6.4. Frobenius normal form

Let M be an $n \times n$-matrix over a field K.

Make K^n a (left) $K[X]$-module by defining

$$f \cdot v := f(M)v \quad \text{for } f \in K[X].$$

(so $3 \cdot v = 3v$, $X \cdot v = Mv$, $X^2 \cdot v = M^2 v$, ...)

$K[X]$ is a principal ideal domain, so the structure th for f.gen. modules over PIDs shows that

$$K^n \cong \bigoplus_{i=1}^{r} K[X]/(f_i) \quad \text{for polynomials } 0 \neq f_1, \dots, f_r \in K[X]$$

satisfying $f_i \mid f_{i+1}$ for $i = 1, \dots, r-1$.

The pol. are unique up to units.

$\Rightarrow$ Unique if we assume w.l.o.g. that $f_1, \dots, f_r$ are monic. These pol. are called the <u>invariant factors</u> of M.

<u>Def</u> The <u>companion matrix</u> C_f of a monic pol. $f(X) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ is the matrix representing mult. by X in the vector space $K[X]/(f(X))$ w.r.t. the basis $1, x, \dots, x^{n-1}$:

$$C_f = \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & \vdots \\ & \ddots & & \\ 0 & & 1 & -a_{n-1} \end{bmatrix}$$

<u>Rmk</u> The char. and min. pol. of C_f are both $f(X)$.

Pf The matrices $I, C_f, C_f^2, \ldots, C_f^{n-1}$ are linearly independent

because $\underbrace{Ie_1}_{e_1}, \underbrace{C_f e_1}_{e_2}, \ldots, \underbrace{C_f^{n-1} e_1}_{e_n}$ are.

$\Rightarrow$ deg(min. pol.) $= n$.

But $f(C_f) = 0$ because mult. by $f(x)$ in $K[x]/(f)$ is the zero map.

$\Rightarrow$ min. pol. $= f(x)$.

min. pol. $\mid$ char. pol.

$\uparrow$ deg $= n$

$\Rightarrow$ char. pol. $= f(x)$. $\square$

We have shown:

Thm 6.4.1

Any $n \times n$-matrix M is similar to exactly one matrix of the form

$$\begin{bmatrix} C_{f_1} & & 0 \\ & \ddots & \\ 0 & & C_{f_r} \end{bmatrix}$$ for monic pol. $f_1 | \cdots | f_r$.

This is called the Frobenius/rational normal form of M.

The char. pol. of M is $f_1(X) \cdots f_r(X)$.
The min. pol. of M is $f_r(X)$.

Rmk Two matrices are similar iff they have the same Fr.n.f.

Cor 6.4.2 If two matrices are similar over a field $L \supseteq K$, they are similar over K.

Thm 6.4.3 (Storjohann, an $O(n^3)$ algorithm for the Frobenius Normal Form)

---

7. The CRT trick

7.1 Determinants

Let M be an $n \times n$-matrix with integer entries.

Q Compute $\det(M)$.

Rmk Gaussian elimination doesn't work well because the intermediate results can be rational numbers with many digits (nr. of digits could grow exponentially in n).

Idea Compute $(\det(M) \bmod p) \in \mathbb{F}_p$ for sufficiently many primes p to be able to reconstruct $\det(M)$ using the Chinese remainder theorem.

Lemma 7.1.1 For large N,

$$\log \prod_{p \le N \text{ prime}} p \sim N \quad \text{and} \quad \#\{p \le N\} \asymp \frac{N}{\log N}.$$

Pf This is an immediate consequence of the prime number theorem. □

Lemma 7.1.2 Any matrix $M \in M_{n \times n}(\mathbb{R})$, $M = (m_{ij})_{i,j}$, satisfies

$$|\det(M)| \le \prod_{i=1}^{n} \sqrt{\sum_{j=1}^{n} m_{ij}^2} =: B(M).$$

Pf $|\det(M)|$ is the volume of the parallelepiped spanned by the rows of M. □

Hence: (cf. section 2.2.3 in Cohen)

Thm 7.1.3 For any $M \in M_{n\times n}(\mathbb{Z})$, we can compute

$\det(M)$ in time $O\left(\left(n + \log B(M)\right)\cdot\left(n^{\omega} + (\log\log B(M))^2\right)\right)$

on an $O(\log n + \log\log B(M))$-bit RAM.

Pf First, compute $B'(M) := \prod_i \left\lceil \sqrt{\sum_j m_{ij}^2} \right\rceil \le 2^n B(M)$.

($v_i \le B(M)$)

Then, find some $N = O(n + \log B)$ s.t. $\prod_{p\le N} p > 2B'(M)$.

($\sum_{p\le N} \lfloor \log_2 p \rfloor > \lfloor \log_2(2B'(M)) \rfloor$)

For each $p \le N$, compute $\det(M \bmod p) \in \mathbb{F}_p$.

(p has $O(\log\log B(M))$ digits and there are $O(\log B(M))$ such primes p)

Finally, find the integer $x \in [-B'(M), B'(M)]$ such that $x \equiv \det(M \bmod p) \bmod p \ \forall p \le N$ similar to Problem 4 on BSet 3. □

For $N = 1, 2, 4, 8, \ldots$, compute all primes $p \le N$ using the sieve of Eratosthenes in time $O(N \log\log N)$, until you find an N that works.

Remark You can also compute the determinant without reducing modulo primes using the Bareiss algorithm (Alg. 2.2.6 in Cohen)