A NOTE ON MATRIX RIGIDITY

Joel Friedman

CS-TR-308-91

June 1990

A Note on Matrix Rigidity

Joel Friedman*
Department of Computer Science
Princeton University
Princeton, NJ 08544

June 25, 1990

Abstract

In this paper we give an explicit construction of $n \times n$ matrices over finite fields which are somewhat rigid, in that if we change at most k entries in each row, its rank remains at least $Cn(\log_q k)/k$, where q is the size of the field and C is an absolute constant. Our matrices satify a somewhat stronger property, we which explain and call "strong rigidity." We introduce and briefly discuss strong rigidity, because it is in a sense a simpler property and may be easier to use in giving explicit constructions.

Recently there has been interest in giving explicit constructions of $n \times n$ matrices which are "rigid," in the sense that their rank is high and remains high when a few of their coefficients are changed (see [Val77], [Gri76], [Raz], and [PSR][1]). It is easy to construct $n \times n$ matrices over infinite fields, $\mathbf{F}$, such that when no more that k of the entries of each row are altered, the rank remains at least n/k; one can take a van der Monde matrix, for example. In this note we give an explicit construction of a matrix which is slightly more rigid than such a construction, for finite fields, $\mathbf{F}$, and k larger than some constant (depending on the size of the field). These matrices are actually "strongly rigid," in a sense that we will discuss later.

Theorem 1 *For any constant $C_1 > 0$ there is a constant $C_2 > 0$ such that the following holds. Let $\mathbf{F}$ be a finite field of q elements. Let A be an $n \times n$ matrix*

*This paper was written while on leave from Princeton, at the Hebrew University. The author wishes to acknowledge the National Science Foundation for supporting this research in part under PYI grant CCR–8858788, and a grant from the program of Medium and Long Term Research at Foreign Centers of Excellence.

[1]Pudlak and Savitzky have shown that over the real numbers, a Hadamard matrix of dimension n remains of rank r if no more that $n^2/(r^4 \log^2 r)$ of its entries are changed. Razborov has improved this to $n^2/(r^3 \log r)$.

such that the first $n/2$ rows are the basis of a linear error-correcting code in $\mathbf{F}^n$ of minimum distance $\geq C_1 n$. Then if B is any $n \times n$ matrix over $\mathbf{F}$ with at most k non-zero entries in each row, where $k \leq n/C_2$, we have

$$\operatorname{rank}(A+B) \geq \frac{n}{C_2 k}\Big(\log_q k + \log_q(q-1)\Big).$$

In the above theorem it is the "$\log_q k$" as opposed to the "$\log_q(q-1)$" which is of interest. We have included the "$\log_q(q-1)$" to remark that when $q \to \infty$ with fixed n and k, the construction does not completely degenerate.

The above matrices satisfy a stronger property, which we call "strong rigidity." After proving this theorem we define and discuss strong rigidity, because it is somewhat easier to work with and may be a useful point of view in constructing other explicit examples.

We recall that there are many types of explicitly specified codes, which for any value of q give a sequence of n's and a code for each such n of dimension $n/2$ and minimum distance $C_1 n$ with C_1 independent of q and n (one can take Justesen codes or Goppa codes, see respectively [vL82] and [vdGvL88]). Thus the above theorem, for any value of q and many of n, gives matrices rigid in the above sense.

Proof The first $n/2$ rows of A represent vectors $v_1, \ldots, v_{n/2}$ which are a basis of linear code (subspace) $\mathcal{C} \subset \mathbf{F}^n$ of minimum distance $\geq C_1 n$. Let $b_1, \cdots, b_{n/2}$ be the first $n/2$ rows of B. If the rank of the matrix consisting of the first $n/2$ rows of $A+B$ is t, then this is just to say that

$$\mathcal{E} \equiv \left\{ w \in \mathbf{F}^{n/2} \;\middle|\; \sum_{i=1}^{n/2} w_i(v_i + b_i) = 0 \right\}$$

(here 0 is the origin in $\mathbf{F}^n$) satisfies

$$\dim \mathcal{E} = \frac{n}{2} - t.$$

Since $\mathcal{E}$ is an $(n/2) - t$ dimensional subspace of $\mathbf{F}^{n/2}$, we can find a non-zero element $w \in \mathcal{E}$ of weight r for any r satisfying

$$\Big|\text{Hamming ball of raidus } r/2 \text{ in } \mathbf{F}^{n/2}\Big| \geq q^t,$$

or more crudely,

$$\binom{n/2}{r/2}(q-1)^{r/2} \geq q^t. \tag{1}$$

But for such a w we have

$$\sum_{i=1}^{n/2} w_i b_i \in \mathcal{C} - \{0\},$$

and so such an r must satisfy $rk \geq C_1 n$. So taking $r_0 = \lceil C_1 n/k \rceil - 1$, equation 1 cannot hold for $r = r_0$, that is to say that t is bounded below by

$$t \geq \log_q \left[\binom{n/2}{r_0/2} (q-1)^{r_0/2} \right] \geq \log_q \binom{n/2}{r_0/2} + \frac{r_0}{2} \log_q(q-1) \geq \frac{n}{C_2 k} \Big(\log_q k + \log_q(q-1) \Big),$$

for large enough C_2, also assuming $k \leq n/C_2$, where we have estimated

$$\log_q \binom{n/2}{r_0/2} \geq \log_q \left[\left(\frac{n}{2} - \frac{r_0}{2} \right)^{r_0/2} \Big/ (r_0/2)^{r_0/2} \right] \geq \frac{n}{C_2 k} \log_q k \ .$$

□

Definition 2 *$\mathcal{C} \subset \mathbf{F}^n$ is (k,t)-*strongly rigid *if every subspace $\mathcal{B}$ spanned by $c = \dim \mathcal{C}$ vectors $b_1, \ldots, b_c$, each of weight $\leq k$, has*

$$\dim(\mathcal{B} \cap \mathcal{C}) \leq \dim \mathcal{C} - t. \tag{2}$$

Glancing at the proof of theorem 1 shows that matrix A is actually (k,t)-strongly rigid with $t = n \log_q k/(C_2 k)$. Strong rigidity is a simpler property to check, in the sense that we do not care about the precise relations between a basis for $\mathcal{C}$ and of one for $\mathcal{B}$. Therefore, as in theorem 1, we hope that it may be easier to work with strong rigidity to give explicit constructions.

To compare strong rigidity to the usual notion of rigidity, we'll say that an $n \times n$ matrix A is (k,t)-rigid if whenever no more than k entries in each row of A are altered, then A's rank remains at least t. It is easy to see (and well-known) that if A is a "random" $n \times n$ matrix in an infinite or sufficiently large field, $\mathbf{F}$, then with high probability[2] A will be (k,t)-rigid with any $t \leq n - (nk)^{1/2}$.

While we cannot assert so large a value of t for the existence of strongly rigid matrices, we can obtain existence for a value of t which is interesting for the some of the intended applications of rigid matrices.

Theorem 3 *Let k, n be integers with $k \leq n/2$ and (for simplicity) n even. Then over any finite field, $\mathbf{F}$, there exists a (k,t)-strongly rigid code $\mathcal{C} \subset \mathbf{F}^n$ of dimension $n/2$, for any t with*

$$t \geq \frac{n}{8} - \frac{1}{2} k \log_q \frac{n}{k} - \frac{k}{4} - \frac{\log_q n}{4},$$

where q is the size of $\mathbf{F}$. The same holds for any infinite field, where in the above equation we substitute 0 for the two occurrences of $\log_q(\ )$, and where we require strict inequality. If we substitute "$n/10$" for the "$n/8$" in the above equation for t, then any $n \times n$ matrix over $\mathbf{F}$ is (k,t)-strongly rigid with "high probability."

[2] If $\mathbf{F}$ is infinite, the entries of A should be chosen from a distribution which has each field element weighted sufficiently small.

Proof This is, as usual, an easy counting argument (in the case of infinite fields one counts dimensions). For any subspaces $\mathcal{B}, \mathcal{C}$ of $\mathbf{F}^n$ with

$$\dim \mathcal{B} = \dim \mathcal{C}, \qquad \dim(\mathcal{B} \cap \mathcal{C}) \geq \dim \mathcal{C} - t, \tag{3}$$

it is easy to see that there exist $v_1, \ldots, v_t \in \mathbf{F}^n$ and $\ell_1, \ldots, \ell_t \in (\mathbf{F}^n)^*$ (i.e. the dual of $\mathbf{F}^n$ as an $\mathbf{F}$-vector space) such that

$$\mathcal{C} = \left\{ v \in \operatorname{sp}\langle B, v_1, \ldots, v_t \rangle \;\middle|\; \ell_i(w) = 0 \quad \forall i \right\}, \tag{4}$$

where $\operatorname{sp}\langle\ \rangle$ denotes the linear span. To see this, notice that equation 3 also implies

$$\dim(\mathcal{B} + \mathcal{C}) \leq \dim \mathcal{C} + t = \dim \mathcal{B} + t\ ;$$

hence we can choose v_i so that

$$\mathcal{B} + \mathcal{C} = \operatorname{sp}\langle \mathcal{B}, v_1, \ldots, v_t \rangle$$

and then choose ℓ_i so that equation 4 holds.

Equation 4 shows that to every code $\mathcal{C}$ of dimension $n/2$ which is not (k,t)-rigid there corresponds (at least one collection of) a $\mathcal{B}$ generated by $n/2$ vectors of weight $\leq k$ and vectors v_i and (dual) vectors ℓ_i as above. In the case of $\mathbf{F}$ finite, the number of vectors of weight $\leq k$ is

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

(assuming $k \leq n/2$), and so the total number of collections $(\mathcal{B}, \{v_i\}, \{\ell_i\})$ is bounded by

$$\leq \left[n(q-1)^k \binom{n}{k} \right]^{n/2} q^{2nt}. \tag{5}$$

On the other hand, the total number of subspaces of $\mathbf{F}^n$ of dimension $n/2$ is

$$\frac{(q^n-1)(q^n-q)\cdots\left(q^n - q^{(n/2)+1}\right)}{(q^{n/2}-1)(q^{n/2}-q)\cdots\left(q^{n/2}-q^{(n/2)-1}\right)} \geq \left(\frac{q^n-1}{q^{n/2}-1}\right)^{n/2} > \left(q^{n/2}\right)^{n/2}.$$

It follows that a (k,t)-rigid $\mathcal{C}$ of dimension $n/2$ exists provided that

$$q^{n^2/4} \geq \left[n(q-1)^k \binom{n}{k} \right]^{n/2} q^{2nt},$$

in particular, using $\binom{n}{k} \leq (n-k)^k/k^k$,

$$t \geq \frac{n}{8} - \frac{1}{2} k \log_q \frac{n}{k} - \frac{k}{4} - \frac{\log_q n}{4}.$$

Also, if we replace the $n/8$ in the above by $n/10$, then a randomly chosen $\mathcal{C}$ of dimension $n/2$ has probability $\leq n^{-n/40}$ of not being (k,t)-rigid.

If the field is infinite, then the dimension of the set of tuples $(\mathcal{B}, \{v_i\}, \{\ell_i\})$ as an $\mathbf{F}$ variety[3] is

$$\frac{kn}{2} + 2nt.$$

This, of course, is the $q \to \infty$ limit of $\log_q$ of the expression in equation 5. The same goes through for the set of all $\mathcal{C}$, i.e. subspaces of dimension $n/2$ in $\mathbf{F}^n$, meaning that one counts its dimension as an $\mathbf{F}$ variety (and gets the $q \to \infty$ limit of $\log q$ of the previously derived expression for finite fields). Therefore we get the aforementioned results, except that we need strict inequality in the inequality for t, and that when we use $n/10$ instead of $n/8$, "high probability" means occurs as a subvariety of codimension $\geq \lfloor n/40 \rfloor$.

□

J. Håstad has pointed out to me that the construction given in theorem 1 will, in general, be no better that (k,t)-rigid for t proportional to $n \log_q k/k$; that is, by starting with $\{b_i\}$ and then choosing appropriate $\{v_i\}$, one can construct many matrices A as in the theorem which are not (k,t)-rigid for some t of order $n \log_q k/k$.

The author wishes to thank A. Wigderson, J. Håstad, and A. Razborov for helpful discussions and comments.

References

[Gri76] D.Y. Grigorjev. *Notes of the Leningrad Branch of the Steklov Mathematical Institute of the Academy of Science of the USSR*, 60:38–48, 1976.

[PSR] Pudlak, Savitzky, and A. Razborov. Observations on rigidity of Hadamard matrices. Personal Communication.

[Raz] A. Razborov. On rigid matrices. *Problems of Pure and Applied Mathematics (Literal Translation from Russian).* to appear.

[Val77] L.G. Valiant. *Graph-theoretic arguments in low-level complexity.* Technical Report, University of Edinburgh, 1977. Computer Science Report 13-77.

[vdGvL88] G. van der Geer and J. van Lint. *Introduction to Coding Theory and Algebraic Geometry.* Birkhäuser Verlag, Boston, 1988.

[3]Throughout this paragraph we will, by a slight abuse of notation, use "$\mathbf{F}$ variety" to mean "algebraic set over $\mathbf{F}$." We do not require these sets to be irreducible.

[vL82] J. van Lint. *Introduction to Coding Theory.* Springer-Verlag, New York, 1982.