THE HILL CIPHER, RINGS, AND SOME LINEAR ALGEBRA

MATH 195

Usually, in linear algebra we take matrices with entries in the real numbers or some other field, but this is not strictly required. As can be seen, this extension has some interesting consequences for cryptography.

Hill Cipher

We take $\mathcal{P} = \mathcal{C} = (\mathbb{Z}/n\mathbb{Z})^k$, $n > 1$, $k \geq 1$, e.g. $n = 26$, $k = 3$. We let $\mathcal{K} = GL(k, \mathbb{Z}/n\mathbb{Z})$ be the *general linear group*, the set of $(k \times k)$-matrices K with entries from $\mathbb{Z}/n\mathbb{Z}$ that are *invertible*, i.e. for which there exists a $k \times k$-matrix L over $\mathbb{Z}/n\mathbb{Z}$ such that $KL = LK = I$, the $k \times k$ identity matrix:

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

We say that L is the *inverse* of K, or $L = K^{-1}$.

For example, $GL(1, \mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$.

The encryption is then $E_K(\alpha) = K\alpha$, where $\alpha \in \mathcal{P}$ is viewed as a column vector. To decrypt, we apply the inverse:

$$D_K(E_K(\alpha)) = D_K(K\alpha) = K^{-1}(K\alpha) = (K^{-1}K)\alpha = I\alpha = \alpha.$$

Elementary Matrices

How can such an invertible matrix K be obtained? For $a \in \mathbb{Z}/n\mathbb{Z}$, we have *elementary matrices*:

$$E_{ij}(a) = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix}$$

where we take ones down the diagonal and a in the ith row and jth column.

Note that $E_{ij}(a)^{-1} = E_{ij}(-a)$, so this matrix is invertible. To obtain a key, we pick $i_1, j_1, a_1, \dots, i_t, j_t, a_t$ and take

$$K = E_{i_1 j_1}(a_1) E_{i_2 j_2}(a_2) \dots E_{i_t j_t}(a_t)$$

This is some of the material covered February 5–7, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight jvoight@math.berkeley.edu.

and the inverse is

$$K^{-1} = E_{i_t j_t}(-a_t) \dots E_{i_1 j_1}(-a_1)$$

since $(gh)^{-1} = h^{-1}g^{-1}$.

Rings

Let us develop this theory a bit further. We can do linear algebra not just over the real numbers or $\mathbb{Z}/n\mathbb{Z}$, but over any ring. [See §5.1 in Fraleigh for a review of rings.]

Definition. A *ring* is a set R together with two operations

$$\begin{aligned} + : R \times R &\to R \\ (a, b) &\mapsto a + b \end{aligned}$$

and

$$\begin{aligned} \cdot : R \times R &\to R \\ (a, b) &\mapsto a \cdot b = ab \end{aligned}$$

such that

- R is an abelian group with respect to $+$ (with neutral element 0);
- $\cdot$ is associative $a(bc) = (ab)c$ and *bilinear*:

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned}$$

- There is an element $1 \in R$ such that for all $a \in R$, $1a = a1 = a$.

Example. $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}$ are rings. $M(k, \mathbb{Z}/n\mathbb{Z})$ is a ring (matrix multiplication is associative, for example, and the identity element is the identity matrix). In fact for any ring R, $M(k, R)$, the set of $(k \times k)$-matrices with entries in the ring R, is itself a ring.

In general, a ring is *not* a group under multiplication (because of a lack of inverses); we define

$$R^* = \{a \in R : \exists b \in R : ab = ba = 1\},$$

and this is the group of *units* (or invertible elements) of R.

Example. We have for the ring $\mathbb{Z}/n\mathbb{Z}$ the group $(\mathbb{Z}/n\mathbb{Z})^*$; for $\mathbb{R}$ we have $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$; $\mathbb{Z}^* = \{1, -1\}$, and $M(k, \mathbb{Z}/n\mathbb{Z})^* = GL(k, \mathbb{Z}/n\mathbb{Z})$.

Why do we need algebra for cryptography? We would like to endow our finite sets with some bit of structure to aid us in encrypting and decrypting. This structure helps us to solve problems, such as if we remove the opposite corners of a checkerboard and try to fill it with dominoes, if we color the squares in the ordinary way we see that it cannot be done (as we have more dark squares than light squares). In this case, we have solved a problem by putting a $\mathbb{Z}/2\mathbb{Z}$ structure on the bland set of squares of the checkerboard.

Note that $R^* = R$ if and only if $R = \{0\}$. If $R = \{0\}$, then certainly $R^* = R$, and conversely, if $R^* = R$ then $0 \in R^*$ so $0 = 0b = 1$ so $a = 1a = 0a = 0$, so $R = \{0\}$.

Not all rings are *commutative*, i.e. $ab = ba$ for all $a, b \in R$: for example, for matrices,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

whereas

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

If $0 \neq 1$, then $1 = 0 + 1 \neq 1 + 1 = 2$, so the matrix ring is not commutative, hence $M(k, R)$ is not commutative if $k \geq 2$, $\#R > 1$.

Determinants

[For a review of determinants, you should consult any linear algebra text, for example, Hill, *Elementary Linear Algebra with Applications*. Elementary matrices are covered in §1.4, Determinants are covered in Chapter 2.]

Now we return to linear algebra over our ring $\mathbb{Z}/n\mathbb{Z}$. The set of all $(k \times k)$-matrices over $\mathbb{Z}/n\mathbb{Z}$ is denoted $M(k, \mathbb{Z}/n\mathbb{Z}) \supset GL(k, \mathbb{Z}/n\mathbb{Z})$. The determinant is the map

$$\det : M(k, \mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$$

$$\det(A) = \sum_{\sigma \in \mathrm{Sym}\, k} \epsilon(\sigma) \prod_{i=1}^{k} a_{i\sigma(i)}$$

$A = (a_{ij})_{1 \leq i,j \leq k}$ where $a_{ij} \in \mathbb{Z}/n\mathbb{Z}$, and the sum is taken over all permutations on the set of indices $1, \dots, k$, where $\epsilon(\sigma)$ is the sign of the permutation ($+1$ if the permutation is even, i.e. composed of an even number of transpositions, -1 if σ is odd).

The determinant has the following properties:

- $\det A \in (\mathbb{Z}/n\mathbb{Z})^*$ if and only if A is invertible.
- For all matrices $A, B \in M(k, \mathbb{Z}/n\mathbb{Z})$, $\det(AB) = (\det A)(\det B)$ in $\mathbb{Z}/n\mathbb{Z}$.
- Every $K \in M(k, \mathbb{Z}/n\mathbb{Z})$ with $\det K = 1$ is the product of finitely many elementary matrices of the form $E_{ij}(a)$.

The first property (multiplicativity) is quite useful: If A is invertible, then there is a matrix B such that $AB = I$, so $\det(A)\det(B) = \det(AB) = \det(I) = 1$, so $\det A$ is invertible in $\mathbb{Z}/n\mathbb{Z}$, which proves one implication of the first property.

Or, more generally, let R be a commutative ring. We can define the determinant

$$\det : M(k, R) \to R.$$

E.g. for $k = 2$ given by

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

for any such matrix, $a, b, c, d \in R$. Notice that then intechanging rows, we get

$$\det \begin{pmatrix} c & d \\ a & b \end{pmatrix} = cb - da = -(ad - bc)$$

since R is commutative.

Rule of thumb: All familiar rules about computing determinants that do not involve division are valid for square matrices over any commutative ring.

For $k = 3$, we have

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei - afh - bdi + bfg + cdh - ceg$$

where we take all permutations with the appropriate sign: we end up with $k!$ terms, numbered by the permutations, in general,

$$\det(a_{ij})_{1\le i,j\le k} = \sum_{\sigma \in \operatorname{Sym} k} \epsilon(\sigma) \prod_{i=1}^{k} a_{i\sigma(i)}$$

as before.

Determinants are multiplicative, but not additive: even though

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

we do *not* necessarily have $\det(A + B) = \det(A) + \det(B)$.

There are a number of rules for computing determinants: in particular, we can row-reduce our matrix: take the matrix over $\mathbb{Z}/26\mathbb{Z}$:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \equiv \begin{pmatrix} -9 & -9 & 5 \\ -5 & -8 & -5 \\ 2 & 2 & -7 \end{pmatrix} \pmod{26}.$$

We can subtract the second column from the first, and this will not change the determinant:

$$\det K = \det \begin{pmatrix} 0 & -9 & 5 \\ 3 & -8 & -5 \\ 0 & 2 & -7 \end{pmatrix} = -3 \det \begin{pmatrix} -9 & 5 \\ 2 & -7 \end{pmatrix} = -3(63 - 10) \equiv -3 \pmod{26},$$

where we have used the property that given a zero, we can forget that row and column when expanding the determinant.

Using row-reduction to calculate determinants will save a great deal of time and is much more efficient than the general expansion (involving $k!$ terms).

We may on occasion like to divide, so we revise our rule:

Rule: All familiar rules about computing determinants are valid for square matrices over any field.

Definition. A *field* is a commutative ring R with the property that $R^* = R \setminus \{0\}$.

Example. $\mathbb{R}$ is a field, but $\mathbb{Z}$ is not a field. $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Since $26 = 2 \cdot 13$, the ring $\mathbb{Z}/26\mathbb{Z}$ is not a field. Instead, if you know about this, we can use the Chinese remainder theorem and reduce the task to a computation modulo 2

$$\det K \equiv \det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \equiv 1 \pmod{2}$$

and modulo 13

$$\det K \equiv \det \begin{pmatrix} 4 & 4 & 5 \\ -5 & 5 & -5 \\ 2 & 2 & 6 \end{pmatrix} \equiv 10 \pmod{13}$$

hence, $\det K \equiv 23 \pmod{26}$.

Or, instead, we can change the size of the alphabet, replace 26 by a prime number, e.g. 29 or maybe 257.