} &= M^n \mathbf{x}^{(0)} = PD^n P^{-1} \mathbf{x}^{(0)} \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & -2 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \left(\frac{1}{2}\right)^n \end{bmatrix} \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \\ 0 & -\frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ b_0 \\ c_0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & \frac{1}{2} - \left(\frac{1}{2}\right)^{n+1} & 0 \\ 0 & \left(\frac{1}{2}\right)^n & 0 \\ 0 & \frac{1}{2} - \left(\frac{1}{2}\right)^{n+1} & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ b_0 \\ c_0 \end{bmatrix} \end{aligned}$$

Thus,

$$
\begin{aligned}
a_n &= a_0 + \left[\frac{1}{2} - \left(\frac{1}{2}\right)^{n+1}\right] b_0 \\
b_n &= \left(\frac{1}{2}\right)^n b_0 \qquad\qquad n = 1, 2, \ldots \\
c_n &= c_0 + \left[\frac{1}{2} - \left(\frac{1}{2}\right)^{n+1}\right] b_0
\end{aligned}
\tag{6}
$$

In the limit, as n tends to infinity, $\left(\frac{1}{2}\right)^n \to 0$ and $\left(\frac{1}{2}\right)^{n+1} \to 0$, so

$$
\begin{aligned}
a_n &\to a_0 + \frac{1}{2} b_0 \\
b_n &\to 0 \\
c_n &\to c_0 + \frac{1}{2} b_0
\end{aligned}
$$

Thus, fertilization of each plant with one of its own genotype produces a population that in the limit contains only genotypes *AA* and *aa*.

Autosomal Recessive Diseases

There are many genetic diseases governed by autosomal inheritance in which a normal gene *A* dominates an abnormal gene *a*. Genotype *AA* is a normal individual; genotype *Aa* is a carrier of the disease but is not afflicted with the disease; and genotype *aa* is afflicted with the disease. In humans such genetic diseases are often associated with a particular racial group—for instance, cystic fibrosis (predominant among Caucasians), sickle-cell anemia (predominant among people of African origin), Cooley's anemia (predominant among people of Mediterranean origin), and Tay-Sachs disease (predominant among Eastern European Jews).

Suppose that an animal breeder has a population of animals that carries an autosomal recessive disease. Suppose further that those animals afflicted with the disease do not survive to maturity. One possible way to control such a disease is for the breeder to always mate a female, regardless of her genotype, with a normal male. In this way, all future offspring will either have a normal father and a normal mother (*AA*–*AA* matings) or a normal father and a carrier mother (*AA*–*Aa* matings). There can be no *AA*–*aa* matings since animals of genotype *aa* do not survive to maturity. Under this type of mating program no future offspring will be afflicted with the disease, although there will still be carriers in future generations. Let us now determine the fraction of carriers in future generations. We set

$$
\mathbf{x}^{(n)} = \begin{bmatrix} a_n \\ b_n \end{bmatrix}, \quad n = 1, 2, \ldots
$$

where

$$
\begin{aligned}
a_n &= \text{fraction of population of genotype } AA \text{ in } n \text{ th generation} \\
b_n &= \text{fraction of population of genotype } Aa \text{ (carriers) in } n \text{ th generation}
\end{aligned}
$$

Because each offspring has at least one normal parent, we may consider the controlled mating program as one