“Prolixity” for Random Functions from the Log-Rank Bound

In this short note we show that a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ chosen uniformly at random has $D(f) \geq n-1$ with high probability. We use the familiar:

Log-Rank Bound. *Let M_f be the $2^n \times 2^n$ matrix (over $\mathbb{F}_2$) associated to f, ie $(M_f)_{x,y} = f(x,y)$. Then $D(f) \geq \log_2 \operatorname{rank}(M_f)$.*

Although the result is weaker than the one proved in the seminar (where the rank in the conclusion was over $\mathbb{R}$), it will turn out to be enough for our purposes. The only other observation we will need is that random $N \times N$ matrices over finite fields have rank $(1-o(1))N$ with high probability. We will actually just need a weak version of this:

Random Matrices Have High Rank. *Let A be chosen uniformly at random from $\operatorname{Mat}_{N\times N}(\mathbb{F}_q)$. Then $\Pr[\operatorname{rank}(A) \geq N/2]$ is at least $1 - \frac{N}{2q^{N/2}}$.*

Proof. We will underestimate the probability in question by just looking at the odds that the first $N/2$ columns of A are linearly independent. To do that, we count the number of A where this happens:

$$\underbrace{\left(q^N-1\right)}_{\text{choose 1st col} \neq 0} \quad \times \quad \underbrace{\left(q^N-q\right)}_{\substack{\text{choose 2nd col} \\ \text{not in span of 1st}}} \quad \times \quad \cdots \quad \times \quad \underbrace{\left(q^N-q^{\frac{N}{2}-1}\right)}_{\substack{(N/2)^{\text{th}} \text{ col not in} \\ \text{span of previous cols}}}$$

Dividing by the number of possible first $N/2$ columns, we get

$$\begin{aligned}
\Pr[\operatorname{rank}(A) \geq N/2] &\geq \left(q^N-1\right)\left(q^N-q\right)\cdots\left(q^N-q^{\frac{N}{2}-1}\right) / \left(q^N\right)^{\frac{N}{2}} \\
&= \left(1-\frac{1}{q^N}\right)\left(1-\frac{1}{q^{N-1}}\right)\cdots\left(1-\frac{1}{q^{\frac{N}{2}+1}}\right)
\end{aligned}$$

As $N \to \infty$, the latter quantity tends to 1. More precisely, it is not hard to show that this quantity, and hence the probability of A being at least “half-rank”, is bounded below by $e^{-N/2q^{N/2}} > 1 - \frac{N}{2q^{N/2}}$. $\square$

Note that, unlike what Pietro guessed during the seminar, a random matrix over $\mathbb{F}_2$ does *not* have full rank with high probability, as its dimensions go to infinity. In fact, the odds that a random $\mathbb{F}_2$-matrix has full rank converges to a finite number strictly between 0 and 1; numerical calculations suggest something around 0.27. Fortunately we don't need full rank to get good lower bounds on $D(f)$:

Random Functions Make You Wordy. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be chosen uniformly at random. Then f has communication complexity at least $n-1$ with probability at least $1 - \frac{1}{2^{2^{n-1}-n+1}}$.*

Proof. Use the high rank lemma with $N = 2^n$ and $q = 2$, then apply the log-rank bound. $\square$