

Discrete Math, 19th day, Friday 8/6/04

REU 2004. Info:

<http://people.cs.uchicago.edu/~laci/reu04>.

Instructor: László Babai
Scribe: Charilaos Skiadas

1 Matrix rigidity (Valiant 1978)

Let A be a matrix over a field \mathbb{F} . Our aim is to explore how we can reduce its rank with changing as few entries as possible. For that, denote by $R_r(A)$ the minimum number of entries that need to be changed in A in order to obtain a matrix of rank less than or equal to r . In other words, this is equal to $\min\{\text{weight}(C) : \text{rk}(A - C) \leq r\}$ where the weight of a matrix is the number of nonzero entries. We are particularly interested in the case when $r = \Theta(n)$.

Exercise 19.1. For the identity matrix we have $R_r(I) = n - r$ (Prove that fewer changes do not suffice!)

Proposition 19.2. For every $n \times n$ matrix A we have $R_r(A) \leq (n - r)^2$.

For instance, this would tell us that $R_{n/2} \leq n^2/4$. For the proof of the proposition, we can without loss of generality assume that $\text{rk}(A) \geq r$, so we can assume that A has a nonsingular $r \times r$ minor B , and let us for simplicity assume it appears in the upper left corner. If we focus on the first r rows of A for the moment, we see that the columns of B are linearly independent. Let A' be the $r \times n$ matrix consisting of the first r rows of A . Hence, all of the other columns of A' can be written as linear combinations of the columns of B . So there are numbers $c_{i,j}$ such that $a_{i,j} = \sum_{k=1}^r a_{i,k} c_{k,j}$ for $i = 1, \dots, r$ and $j = r + 1, \dots, n$. Now, if we simply change the entries in the $(n - r) \times (n - r)$ bottom right corner, and redefine them according to the above equation (we define $a'_{i,j} = \sum_{k=1}^r a_{i,k} c_{k,j}$ for $i, j = r + 1, \dots, n$), then this equation now hold for all j , in other words all the columns of A are linear combinations of the first r columns. These first r columns are linearly independent, since the columns of B are. This gives us a matrix with rank r , and we had to make $(n - r)^2$ changes, hence the proposition is proved.

Theorem 19.3. Over infinite fields, almost all matrices satisfy $R_r(A) = (n - r)^2$.

The meaning of “almost all” is that while $\dim M_n(\mathbb{F}) = n^2$, the “dimension” of the set (“variety”) of matrices with $R_r(A) < (n - r)^2$ is strictly less than n^2 .

Think of all $n \times n$ matrices, $M_n(\mathbb{F})$, and let D_r be the subset consisting of all matrices of rank r or less. Then this is defined by a set of algebraic equations, namely all $(r+1) \times (r+1)$ minors are equal to 0. There are $\binom{n}{r+1}^2$ such equations. Such a set, an “affine variety”, has an intuitive notion of dimension. We want to find what that is for D_r . Notice that all of the equations above are independent since, for any $(r+1) \times (r+1)$ minor, the matrix which is the identity on that minor and 0 everywhere else satisfies all but one of the equations. A better way to measure dimension is how many independent directions there are for small changes: Suppose the rank of a matrix is r , and that the top left $r \times r$ minor is nonsingular. We would like to know how many parameters we can change slightly, while keeping the rank r . We can freely slightly change all entries in the first r rows and in the first r columns and still keep the top left $r \times r$ minor non-singular. But all the other $(n-r)^2$ entries are completely determined, if we want to keep the rank no more than r . So we end up with $rn + r(n-r) = r(2n-r) = 2rn - r^2 = n^2 - (n-r)^2$ free choices. So this is the dimension of D_r . (D_r is a finite union of spaces of the above form, for the various choices of minors. But a finite union of sets of a given dimension still has the same dimension as them. This is only true over an infinite field!) Suppose now that we permit m entries to be changed before getting a matrix of rank r . Then each of these entries increases the dimension by 1, giving us one more free variable, hence the whole process will increase the dimension overall by m . Denote $E_{r,m}$ to be the set of matrices B such that there exists a matrix $A \in D_r$ with $\text{weight}(B-A) \leq m$. Then by the above discussion we have $\dim E_{r,m} \leq \dim D_r + m$. So for $m < n^2 - \dim D_r$, almost all matrices satisfy $R_r(A) > mn$ since the set $E_{r,m} = \{A \mid R_r(A) \leq m\}$ has dimension $\leq n^2 - \dim D_r + m < n^2$. So for almost all matrices, $R_r(A) \leq n^2 - \dim D_r = (n-r)^2$, and since it was also less than or equal to it, it is actually equal to it. Let us emphasize again, that this only works over infinite fields.

Exercise 19.4. Prove that if \mathbb{F} is a fixed finite field, then almost all matrices satisfy

$$R_{\frac{n}{2}}(A) > c \frac{n^2}{\log n}.$$

“Almost all” here means that the proportion of matrices satisfying the inequality goes to 0 as $n \rightarrow \infty$.

What we need is **explicit families** of matrices with high rigidity ($R_{cn}(A) > n^{1+\varepsilon}$). This is not known for any fixed $\varepsilon > 0$. We have some examples of non-explicit families: For instance, a matrix with independent transcendental entries. In other words, a “generic matrix” is not explicit. Independent transcendental entries means that if $f(a_{1,1}, \dots, a_{n,n}) = 0$ for some $f \in \mathbb{Z}[a_{i,j}]$, then $f = 0$.

The big question here is: Can one construct matrices with high rigidity with integer entries, where the integer entries have at most polynomially increasing number of digits (i.e., the number of digits is at most n^c for some absolute constant c)?

All nonzero Vandermonde matrices are candidates. A special case of interest is Vandermonde matrix $V_n(1, \omega, \omega^2, \dots, \omega^{n-1})$, where ω is a primitive n -th root of unity (this is known

as the discrete Fourier Transform (DFT) matrix.) One way to generalize this is as follows: Recall that a **character** of a finite abelian group is a homomorphism $\chi : G \rightarrow \{z \in \mathbb{C}, |z| = 1\}$.

Exercise 19.5. Show that a finite abelian group of order n has exactly n characters.

The **character table** of an abelian group is an $n \times n$ matrix with rows indexed by characters and columns indexed by elements of G . The entries are evaluations of the characters on the elements.

Exercise 19.6. Show that the characters of a finite abelian group are orthogonal (i. e., the rows of the character table are orthogonal).

For example, if $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, all the characters are of the form $\chi_i(a) = \omega^{ai}$, where ω is as above. Then the above matrix is simply the character table of \mathbb{Z}_n . Another example would be $G = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 = (\mathbb{F}_2^k, +)$. Then $|G| = 2^k$. If $\underline{a}, \underline{b} \in G$, then $\chi_{\underline{b}}(\underline{a}) = (-1)^{\underline{a}\underline{b}}$ is a character, so every element of G defines a character, and the character table in this case is the Sylvester matrix. More generally, all Hadamard matrices are expected to be good candidates for rigidity.

The best known result at this time is:

Theorem 19.7 (S. Lokam). $R_{\frac{n}{17}}(P) > cn^2$, for P the matrix made out of the square roots of the first n^2 prime numbers.

Unfortunately, this is not exactly explicit. The dimension of the extension of \mathbb{Q} by these numbers is 2^{n^2} , so this field has exponentially large dimension.

Exercise 19.8. The square roots of all square-free numbers are linearly independent over \mathbb{Q} .

This is the best we can say at the moment.

Open question: Give a nonlinear lower bound on R_{cn} for the generic Vandermonde matrix. Lokam's proof gives $R_{\sqrt{n}/2}(V_n(x_1, \dots, x_n)) > cn^2$.