Lab 3
Due 11/05/2018

I Instruction.

In this lab, we will use Matlab to

(a) Find bases for the column space, row space and null space of a matrix.

(b) Learn how Hill cipher works.

You will need to explain briefly each step, not just show Matlab code. **You are allowed to directly use the command *rref* to obtain reduced row echelon form of matrices.** A good length for this report is 3 - 4 pages.

II Practice.

Practice 1:

Consider the vectors

$$\begin{aligned} v_1 &= (1, 2, 3, 0) \\ v_2 &= (2, 4, 7, -1) \\ v_3 &= (0, 0, 1, -1) \\ b &= (-1, -3, 4, 5) \end{aligned}$$

Denote by V the subspace of $\mathbb{R}^4$ spanned by v_1, v_2, v_3. By definition, V consists of all linear combinations of these vectors. Suppose we want to find a basis of V. Recall that there are two ways to do it. The *first method* is to extract from the set $\{v_1, v_2, v_3\}$ a basis. This is done by making a matrix whose columns are v_1, v_2, v_3.

```
>> A = [v1 v2 v3]
```

Then reduce A into RREF by the command

```
>> rref(A)
```

The output is

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

We see that the first and second columns are pivot. This suggests that first and second columns of A form a basis for V. Thus, a basis of V is $\{v_1, v_2\}$. The dimension of V is 2.

The *second method* is to make a basis out of new and "simpler" vectors. This is done by making a matrix whose rows are v_1, v_2, v_3. You can use either of the following commands:

```
>> B = [v1;v2;v3]
```

or

```
>> B = transpose(A)
```

The command *transpose* produces the transpose of a matrix: the rows of B are columns of A and vice versa. Next, compute the RREF of B. The output is

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

The nonzero rows of B form a basis for V. In this case, it is $S = \{(1, 2, 0, 3), (0, 0, 1, -1)\}$. It does not matter whether you write a vector in form of row or column in the answer.

Suppose we are to add more vectors to basis S of V to get a basis of $\mathbb{R}^4$. The second method is more helpful in this case. We need to add two more vectors to S. The strategy is to remove the zero row(s) of C (the RREF of B) and append two more vectors such that the RREF of the new matrix would be the I_4 (the identity matrix). This is done by spoting the missing leading 1's in C. The second and fourth leading 1's are missing. Thus, we can supplement vectors $(0, 1, 0, 0)$ and $(0, 0, 0, 1)$ to S.

Practice 2:

Suppose person A wants to send a message to person B, but doesn't want any third party to detect the content of its during transmission. This requires a method to encrypt the message before A sends, and decrypt it after B receives. Hill cipher is such a cryptology method. It was introduced by Lesler Hill in 1929 based on linear algebra and number theory. Let us consider one of the simpliest types of Hill cipher, called Hill 2-cipher.

First, each alphabet and special character is labeled by a unique number. For example, the alphabets from a to z are labeled from 1 to 26. The blank space is labeled 0, the apostrophe 27, the comma 28, the period 29, and the colon 30. A message is considered as a string of characters. Suppose the original message is:

let's rule the world

which corresponds to a list (vector) of numbers:

12 5 20 27 19 0 18 21 12 5 0 20 8 5 0 23 15 18 12 4

We group these numbers in pairs: $(12, 5)$, $(20, 27)$,...,$(12, 4)$. Next, we choose a *key*, which is an invertible 2×2 matrix, denoted by H. For example,

$$H = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$$

Each of these 10 pairs of numbers, say v, will be "encoded" as Hv (multiplication of a matrix by a column vector). This gives a new pair of numbers. Thus, we have 10 new pairs of numbers. These numbers are to be converted into characters, so we don't want any of them to exceed 30. Thus, we take modulo 31 after matrix multiplication. For example, if $v = (12, 5)$ then

$$Hv = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} 22 \\ 39 \end{bmatrix}$$

which is $(22, 8)$ in modulo 31. The first pair $(12, 5)$ now corresponds to $(22, 8)$. Similarly, the second pair $(20, 27)$ corresponds to $(12, 28)$ and so on. The original list of numbers becomes:

22 8 12 28 19 7 29 6 22 8 9 29 18 0 15 7 20 22 20 5

which corresponds to the string:

vhl,sg.fvhi.r ogtvte

This is the message A sends. Without knowing the key, third parties cannot know the original message. After receiving the encrypted message, B decrypts it by using the reverse key: $K = H^{-1}$, which is in modulo 31 equal to

$$\begin{bmatrix} 28 & 2 \\ 2 & 30 \end{bmatrix}$$

B repeats the process as A did, only replacing H by K, and retrieve the original message:

let's rule the world

On Canvas or the course webpage, download four following files: *char2num.m, num2char.m, string2pairs.m, pair2string.m,* and store them in the folder you are currently working on in Matlab. After putting those files in the folder, you should be able to see them on the left panel of Matlab (in the window called Current Folder). Each file is a *function*, which takes input(s) and gives output(s):

- char2num: takes a character, returns a number (its label).
- num2char: takes a number, returns the corresponding character.
- string2pairs: takes a string, returns a $2 \times n$ matrix of numbers. Each column of the matrix is a pair of numbers.
- pairs2string: takes a $2 \times n$ matrix, returns the corresponding string.

With these functions, the above procedure can be implemented in Matlab as follows. First, we enter the string:

```
>> s = 'let''s rule the world'
```

Note that the apostrophe after *let* is typed twice because apostrophe is a special character in Matlab. Next, we get the matrix, each column of which is a pair of numbers:

```
>> A = string2pairs(s)
```

You might have noticed a subtle issue here: what if the length of the string is odd? In the function *string2pairs*, you can see that the issue is fixed by padding a blank space after the string if needed to make its length even. Next, apply the key matrix to A:

```
>> B = mod(H*A,31)
```

Next, convert B to string:

```
>> st = pairs2string(B)
```

This is the encrypted string. To get back the original string from here, we repeat the process, only replacing H by its inverse (in modulo 31). Here we run into a little issue in number theory. We know from linear algebra that the inverse of

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

is

$$H^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

But if $\det(H) = ad - bc$ is not ± 1, the entries of H^{-1} might be whole numbers! The remedy lies in the observation that we only want to take the reciprocal of $\det(H)$ in modulo 31. For example, the reciprocal of 2 is 16 because $2 \times 16 = 32 = 1$ in modulo 31. The reciprocal of 3 is 21 because $3 \times 21 = 63 = 1$ in modulo 31. The reciprocal of -1 is 30 because $-1 \times 30 = -30 = 1$ in modulo 31, etc. Because number theory is not our focus here, we only consider the case when $\det(H) = \pm 1$.

```
>> K = mod(inv(H),31)
```

which gives

$$K = \begin{bmatrix} 28 & 2 \\ 2 & 30 \end{bmatrix}$$

(Well, Matlab also shows 0-digits after decimal points. Just reenter K to make it in a nice integer form as above.) The following command should give us back the matrix B:

```
>> C = string2pairs(st)
```

Then apply the inverse key to get back A:

```
>> D = mod(K*C,31)
```

Then apply the function *pairs2string* to get back the original string:

```
>> pairs2string(D)
```

III Exercises.

1. Consider the vectors

$$\begin{aligned} v_1 &= (1, -1, 3, 2, 5) \\ v_2 &= (2, 0, -1, -1, 3) \\ v_3 &= (3, 2, -4, -6, -4) \\ v_4 &= (-5, -4, 12, 12, 8) \\ b &= (4, -3, 4, 5, 18) \end{aligned}$$

   Let $V = \text{span}\{v_1, v_2, v_3, v_4\}$.

   (a) Determine a basis of V. What is the dimension of V? What vectors would you add to this basis to obtain a basis of $\mathbb{R}^5$?

   (b) Check if b belongs to V.

2. Consider a 5×7 matrix

$$A = \begin{bmatrix} 4 & 4 & 8 & 0 & -2 & 14 & 1 \\ 2 & 2 & 3 & 0 & 0 & -1 & 2 \\ 8 & 8 & 16 & -1 & -1 & 27 & 2 \\ -4 & -4 & -6 & 0 & 0 & 7 & -7 \\ 4 & 4 & 8 & 0 & -2 & 19 & -2 \end{bmatrix}$$

   (a) Find a basis for the column space of A. What is its dimension?

   (b) Find a basis for the row space of A. What is its dimension? What vectors would you add to this basis to obtain a basis of $\mathbb{R}^7$.

   (c) Find the basis for the null space of A. What is its dimension?

   (d) What are the rank and nullity of A? Is the rank-nullity theorem satisfied for matrix A?

3. Two persons A and B communicate with each other using Hill 2-cipher. A third-party agent C attempts to crack their secured communication. C sends spyware to B's computer, which in one occasion informs C that the encrypted message "lgzo" which B receives from A becomes "abcd" after being decrypted.

   (a) What is the key matrix H?

   (b) With this key, C can now figure out any encrypted message sent from A. What is the original message of the following (ignore the double quotation mark)?

   "ghv.:xec,btkjuchzcl chje p..rqr'd'jejwk.chjehvitkpit.bixg,je"