Further applications of linear algebra

The inverse matrix in cryptology, the discrete cases of Lanchester's warfare model and Richardson's arms race model

Notes created by
Prof. Diego Maldonado and Prof. Virginia Naibo

Department of Mathematics
Kansas State University
Manhattan, KS 66506

Math551: Applied Matrix Theory

The inverse matrix in cryptology

Messages as matrices

Code the alphabet by using the ordinal number of each letter. Also, assign the value 27 to the blank space. That is,

a	b	c	d	e	f	g	h	i	j	k	l	m	n
1	2	3	4	5	6	7	8	9	10	11	12	13	14

o	p	q	r	s	t	u	v	w	x	y	z	space
15	16	17	18	19	20	21	22	23	24	25	26	27

An example

In order to turn the message

the keys are behind the tv

into a matrix. We consider its numerical equivalent

20 8 5 27 11 5 25 19 27 1 18 5 27 2 5 8 9 14 4 27 20 8 5 27 20 22

and arrange those numbers as columns of, say, a 3×9 matrix as follows

$$M = \begin{bmatrix} 20 & 27 & 25 & 1 & 27 & 8 & 4 & 8 & 20 \\ 8 & 11 & 19 & 18 & 2 & 9 & 27 & 5 & 22 \\ 5 & 5 & 27 & 5 & 5 & 14 & 20 & 27 & 27 \end{bmatrix}$$

Notice how we completed the matrix by adding that last 27.

Now, the secrecy

In order to encrypt the message M, we choose any non-singular (i.e. invertible) 3×3 matrix E, say,

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

and create a new matrix P by multiplying E and M, that is,

$$P = EM = \begin{bmatrix} 71 & 98 & 86 & 34 & 80 & 28 & 46 & 7 & 77 \\ -15 & -22 & 2 & 4 & -22 & 6 & 16 & 19 & 7 \\ 31 & 44 & 36 & 32 & 26 & 12 & 38 & -9 & 37 \end{bmatrix}$$

We say that P encodes the message in M. To pass from P to M we do

$$M = E^{-1}P$$

That is, you can send out the message P to anyone, but, unless they have access to E^{-1}, they won't be able to get to M.

Another example: breaking the code

Suppose that we got the message P given by

$$P = \begin{bmatrix} 59 & 33 & 51 & 57 & 63 & 48 & 39 \\ 64 & 42 & 64 & 60 & 84 & 56 & 68 \\ -13 & -9 & -41 & -7 & -9 & 6 & -11 \end{bmatrix}$$

and we are certain that it encodes the sentence

I will see you at ten

Can we break the code in general? That is, can we figure out the encrypting matrix E in this case?

In matrix form, the message **I will see you at ten** looks like

$$M = \begin{bmatrix} 9 & 9 & 27 & 5 & 15 & 1 & 20 \\ 27 & 12 & 19 & 27 & 21 & 20 & 5 \\ 23 & 12 & 5 & 25 & 27 & 27 & 14 \end{bmatrix}$$

and we are looking for a 3×3 matrix E such that

$$P = EM$$

K-STATE.

The encrypting matrix E as a solution to a linear system

We are familiar with solving systems of the form $Ax = b$, and, more generally,

$$AX = B$$

where A and B are data and X is an unknown matrix. We can solve for X by doing

$$>> rref([A, B])$$

Since we are looking for E such that $P = EM$, we transpose this equality to obtain

$$M^t E^t = P^t,$$

from which M^t and P^t are data and E^t is the unknown.

Finding E^t

In Matlab notation, we do

```
>> rref([M',P'])

ans =

     1     0     0     1     2    -1
     0     1     0     1     0    -1
     0     0     1     1     2     1
     0     0     0     0     0     0
     0     0     0     0     0     0
     0     0     0     0     0     0
     0     0     0     0     0     0
```

which shows that our unknown E^t is given by

$$E^t = \begin{bmatrix} 1 & 2 & -1 \\ 1 & 0 & -1 \\ 1 & 2 & 1 \end{bmatrix}$$

Access granted

Once we found E^t, we can transpose it to get E and then compute E^{-1}.

Next, whenever we intercept any other coded message P we only need to left-multiply it by E^{-1} to decode it.

Can you think of a way of encoding images?

Problem 1

Suppose that the coded message

$$P = \begin{bmatrix} 122 & 123 & 87 & 127 \\ 84 & 95 & 106 & 89 \\ 124 & 79 & 53 & 99 \end{bmatrix}$$

means **No way Jose**. What does the following mean?

$$Q = \begin{bmatrix} 131 & 21 & 47 & 37 & 122 & 109 & 70 & 113 \\ 101 & 26 & 98 & 34 & 76 & 50 & 65 & 69 \\ 95 & 55 & 17 & 79 & 108 & 147 & 60 & 157 \end{bmatrix}$$

Lanchester's warfare model: the discrete case

About F. W. Lanchester

The following model for warfare was introduced by Frederick William Lanchester (1868-1945), an English engineer who also made contributions to automotive design and the theory of aerodynamics.

A discrete dynamical system

Let X and Y denote two fighting groups and let x_k and y_k, represent the number of X and Y units, respectively, at a given moment $k = 0, 1, 2, ...$
Suppose that X and Y start fighting each other at $k = 0$.
Also, assume that $a > 0$ and $b > 0$ denote the fighting effectiveness of the units X and Y respectively, that is, each unit eliminates a or b enemy units per unit of time (e.g., per minute, per hour, etc.)
This leads to

$$\begin{cases} x_{k+1} = x_k - by_k, \\ y_{k+1} = y_k - ax_k \end{cases} \tag{1}$$

Matrix form

For $k = 0, 1, 2, \ldots$ let's introduce the vector

$$u_k = \begin{bmatrix} x_k \\ y_k \end{bmatrix}$$

and the step matrix

$$A = \begin{bmatrix} 1 & -b \\ -a & 1 \end{bmatrix}$$

Hence, the system (1) can be expressed as

$$u_{k+1} = Au_k, \quad k = 0, 1, 2\ldots$$

and, equivalently,

$$u_k = A^k u_0, \quad k = 0, 1, 2, \ldots$$

Example

Suppose that the effectiveness for X and Y are $a = .3$ and $b = .1$, respectively, and X goes to battle with 1000 units while Y goes to battle with 2000 units. That is, although X is outnumbered (2 to 1) by Y, the X units are three times as effective as the Y units. We then have

```
>> A=[1 -.1; -.3 1]
A =
    1.0000   -0.1000
   -0.3000    1.0000

>> u0=[1000 2000]'
u0 =
        1000
        2000
```

The outcome of the battle

To follow the evolution of the battle we look at the products Au_0, A^2u_0, A^3u_0,... to see how the vector u_k changes with time. Say k is measured in hours. Then, rounding off, we compute

```
>> round(A*u0)

ans =

         800
        1700

>> round(A^2*u0)

ans =

         630
        1460
```

```
>> round(A^3*u0)

ans =

         484
        1271

>> round(A^4*u0)

ans =

         357
        1126
```

```
>> round(A^5*u0)

ans =

         244
        1019

>> round(A^6*u0)

ans =

   142
   945
```

```
>> round(A^7*u0)
ans =

    48
   903

>> round(A^8*u0)
ans =

   -42
   888
```

That is, after 7 to 8 hours of battle, the Y units win, with a high percentage of survivors too.

A better strategy for the X units

Suppose that, before the battle, the X units had been able to split the Y ones into two equal forces and fight them sequentially. What would the outcome be? In this case, for the first battle we have

```
>> u0=[1000 1000]'
u0 =

        1000
        1000

>> round(A*u0)
ans =

   900
   700
```

```
>> round(A^2*u0)
ans =

   830
   430

>> round(A^3*u0)
ans =

   787
   181
```

```
>> round(A^4*u0)
ans =
   769
   -55
```

That is, after 3 to 4 hours the X units win the first battle.
Suppose that after the first 3 hours the remaining Y units join the first ones and the second battle starts. We now have,
X units $=$ 787 survivors from the first battle
Y units $=$ 1000 fresh units plus 181 survivors from the first battle
The updated initial vector is then

```
>> u0=[787 1181]'
u0 =
         787
        1181
```

The second battle

```
>> round(A*u0)

ans =

   669
   945

>> round(A^2*u0)

ans =

   574
   744
```

```
>> round(A^3*u0)

ans =

   500
   572

>> round(A^4*u0)

ans =

   443
   422
```

```
>> round(A^5*u0)

ans =

   401
   289

>> round(A^6*u0)

ans =

   372
   169
```

```
>> round(A^7*u0)
ans =
   355
    57

>> round(A^8*u0)
ans =
   349
   -49
```

That is, after 7 to 8 hours of engaging in the second battle, the X units win, with a significant percentage of survivors.

What is your conclusion?

Problem 2

Set up the equations (as a system and also in matrix form) of a warfare model for a three-way battle involving units from armies X, Y, and Z.

Richardson's arms race model: the discrete case

About L. F. Richardson

Lewis Fry Richardson (1881-1953) was an English physicist of Quaker background whose aversion to war led him to undertake a study of its causes. He pioneered the modern mathematical techniques of weather forecasting. Reportedly, the discovery that his meteorological work was of value to chemical weapons designers led him to abandon all his efforts in this field, and destroy findings that he had yet to publish.

Richardson crater on Mars

Recall that Mars was the name of the Roman god of war.

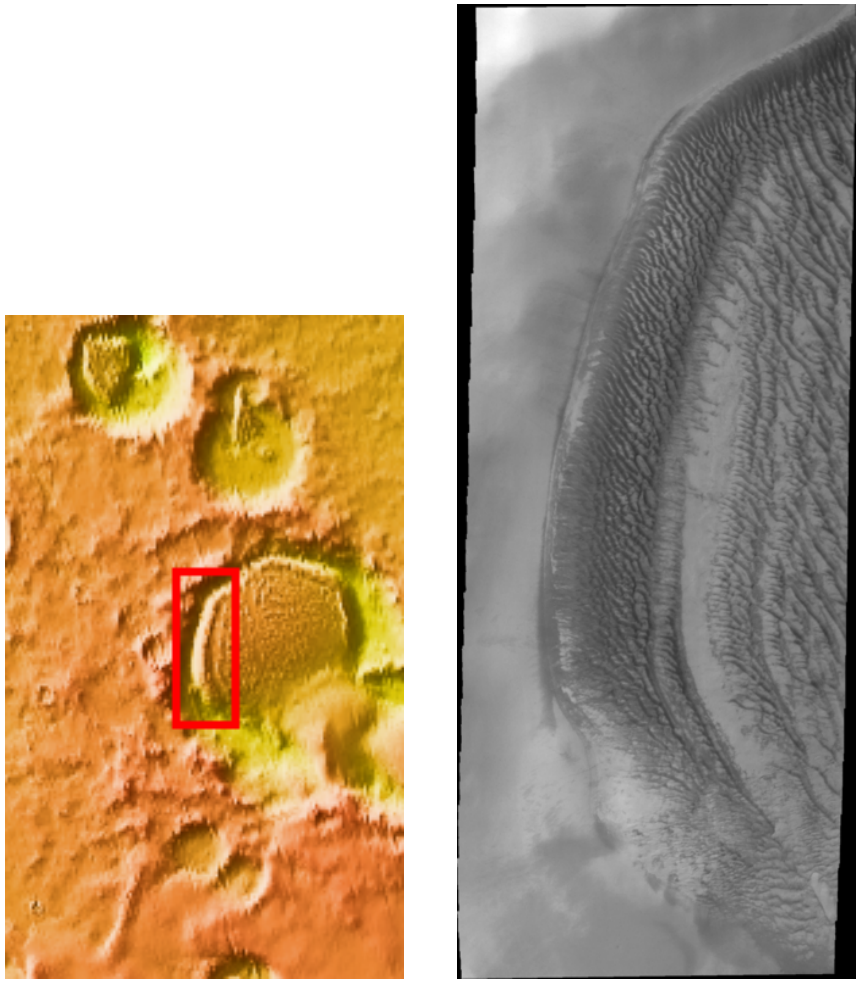

Figure: Image credit: NASA/JPL/MOLA at http://themis2.mars.asu.edu/zoom-20090806a

The main assumptions in Richardson's model

Richardson postulated three motives which lead a nation in times of peace to increase or decrease its preparation for war:

1. There is the motive of revenge or hostility which is independent of existing armaments, and which tends to be enduring and constant.
2. There is the very strong motive of fear, which moves each group to increase its armaments because of the existence of those of the opposing group.
3. There is always a tendency for each group to reduce its armaments in order to economize expenditure and effort.

A discrete dynamical system

Let x_k and y_k denote the expenditure on arms by two countries X and Y at a given moment k (measured in months, years, etc.) Richardson's model is given by

$$\begin{cases} x_{k+1} = x_k + ay_k - mx_k + r, \\ y_{k+1} = y_k + bx_k - ny_k + s \end{cases} \tag{2}$$

The coefficients $a > 0$ and $b > 0$ are referred to as **fear**, **reaction**, or **threat** coefficients.
The coefficients $m > 0$ and $n > 0$ are related to the economic burden or the fatigue associated with procuring and maintaining a country's arsenal and to the reluctance of a nation to spend more of its budget on arms and they are called the **fatigue** coefficients.
The numbers r and s will be positive or negative in the case of mutual suspicions and negative in case of mutual goodwill. According to their sign, they are called the **grievance** or **hostility** or **peace** values.

Matrix form

As usual, for $k = 0, 1, 2, \ldots$ set up the vector

$$u_k = \begin{bmatrix} x_k \\ y_k \end{bmatrix}$$

and the step matrix

$$A = \begin{bmatrix} 1-m & a \\ b & 1-n \end{bmatrix}.$$

Also, put

$$v = \begin{bmatrix} r \\ s \end{bmatrix}$$

Hence, the system (2) can be expressed as

$$u_{k+1} = Au_k + v, \quad k = 0, 1, 2\ldots$$

The presence of a fixed vector v

For $k = 0$, we have

$$u_1 = Au_0 + v.$$

For $k = 1$, we have

$$u_2 = Au_1 + v = A(Au_0 + v) + v = A^2u_0 + Av + v.$$

For $k = 2$, we have

$$u_3 = Au_2 + v = A(A^2u_0 + Av + v) + v = A^3u_0 + A^2v + Av + v$$

The general expression

For any k we now deduce that

$$u_k = A^k u_0 + A^{k-1} v + A^{k-2} v + \cdots + Av + v,$$

that is,

$$u_k = A^k u_0 + \sum_{j=0}^{k-1} A^j v,$$

where we agree upon the notation $A^0 = I$ (the identity matrix), so that $A^0 v = v$.

War and peace

For the sake of simplicity, suppose that $r = s = 0$, that is, $v = [0 \quad 0]'$, there are no grievances between X and Y. Then, the general formula for the expenditure on arms takes the form

$$u_k = A^k u_0, \quad k = 0, 1, 2...,$$

When will there be (the hope of) peace? One way to describe peace would be that the countries X and Y stop their arms race. That is, there exists a year k_0 such that $u_{k_0} = u_{k_0+1}$. Notice that this only means that in year $k_0 + 1$ the countries will spend the same amount on weapons as they did in year k_0.
This doesn't mean that they stopped spending money on weapons, it only means that they are not **increasingly** spending money on weapons.

Finding peace or not

The vector u_{k_0} satisfies

$$u_{k_0} = u_{k_0+1} = Au_{k_0},$$

that is, if we rename the vector u_{k_0} as p (after *peace*), the vector p satisfies

$$p = Ap.$$

Of course, the existence of such a vector p will depend on the nature of the matrix A.

Example

Suppose that $r = s = 0$, $a = .5$, $b = .8$, $m = .1$ and $n = .2$. Then,

```
>> A=[.9 .5; .8 .8]

A =

    0.9000    0.5000
    0.8000    0.8000
```

and suppose an initial expenditure given (in billions of dollars) by

```
>> u0=[50 60]';
```

```
>> A*u0

ans =

    75
    88

>> A^2*u0

ans =

  111.5000
  130.4000
```

```
>> A^3*u0
ans =
  165.5500
  193.5200

>> A^4*u0
ans =
  245.7550
  287.2560

>> A^5*u0
ans =
  364.8075
  426.4088
```

Can there be a peace vector in this situation? Apparently not, since it looks like the amounts of money spent in weapons keeps increasing.
Let's deduce the impossibility of peace under these coefficients by using our *rref* skills.
The vector p solves $Ap = p$, that is,

$$(A - I)p = 0.$$

If we solve for p, we get

```
>> rref([A-eye(2), [0 0]'])
ans =
     1     0     0
     0     1     0
```

That is, is the only solution is $p = [0,\ 0]'$, which says that the only way that peace has a chance under the given fear and fatigue coefficients is that the countries never spend any money on weapons. Otherwise, the situation will escalate to an unstoppable arms race.

Let's give peace a chance

When can the coefficients a, b, m and n (always assuming $r = s = 0$) allow for a non-zero vector p?
Recall that the step matrix A is of the form

$$A = \begin{bmatrix} 1-m & a \\ b & 1-n \end{bmatrix}.$$

When can we assure that A will admit a non-zero vector p such that

$$Ap = p?$$

Stochastic matrices

A matrix is called **column stochastic** if its entries are non-negative numbers and its columns add up to 1.
A matrix is called **row stochastic** if its entries are non-negative numbers and its rows add up to 1.
A row stochastic or columns stochastic matrix S will *always* admit a non-zero vector p such that

$$Sp = p.$$

When is Richardson's matrix stochastic?

Notice that the step matrix A from Richardson's model is row stochastic if all the numbers a, b, m and n are between 0 and 1 (for instance, if they are thought of as percentages) and if $a = m$ and $b = n$. The last equalities say that the fear factor in country X equals its fatigue factor and the fear factor in country Y equals its fatigue factor as well.
Also, A is column stochastic if the coefficients are percentages and if $b = m$ and $a = n$. The last equalities mean that the fear factor of country Y equals the fatigue factor of country X and that the fear factor of country X equals the fatigue factor of country Y.

Problem 3

The cost of peace by having the bigger stick. Consider the following situations for countries X and Y and their corresponding fear and fatigue factors:

1. $a = .4$, $m = .4$ and $b = .2$, $n = .2$. Notice that the corresponding Richardson matrix is row stochastic; thus, peace is possible.
   Find a non-zero peace vector $p = [p_1, p_2]'$. Look at the ratio p_2/p_1
2. $a = .3$, $m = .6$ and $b = .6$, $n = .3$. Notice that the corresponding Richardson matrix is column stochastic; thus, peace is possible here too.
   Find a non-zero peace vector $p = [p_1, p_2]'$. Look at the ratio p_2/p_1.

Between those two peaceful scenarios, which one is more convenient for country Y? Justify.