The Amazing Smith Normal Form

Joshua Ducey

James Madison University

September 24, 2012

- This talk is about integer matrices.

- This talk is about integer matrices.
- We are all interested in these.

- This talk is about integer matrices.
- We are all interested in these.
- When we learn about linear algebra, or teach it, what is our first example of a matrix?

- This talk is about integer matrices.
- We are all interested in these.
- When we learn about linear algebra, or teach it, what is our first example of a matrix?
- $\begin{bmatrix} \pi & e & \cdots \\ \ln(2) & \Phi & \cdots \\ \vdots & & \end{bmatrix}$

- Today I'm going to teach you a cool fact about integer matrices (a neat trick).

- Today I'm going to teach you a cool fact about integer matrices (a neat trick).
- Show it to your friends...

Outline

Equivalence of Matrices

- Let A be an $m \times n$ matrix with entries from a field (like the real numbers).

Equivalence of Matrices

- Let A be an $m \times n$ matrix with entries from a field (like the real numbers).
- If
$$PAQ = B$$
for invertible matrices P and Q, then we say that A and B are "equivalent."

- FACT: The matrix A is equivalent to a unique matrix of the form

$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & 0 & & \\ & & & & & 0 & \\ & & & & & & \end{bmatrix}.$$

- FACT: The matrix A is equivalent to a unique matrix of the form
$$\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & 0 & & \\ & & & & & 0 & \\ \end{bmatrix}.$$
- (The number of 1s is the rank of A.)

Integer Equivalence

- Now let A be an $m \times n$ *integer* matrix. Suppose B is an $m \times n$ integer matrix, and

$$PAQ = B,$$

where P and Q are invertible integer matrices *whose inverses are also integer matrices*.

Integer Equivalence

- Now let A be an $m \times n$ *integer* matrix. Suppose B is an $m \times n$ integer matrix, and

$$PAQ = B,$$

where P and Q are invertible integer matrices *whose inverses are also integer matrices*.

- Then A and B are said to be "integer equivalent."

- The condition that P and Q have integer inverses is the same as insisting that P and Q have determinants ± 1.

- The condition that P and Q have integer inverses is the same as insisting that P and Q have determinants ± 1.
- Such matrices are called *unimodular*.

- FACT: The integer matrix A is integer equivalent to a unique matrix of the form

$$\begin{bmatrix} s_1 & & & & & & \\ & s_2 & & & & & \\ & & s_3 & & & & \\ & & & \ddots & & & \\ & & & & 0 & & \\ & & & & & 0 & \\ \end{bmatrix},$$

where the s_i are integers with $s_i | s_{i+1}$ for all i.

An Example

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix},\ P = \begin{pmatrix} 1 & 0 \\ 4 & -1 \end{pmatrix},\ Q = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

$$PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}.$$

Smith Normal Form

- The unique matrix described above that is integer equivalent to A is called the *Smith normal form of A*.

Smith Normal Form

- The unique matrix described above that is integer equivalent to A is called the *Smith normal form of* A.
- The entries down the main diagonal are called the *invariant factors of* A.

GCDs of Minors

It follows from the Cauchy–Binet formula that $s_1 \cdot s_2 \cdots s_j$ is equal to the greatest common divisor of all determinants of $j \times j$ submatrices of A.

Outline

1. Equivalence of Integral Matrices
2. Some Uses
   - Distinguishing Combinatorial Structures
   - p-rank
3. Finite Abelian Groups

Distinguishing Combinatorial Structures

- Given a relation between two finite sets, encode this relation in a zero-one matrix.

Distinguishing Combinatorial Structures

- Given a relation between two finite sets, encode this relation in a zero-one matrix.
- Various numerical invariants of this “incidence matrix” now become invariants of the relation (of the incidence structure that it defines).

Distinguishing Combinatorial Structures

- Given a relation between two finite sets, encode this relation in a zero-one matrix.
- Various numerical invariants of this “incidence matrix” now become invariants of the relation (of the incidence structure that it defines).
- For example, Smith normal form.

Example: skew lines in $\mathrm{PG}(3,4)$

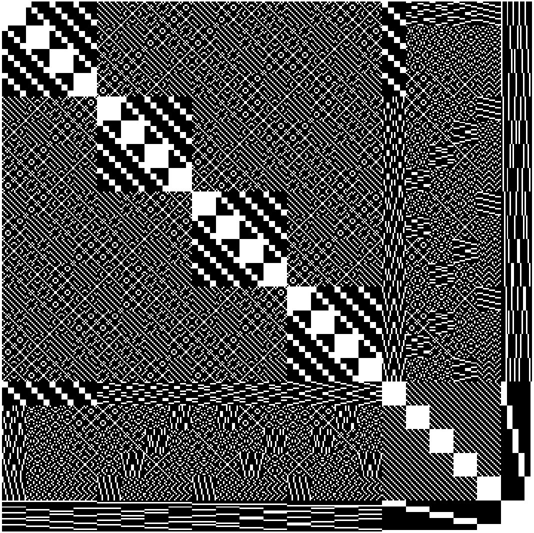

Table: The invariant factors of the incidence matrix of lines vs. lines in $\mathrm{PG}(3,4)$, where two lines are incident when skew.

Inv. Fac.	1	2	2^2	2^3	2^4	2^5	2^6	2^7	2^8
Multiplicity	36	16	220	0	32	16	36	0	1

Rota's Basis Conjecture

- Stephanie Bittner, Mike Cheung, Xuyi Guo, Adam Zweber (Summer 2012)

Rota's Basis Conjecture

- Stephanie Bittner, Mike Cheung, Xuyi Guo, Adam Zweber (Summer 2012)
- Given n bases of an n-dimensional vector space:

$$\begin{array}{cccc} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \\ \vdots & \vdots & & \vdots \\ k_1 & k_2 & \cdots & k_n \end{array}$$

Rota's Basis Conjecture

- Stephanie Bittner, Mike Cheung, Xuyi Guo, Adam Zweber (Summer 2012)
- Given n bases of an n-dimensional vector space:

$$\begin{array}{cccc} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \\ \vdots & \vdots & & \vdots \\ k_1 & k_2 & \cdots & k_n \end{array}$$

- RBC asserts that one can repartition this multiset union of vectors into n disjoint transversals, each of which forms a basis.

Rota's Basis Conjecture

- Stephanie Bittner, Mike Cheung, Xuyi Guo, Adam Zweber (Summer 2012)
- Given n bases of an n-dimensional vector space:

$$\begin{array}{cccc} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \\ \vdots & \vdots & & \vdots \\ k_1 & k_2 & \cdots & k_n \end{array}$$

- RBC asserts that one can repartition this multiset union of vectors into n disjoint transversals, each of which forms a basis.
- A_n is the incidence matrix of "disjoint tranversals."

$$\begin{array}{c} \\ (a_1,b_1) \\ (a_1,b_2) \\ (a_2,b_1) \\ (a_2,b_2) \end{array} \begin{array}{c} \begin{array}{cccc} (a_1,b_1) & (a_1,b_2) & (a_2,b_1) & (a_2,b_2) \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

A_n for $n = 2$

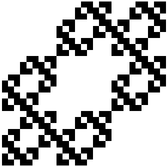

Figure: A_n for $n = 3$, a 27×27 matrix

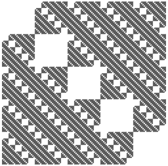

Figure: A_n for $n = 5$, a 3125×3125 matrix

Conjecture: The invariant factors of A_n are

$$(n-1)^k$$

occurring with multiplicity

$$(n-1)^{n-k}\binom{n}{k},$$

for $0 \leq k \leq n$.

p-rank

- Let A be an $m \times n$ integer matrix.

p-rank

- Let A be an $m \times n$ integer matrix.
- Can view entries of A as coming from a finite field $\mathbb{F}_q$ of $q = p^t$ elements.

p-rank

- Let A be an $m \times n$ integer matrix.
- Can view entries of A as coming from a finite field $\mathbb{F}_q$ of $q = p^t$ elements.
- The matrix now defines a map

$$\mathbb{F}_q^n \to \mathbb{F}_q^m.$$

p-rank

- Let A be an $m \times n$ integer matrix.
- Can view entries of A as coming from a finite field $\mathbb{F}_q$ of $q = p^t$ elements.
- The matrix now defines a map

$$\mathbb{F}_q^n \to \mathbb{F}_q^m.$$

- The dimension of the image is known as the "p-rank" of A.

- FACT: The Smith normal form of A tells you the p-rank of A, for any prime p!

- FACT: The Smith normal form of A tells you the p-rank of A, for any prime p!
- Application to error-correcting codes.

Outline

- You may be familiar with:

  FACT: Any finite abelian group G is isomorphic to a direct sum of cyclic groups.

- You may be familiar with:

  FACT: Any finite abelian group G is isomorphic to a direct sum of cyclic groups.

- Furthermore, there is a unique cyclic decomposition

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$$

  with the property that $m_i | m_{i+1}$ for all i.

- You may be familiar with:

  FACT: Any finite abelian group G is isomorphic to a direct sum of cyclic groups.
- Furthermore, there is a unique cyclic decomposition

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$$

  with the property that $m_i | m_{i+1}$ for all i.
- This looks familiar...