THE HILL CIPHER (CONTINUED): COMPUTING THE INVERSE OF A MATRIX

MATH 195

Recall that given a commutative ring R, we consider the $k \times k$ square matrices with entries in R, denoted $M(k, R)$. We have a map $\det : M(k, R) \to R$ called the determinant. We also have the following rule of thumb: All usual rules for computing determinants avoiding divisions are valid over any commutative ring R.

Now we would like to compute inverses of a matrix. Suppose A is a $(k \times k)$-matrix over a commutative ring R, say $A = (a_{ij})_{1 \le i,j \le k}$, $a_{ij} \in R$. Define $A^* = (a^*_{ij})_{1 \le i,j \le k} \in M(k, R)$ by

$$a^*_{ij} = (-1)^{i+j} \det(A_{ji}) \in R$$

where A_{ji} is the $(k-1) \times (k-1)$ matrix obtained from A by deleting the jth row and the ith column.

(It is important to transpose i and j: the text is wrong on this point.)

For example, if

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

then $a^*_{11} = a^* = (-1)^2 d = d$, $a^*_{22} = d^* = a$, and $a^*_{12} = b^* = (-1)^{1+2} b = -b$, $a^*_{21} = c^* = -c$, so

$$A^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Note that given a ring R, the set $R^* = \{a \in R : \exists b \in R,\ ab = 1\}$ of units of R is much different than the adjoint matrix A^* of a matrix $A \in M(k, R)$!

Then we have the following amazing fact:

$$AA^* = A^*A = \det(A)I = \begin{pmatrix} \det(A) & 0 & \dots & 0 \\ 0 & \det(A) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \det(A) \end{pmatrix}.$$

For example, for the 2×2 matrix above, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = (\det A) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Fact. A is invertible (i.e. belongs to $GL(k, R)$) if and only if $\det(A) \in R^*$.

(Note that the text makes an error: the determinant needs to be not only nonzero but invertible!)

This is some of the material covered February 12, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

Proof. If A is invertible, there exists a B such that $AB = I$, hence

$$\det(AB) = \det(A)\det(B) = \det(I) = 1$$

so $\det(A) \in R^*$ (the inverse is $\det(B)$). In the other direction, suppose $\det A \in R^*$, then $A((\det A)^{-1}A^*) = I$, so $A^{-1} = (\det A)^{-1}A^*$. □

Example. Let $R = \mathbb{Z}/26\mathbb{Z}$, $k = 3$. Let

$$K = \begin{pmatrix} -9 & -9 & 5 \\ -5 & -8 & -5 \\ 2 & 2 & -7 \end{pmatrix}.$$

Then

$$K^* = \begin{pmatrix} (-8)(-7) - (-5)2 & \\ & -((-9)(-5) - 5(-5)) \\ & \end{pmatrix} \equiv \begin{pmatrix} -12 & -1 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \pmod{26}$$

and indeed

$$\begin{pmatrix} -9 & -9 & 5 \\ -5 & -8 & -5 \\ 2 & 2 & -7 \end{pmatrix} \begin{pmatrix} -12 & -1 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Here is the "usual algorithm" for finding the inverse of a matrix over a field F. Say for example $F = \mathbb{Z}/7\mathbb{Z}$, and

$$A = \begin{pmatrix} 3 & 3 & -2 \\ 0 & -3 & 0 \\ 2 & 2 & -2 \end{pmatrix}.$$

We write down

$$\begin{pmatrix} 3 & 3 & -2 & 1 & 0 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 \\ 2 & 2 & -2 & 0 & 0 & 1 \end{pmatrix}.$$

Now we multiply the first row by the inverse $3^{-1} = -2 \pmod 7$ to get:

$$\begin{pmatrix} 1 & 1 & -3 & -2 & 0 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 \\ 2 & 2 & -2 & 0 & 0 & 1 \end{pmatrix}.$$

Now multiply the first row by 2 and subtract it from the last row:

$$\begin{pmatrix} 1 & 1 & -3 & -2 & 0 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & -3 & -3 & 0 & 1 \end{pmatrix}.$$

Now invert $(-3)^{-1} = 2$ and scale the middle and bottom rows:

$$\begin{pmatrix} 1 & 1 & -3 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{pmatrix}.$$

Now subtract the second row from the first and add three times the last to the first:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & -2 & -1 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{pmatrix}.$$

Recall inside the matrices $M(k, R)$, we have the invertible matrices $GL(k, R)$ called the *general linear group*. Inside $GL(k, R)$ we have $SL(k, R) = \{A \in M(k, R) :$

$\det A = 1\}$, called the *special linear group*. Inside $SL(k, R)$ we have the elementary subgroup $E(k, R)$, those matrices that can be obtained as the product of elementary matrices. If R is a field or $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$, $E(k, R) = SL(k, R)$. But it is not true for every commutative ring R: this is a fascinating field of mathematics known as K-theory.