1 Matrix Rigidity continued

Matrix rigidity Let $A$ be a matrix over a field $\mathbb{F}$. Recall from last time that $R_r(A) = \min \{ \text{weight}(C) : \text{rk}(A - C) \leq r \}$, the rigidity function. We “proved” that if $\mathbb{F}$ is infinite, then for almost all $n \times n$ matrices $A$ we have that $R_r(A) = (n - r)^2$. So, if $r < (1 - \epsilon)n$ then $R_r(A) = \Omega(n^2)$ for almost all matrices. We don’t know any “explicit” examples of families of such matrices. But we know

**Theorem 20.1 (S. Lokam).** $R_{\sqrt{n}}(V_n(x_1, \ldots, x_n)) > cn^2$, where the $x_i$ are independent transcendentals.

For $r > 2\sqrt{n}$, even a $n^{1+\epsilon}$ lower bound is not known. We will see the idea for the proof by looking instead at the matrix in the following theorem:

**Theorem 20.2.** Let $P$ be the matrix with entries the square roots of the first $n^2$ primes, then $R_{\sqrt{n}}(P) > cn^2$.

We will use that the square roots of all square-free integers are linearly independent over $\mathbb{Q}$. The main tool in the proof is the Shoup-Smolensky invariant of a set of numbers. This is defined as follows: $S_t(a_1, \ldots, a_n) = \text{rk}_{\mathbb{Q}} \{ a_{i_1} \cdots a_{i_t} : 1 \leq i_1 < \cdots < i_t \leq m \}$. For example, $S_2(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ is the rank of $\{ \sqrt{6}, \sqrt{10}, \sqrt{14}, \sqrt{15}, \sqrt{21}, \sqrt{35} \} = 6$, while $S_3(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}) = 4$. If $A$ is an $n \times m$ matrix with entries $a_{i,j}$, then $S_t(A) = S_t(a_{1,1}, \ldots, a_{n,m})$. Also let $S_t^*(a_1, \ldots, a_n)$ is same as above, only with repetitions permitted. Obviously $S_t \leq S_t^*$.

**Lemma 20.3.** $S_t^*(AB) \leq S_t(A)S_t(B)$.

**Proof:** In $AB$, if we take the product of $t$ entries, then each such entry is a sum of products of pairs. So a $t$-wise product is going to be a sum of $t$-wise products from $A$ times $t$-wise products from $B$. So the space on the left hand side will be generated by those products. This proves the above bound.
Corollary 20.4. If $A \in M_n(\mathbb{F})$ with $rk(A) = r$, then $S^r_t(A) \leq \binom{nr+t-1}{t-1}^2$.

Proof: The rank of $A$ is less than or equal to $r$, if and only if $A$ can be represented as $A = BC$, where $B$ has $r$ columns and $C$ has $r$ rows. Hence $S^r_t(A) \leq S^r_t(B)S^r_t(C)$. Now each of those is no greater than the number of all $t$-wise products with repetition, which gives us the above binomial estimate. (Recall the cookies problem, where not everyone necessarily gets a cookie). In general, if $B$ is an $n \times r$ matrix, then $S^r_t(B) \leq \binom{nr+t-1}{t-1}$.

Lemma 20.5. With $P$ as in the theorem above (the one containing square roots of primes), suppose weight($C$) = $w$. Then $S_t(P - C) \geq \binom{n^2-w}{t}$. The proof is immediate (using the fact that square roots of the square-free positive integers are linearly independent). So if $w = R_r(P)$, we have that $\binom{n^2-w}{t} \leq S_t(P - C) \leq \binom{nr+t}{t}^2$. Setting $t = nr$, we get that $\binom{n^2-w}{nr} < \binom{nr+t}{nr} \leq \binom{2nr}{nr}^2 < 16^{nr}$. This gives us that $n^2 < 16$. We find that $w \geq n^2(1 - \frac{36r}{n})$. So we have shown that $R_r(P) \geq n^2(1 - \frac{36r}{n})$, which proves the theorem, if we set $r = \frac{n}{n}$. 

Exercise 20.6. Prove with a similar argument Lokam’s theorem, that $R_{\sqrt{n}/2}(V_n(x_1, \ldots, x_n)) > cn^2$.

Exercise 20.7. Prove the same when $x_i = p_i^{1/n}$.

Note, that $\dim \mathbb{Q}(p_1^{1/n}, \ldots, p_n^{1/n}) = n^2$, so this is not very “explicit” either.

A linear code of length $n$ and dimension $k$ over $\mathbb{F}_q$ is an $k$-dimensional subspace $C$ in $\mathbb{F}_q^n$. The information rate is $\frac{k}{n}$. The idea is that our original message is in $\mathbb{F}_q^k$, and is encoded using the encoding $\mathbb{F}_q^k \cong C$. The minimum weight of $C$ is the minimum of the weights of all $x \in C$, $x \neq 0$. The Hamming distance of $x, y \in \mathbb{F}_q^n$ is the weight of $x - y$. For any $x \neq y$ with $x, y \in C$, $\text{dist}(x, y) \geq \text{minweight}(C)$. Let $d = \text{minweight}(C)$, the coding distance. In noisy transmission, up to $d - 1$ errors can be recognized, and up to $d - 1$ errors can be uniquely corrected. The goal of algebraic coding theory is to find codes with large information rate and large coding distance, and of course that are explicit.

Suppose $C \leq \mathbb{F}_q^n$, $\dim C = k$. Then $\dim C^\perp = n - k$. A basis of $C^\perp$ will be given by a $n - k \times n$ matrix $B$.

Exercise 20.8. $\text{minweight}(C) \geq d$ iff the rows of $B$ are $d - 1$-wise linearly independent.

OPEN QUESTION: Do there exist good cyclic codes (cyclic codes are those where a cyclic permutation of the entries preserves the space.) Good means $\frac{k}{n} = \Omega(1)$, $d = \Theta(n)$.

In $\mathbb{F}_q^n$, we have $q$ vectors that were $n$-wise independent, namely the elements of the form $(1, a, a^2, \ldots, a^{d-1})$. This will give us a code in $\mathbb{F}_q^n$. Then, $\dim C^\perp = d$, rate is $1 - \frac{q}{n}$. If we do this over a large field, we get excellent rate and error-correction. These are good codes over large field. What we want though is a family of codes which is good over a fixed finite field. Most important are the binary codes, over $\mathbb{F}_2$. 

2