REEU 2005 · Discrete Mathematics · Lecture 8

Instructor: László Babai
Scribes: T. Schedler, S. Chakraborty

July 6, 2005. Last updated July 8, 2005

1 Lecture 8

1.1 When is a matrix invertible?

Given an $n \times n$ matrix A, we recall that the following conditions are equivalent:

- A^{-1} exists
- $\det(A) \neq 0$
- the rows are linearly independent
- the rows span the space of all possible rows
- the columns span the space of possible columns.

Let $A \in \mathbb{Z}^{n \times n}$ (i.e. A is integral). When is A^{-1} integral?

Claim 1.1. *Let $A \in \mathbb{Z}^{n \times n}$. Then A^{-1} is integral iff $\det(A) = \pm 1$.*

Proof. Necessity: We use the following exercise.

Exercise 1.2. *Determinant is multiplicative, i.e. for all matrices A and B, $\det(AB) = \det(A)\det(B)$. [HINT: Elementary operations on rows of B.]*

From the exercise we get the following corollary:

Corollary 1.3. *For any matrix A we have $\det(A^{-1}) = \frac{1}{\det(A)}$.*

Proof. $\det(A) \cdot \det(A^{-1}) = \det(A \cdot A^{-1}) = \det(I) = 1$, where I is the identity matrix. □

Now let A be a integral matrix. We want to show A^{-1} is integral then $\det(A) = \pm 1$.

Lemma 1.4. *If A is integral then $\det(A)$ is an integer.*

Proof. $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$. □

From the lemma and from the corollary of the exercise we get that $\det(A^{-1}$ is reciprocal of an integer. But since A^{-1} is also integral so by the lemma its determinant is also integer. So the only possiblity is that $\det(A) = \pm 1$.

$\square$

Note, we did not prove the sufficiency.

1.2 Smith Equivalence

Definition 1.5. Let A, B be $k \times \ell$ **integral** matrices (*i.e.* with entries that are integers), then A is Smith-equivalent to B if there exists integral matrices C, D such that C^{-1}, D^{-1} exist and are integral, and

$$CAD = B.$$

Claim 1.6. *Smith equivalence is an equivalence relation.*

Proof. **Reflexive:** $IAI = A$ where I is the identity matrix.

Symmetry: Since $CAD = B$ and C and D are invervible integral matrices and their inverses are also integral. It follows that $C^{-1}BD^{-1} = A$, so the condition is symmetric.

Transitivity: Exercise.

$\square$

Exercise 1.7. *If "$\sim$" is an equivalence relation on a set Ω then there exists a unique partition $\Omega = \dot{\bigcup}\Omega_i$ (here $\dot{\bigcup}$ denotes a disjoint union, i.e. a union such that $\Omega_i \cap \Omega_j = \emptyset$ for $i \neq j$) such that $\forall x, y \in \Omega$, $x \sim y \Leftrightarrow (\exists i)(x, y \in \Omega_i)$.*

So the Smith equivalence partitions the set of all matrices into disjoint classes called *Smith equivalence classes.*

1.3 Smith Normal Form

Definition 1.8. A *Smith-normal-form matrix* is an integral diagonal matrix (here diagonal means that the only nonzero entries are $a_{ii}, i \geq 1$, which makes sense also for non-square matrices) such that $(\forall i)(a_{ii} \mid a_{i+1,i+1})$. For example,

$$\begin{pmatrix} 1 & & & & & & & & \dots \\ & 1 & & & & & & & \dots \\ & & 2 & & & & & & \dots \\ & & & 6 & & & & & \dots \\ & & & & 6 & & & & \dots \\ & & & & & 18 & & & \dots \\ & & & & & & 0 & & \dots \\ & & & & & & & 0 & \dots \end{pmatrix}$$

is a Smith-normal-form matrix.

Theorem 1.9. *Every Smith equivalence class has exactly one Smith-normal-form matrix.*

Definition 1.10. If A is a $k \times \ell$-integral matrix then its Smith Normal Form is the unique Smith-Normal-Form matrix which is Smith-equivalent to A.

One consequence of the above theorem is that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \not\sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.
Observe that if $A = 2A'$ then $\mathrm{SNF}(A) = 2 \cdot \mathrm{SNF}(A')$.
The theorem also holds if entries are not **integers** but are polynomials over a field.
From the theorem we get the following corollaries.

Corollary 1.11. *Sandpile group invariants are the diagonal entries of the Smith Normal Form (SNF) of the reduced Laplacian.*

Corollary 1.12. *The Jordan normal form of matrices.*

Corollary 1.13. *The fundamental theorem of finitely generated abelian groups.*

Recall the

Theorem 1.14. *(Fundamental Theorem of Finitely Generated Abelian Groups). Let G be any finitely generated abelian group. Then $G \cong C_{n_1} \times \cdots \times C_{n_k}$, for nonnegative integers n_i such that $n_1 \mid n_2 \mid \ldots \mid n_k$.*

Now, if A is a square matrix then any Smith equivalent matrix is of the form CAD. Now, $\det(CAD) = \det(C)\det(A)\det(D) = \pm\det(A)$ since C, D are integral and have integral inverses, implying $\det(C) = \pm 1$ and $\det(D) = \pm 1$. Hence $\det(SNF(A)) \mid \det(A)$. In fact we can get a much stronger theorem.

Theorem 1.15. *Let $A = (a_{ij})$ and let $SNF(A) = S = (s_{ij})$. Then*

1. *If* $\gcd(a_{ij}) = s_{11}$.
2. $\gcd(2 \times 2 - \textit{submatrices}) = s_{11} \cdot s_{22}$. *[the number of 2×2-submatrices is $\binom{k}{2} \cdot \binom{\ell}{2}$.]*
3. $\gcd(t \times t - \textit{submatrices}) = s_{11} \cdot s_{22} \cdots s_{tt}$. *[the number of $t \times t$-submatrices is $\binom{k}{t} \cdot \binom{\ell}{t}$.]*
4. *In particular if A is square, we have that* $\det(A) == s_{11} \cdot s_{22} \cdots s_{nn} = \det(S)$.

1.4 Proof of the Theorem

Recall that **elementary row operations** for $A = \begin{pmatrix} \mathbf{a_1} \\ \vdots \\ \mathbf{a_k} \end{pmatrix}$, where $\mathbf{a_i}$ is the i^{th} row, are the following:

1. $\mathbf{a_i} := \mathbf{a_i} + \lambda \mathbf{a_j}, \lambda \in \mathbb{Z}$;

2. $\mathbf{a_i} := -\mathbf{a_i}$;

3. permute rows.

Similarly, column operations can be defined.

Claim 1.16. $\gcd(a_{ij})$ *does not change under elementary operations.*

Claim 1.17. *If A' is obtained from A'_{ij} under elementary operations, then $A' \sim A$ (Smith equivalent).*

Claim 1.18. *Using elementary operations only, one can arrive at the SNF.*

Note that the above three claims prove that first part of the thoerem, *i.e.*, $\gcd(a_{ij}) = s_{11}$. Recall the definition of matrix multiplication:

Definition 1.19. If $A = (a_{ij}), B = (b_{jk})$ then $AB = C = (c_{ik})$ where $c_{ik} = \sum_j a_{ij} b_{jk}$.

So, if $\mathbf{a_2} \mapsto \mathbf{a_2} + \lambda \mathbf{a_1}$, where $\mathbf{a_i}$ are columns, then the new matrix is $A(I + \Lambda) = A + A\Lambda$ where Λ has only one nonzero entry, λ, in the first row and second column. The matrix $I+\Lambda$ is an **elementary matrix**, which is defined to be $I + \Lambda$ for some $\Lambda(\lambda, i', j') = (\lambda_{ij})$ where $\lambda_{ij} = \lambda$ if $i = i', j = j'$ and $\lambda_{ij} = 0$ otherwise. An elementary column operation of type (1) corresponds to multiplying on the right by an elementary matrix, and an elementary row operation of type (1) corresponds to multiplying on the left by an elementary matrix.

Similarly, elementary operations of type (2) correspond to multiplying by a diagonal matrix where one entry is -1 and the others are 1 (of determinant -1).

An elementary operation of type (3) corresponds to multiplying by a permutation matrix (one of the form $P = (p_{i\sigma(i)})$ for some permutation σ), of determinant $\operatorname{sgn}(\sigma)$.

Exercise 1.20. *If A, A^{-1} are integral then A is a product of elementary matrices, permutation matrices, and diagonal matrices with entries ± 1.*

Let A and A^{-1} be integral matrices. Then we know that $\det(A) = \pm 1$. Now since $\det(A) = \pm \det(\mathrm{SNF}(A)) = s_{11} s_{22} \cdots s_{nn}$, we conclude that $\mathrm{SNF}(A) = I$, the identity matrix. (Recall here that the Smith normal form has nonnegative entries in order to be unique.)

Game to play: turning a matrix into Smith normal form.

$$\begin{pmatrix} 52 & 18 \\ * & * \end{pmatrix} \sim \begin{pmatrix} 16 & 18 \\ * & * \end{pmatrix} \sim \begin{pmatrix} 16 & 2 \\ * & * \end{pmatrix} \sim \begin{pmatrix} 0 & 2 \\ * & * \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ * & * \end{pmatrix}.$$

Here we note that $\gcd(52, 18) = \gcd(16, 2) = \gcd(2, 0) = 2$. Here we use that $52 = 18 \cdot 2 + 16$; $18 = 16 \cdot 1 + 2$; and $16 = 2 \cdot 8 + 0$ to compute the gcd of 2 using the Euclidean algorithm.

Using similar tricks prove the following exercise.

Exercise 1.21. *Prove Claim 1.18. for 2×2-matrices.*

Exercise 1.22. *(cf. Corollary 1.13, Theorem 1.14, and last class's notes) Use the Smith Normal Form to prove the Fundamental Theorem of Finitely Generated Abelian groups.*