A Remark on Matrix Rigidity

M.A. Shokrollahi, D.A. Spielman, and V. Stemann

November 26, 1997

Abstract. The rigidity of a matrix is defined to be the number of entries in the matrix that have to be changed in order to reduce its rank below a certain value. Using a simple combinatorial lemma, we show that one must alter at least $c\frac{n^2}{r}\log\frac{n}{r}$ entries of an $(n \times n)$-Cauchy matrix to reduce its rank below r, for some constant c. In the second part of the paper we apply our combinatorial lemma to matrices obtained from asymptotically good algebraic geometric codes to obtain a similar result for r satisfying $2n/(\sqrt{q}-1) < r \le n/4$.
Key words. Computational complexity, theory of computation

1. Introduction

Valiant [11] defined the rigidity $\mathcal{R}_M^K(r)$ of a matrix M over a field K to be the number of entries of M that have to be changed to reduce its rank below r:

$$\mathcal{R}_M^K(r) := \min\{\mathrm{wt}(P) \mid \mathrm{rk}(M+P) \le r\}.$$

Here $\mathrm{wt}(P)$ denotes the number of nonzero entries of P. He proposed the fundamental problem of finding matrices with high rigidity. If ε and δ are constants and (M_n) is a sequence of $n \times n$-matrices, where each M_n has entries in a field K_n, such that $\mathcal{R}_{M_n}^{K_n}(\varepsilon n) \ge n^{1+\delta}$, then multiplication of vectors by the matrices M_n cannot be performed by linear circuits of linear size and logarithmic depth. For references to other applications see the paper by Lokam [6].

Lickteig [5] has shown that multiplication of vectors by $n \times n$-matrices in which the entries are square roots of distinct primes cannot be performed by a linear circuit of size $O(n^2/\log n)$. Similar results can be obtained for $n \times n$-matrices defined over the rationals in which the entries are very large integers, see [2, Chapters 9 and 13]. However, researchers have had less success in finding explicit matrices with corresponding properties and entries from a fixed finite set or even a field of size polynomial in n (which we shall refer to as a *small* field). By Valiant's result, an explicit sequence of rigid matrices would imply a size-depth tradeoff for their computation.

The best known lower bounds for the rigidity of explicit $n \times n$ matrices are $\Omega\left(\frac{n^2}{r}\log\frac{n}{r}\right)$ over a fixed finite field due to Friedman [3] and $\Omega\left(\frac{n^2}{r}\right)$ for various matrices with entries from a fixed finite set due to several authors [4, 7, 8, 9].

We start with a combinatorial lemma: if one changes fewer than $cn^2/r\log(n/r)$ entries of an $n \times n$-matrix M, where c is an absolute constant, then there will be an $r \times r$-submatrix of M which has not been altered (Corollary 2.2). By a $k \times k$-submatrix of an $n \times n$-matrix M we mean a matrix obtained from M by deleting some set of $n-k$ rows and $n-k$ columns of M.

To apply our combinatorial lemma we need to find $n \times n$-matrices for which any $r \times r$-submatrix has high rank. Over small fields, Cauchy matrices provide explicit examples of matrices of rigidity $\Omega\left(\frac{n^2}{r}\log\frac{n}{r}\right)$. To obtain examples over a fixed finite field $\mathbb{F}_q$, we use asymptotically good algebraic-geometric codes to construct a sequence of $n \times n$-matrices A_n with $\mathcal{R}^{\mathbb{F}_q}_{A_m}(r) \geq \frac{n^2}{8r}\log\frac{n}{2r-1}$ for all r satisfying $2/(\sqrt{q}-1) < r/n \leq 1/4$.

2. A Simple Combinatorial Lemma

Lemma 2.1. *If fewer than*

$$\mu(n,r) = n(n-r+1)\left(1-\left(\frac{r-1}{n}\right)^{\frac{1}{r}}\right)$$

entries of an $n \times n$ matrix are marked, then that matrix contains an $r \times r$ submatrix that contains no marks.

Proof. Let V_1 and V_2 be the set of rows and the columns of the matrix respectively, and consider the bipartite graph $G = (V_1 \cup V_2, E)$ which has an edge (x, y) if and only if the entry corresponding to column x and row y of the matrix has *not* been marked. Let R be the number of marks in the matrix. Obviously $|E| = n^2 - R$, and the matrix contains an unmarked square submatrix of size r if and only if G contains a complete bipartite subgraph $K(r, r)$ with $2r$ nodes. It is well known that if G has more than

$$(r-1)^{\frac{1}{r}}(n-r+1)n^{1-\frac{1}{r}} + (r-1)n = n^2 - \mu(n,r)$$

edges, then G contains a $K(r, r)$ subgraph (see, e.g., [1, p. 310]). Hence, this condition is satisfied for $R < \mu(n, r)$. □

In the sequel we will use the above lemma in the following form.

Corollary 2.2. *Let $\log^2 n \leq r \leq \frac{n}{2}$ and let n be sufficiently large. If in an $n \times n$ matrix fewer than*

$$\frac{n^2}{4r}\log\frac{n}{r-1}$$

entries are marked, then there exists an $r \times r$ submatrix that has not been marked.

Proof. As $n(n-r+1) \geq n^2/2$ for $r \leq n/2$, it suffices to prove that

$$\left(1-\left(\frac{r-1}{n}\right)^{\frac{1}{r}}\right) \geq \frac{1}{2r}\log\frac{n}{r-1}$$

for $r \geq \log^2 n$. A simple manipulation shows that the latter inequality is equivalent to

$$\left(1-\frac{1/2}{r/\log\frac{n}{r-1}}\right)^{r/\log\frac{n}{r-1}} \geq \left(\frac{r-1}{n}\right)^{1/\log\frac{n}{r-1}} = \frac{1}{2}.$$

This inequality is true for large n since for $r \geq \log^2 n$ the left-hand side converges to $1/\sqrt{e} > 1/2$. □

3. Rigidity over Small Fields

In this section, we construct $n \times n$ matrices over any field K_n that contains at least $2n$ elements. Let $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ be elements of a field K_n with the property that $\prod_{i \neq j}(x_i - x_j) \neq 0$, $\prod_{i \neq j}(y_i - y_j) \neq 0$, and $\prod_{i,j}(x_i + y_j) \neq 0$. It is easy to find such sets in any field with at least $2n$ elements. It is well known that the *Cauchy matrix*

$$C := \left(\frac{1}{x_i + y_j}\right)_{1 \leq i,j \leq n}$$

is generic, in the sense that for every $1 \leq r \leq n$ each of its $r \times r$-subdeterminants is nonzero. Corollary 2.2 implies:

Theorem 3.1. *Let K_n be a sequence of fields and let (C_n) be a sequence of Cauchy matrices where $C_n \in K_n^{n \times n}$. Then*

$$\mathcal{R}_{C_n}^{K_n}(r) = \Omega\left(\frac{n^2}{r} \log \frac{n}{r}\right),$$

provided $\log^2 n \leq r \leq n/2$.

4. Rigidity over Fixed Finite Fields

In this section we examine an infinite family of matrices with entries from a fixed finite field. These matrices are obtained from asymptotically good algebraic-geometric codes.

A linear $[n, k, d]$-code over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ in which each nonzero element has at least d nonzero entries.

Theorem 4.1. *Let q be a square prime power. There exists an explicit sequence of matrices $A_m \in \mathbb{F}_q^{n_m \times n_m}$, where n_m goes to infinity with m, such that for any r with* $\max\{2n_m/(\sqrt{q} - 1), \log^2 n_m\} < r \leq n_m/4$ *we have*

$$\mathcal{R}_{A_m}^{\mathbb{F}_q}(r) \geq \frac{n_m^2}{8r} \log \frac{n_m}{2r - 1}.$$

Proof. From the theory of algebraic-geometric codes [10] we know that there is an explicit sequence (Γ_m) of linear $[2n_m, n_m, d_m]$-codes over $\mathbb{F}_q$ satisfying $d_m \geq (1 - 2/(\sqrt{q} - 1))n_m$. Without loss of generality we may suppose that Γ_m has a generator matrix of the form $(I \mid A_m)$, where I is the $n_m \times n_m$-identity matrix. (A generator matrix of a code is a matrix whose rows form a basis of the code.) A $2r \times 2r$-submatrix of A_m of rank $< r$, would give rise to a nonzero codeword of weight at most $n_m - r < (1 - 2/(\sqrt{q} - 1))n_m \leq d_m$, which would be a contradiction. Thus, every $2r \times 2r$-submatrix of A_m has rank at least r. The theorem now follows from Corollary 2.2. □

5. Acknowledgements

We would like to thank an anonymous referee for very useful comments.

References

[1] B. Bollobás. *Extremal Graph Theory.* Academic Press, 1978.

[2] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory.* Springer Verlag, 1996. To appear.

[3] J. Friedman. A note on matrix rigidity. *Combinatorica*, 13(2):235–239, 1993.

[4] P. Kimmel and A. Settle. Reducing the rank of lower triangular all-ones matrix. Technical Report CS 92-21, Univ. of Chicago, November 1992.

[5] T. Lickteig. Ein elementarer Beweis für eine geometrische Gradschranke für die Zahl der Operationen bei der Berechnung von Polynomen. Diplomarbeit, Univ. Konstanz, 1980.

[6] S. Lokam. Spectral methods for matrix rigidity with applications to size-depth tradeoffs and communication complexity. In *36th Symposium on Foundations of Computer Science*, pages 6–15, 1995.

[7] P. Pudlák. Large communication in constant depth circuits. *Combinatorica*, 14(2):203–216, 1994.

[8] P. Pudlák and Z. Vavřín. Computation of rigidity of order n^2/r for one simple matrix. *Comment. Math. Univ. Carolinae*, 32(2):213–218, 1991.

[9] A. Razborov. On rigid matrices. (Manuscript, in Russian).

[10] M.A. Tsfasman and S.G. Vlădut. *Algebraic-Geometric Codes.* Mathematics and its Applications. Kluwer Academic Publishers, Dordrecht, 1991.

[11] L.G. Valiant. Graph theoretic arguments in low-level complexity. Number 53 in LNCS, pages 162–176. Springer Verlag, 1977.

M.A. Shokrollahi, V. Stemann
International Computer Science Institute
1947 Center Street, Suite 600
Berkeley, CA 94704–1198
USA
{amin,stemann}@icsi.berkeley.edu

D.A. Spielman
Department of Mathematics
Massachusetts Institute of Technology (MIT)
Cambridge, MA 02139
USA
spielman@math.mit.edu