1 Razborov's Set Disjointness Lower Bound (conclusion)

Today we will complete the proof of Step 2 of the lower bound proof.

Proof. **(continued)**

We wish to prove a rank lower bound for any matrix Q that approximates the communication matrix M_f for the set disjointness function f. For concreteness, we will specialize our proof to the case of the matrix P, which gives the probability of acceptance for pairs of inputs.
Recall that we had

$$\begin{aligned} p(i) &= \text{average probability of acceptance on inputs } (x,y) \text{ given } |x \cap y| = i, |x| = |y| = k = \frac{n}{8} \\ &= \begin{cases} \geq \frac{2}{3} & \text{if } i = 0\text{, and} \\ \leq \frac{1}{3} & \text{if } i > 0. \end{cases} \end{aligned}$$

Moreover,

$$\begin{aligned} p(i) &= \sum_{t=0}^{k} a_t \lambda_{i,t}, \text{ and} \\ \lambda_{i,t} & \begin{cases} \text{is a polynomial in } i \text{ of degree} \leq t \\ \leq N^{-1} exp(-\alpha t) \quad \text{for some constant } \alpha\text{, where } N = \binom{n}{k}. \end{cases} \end{aligned}$$

Also, recall that $\operatorname{rank}(P) \leq 2^{2m}$, P is an $N \times N$ matrix, and $0 \leq P(x,y) \leq 1$.
The polynomial p has degree k. We first derive a polynomial $\tilde{p}$ from it that has degree $O(m)$ and continues to approximate the NOR function.
Note that

$$\| P \|_{\mathrm{tr}} \leq 2^{2m} \|P\|,$$

where $\| \cdot \|$ is the 2-norm, defined as $\|P\| = \max_{|\phi\rangle} \|P|\phi\rangle\|$. It is also equal to the maximum singular value of P. For any unit vector $|\phi\rangle = \sum_i \alpha_i |i\rangle$,

$$\begin{aligned} \|P|\phi\rangle\|^2 &= \sum_i |(P|\phi\rangle)_i|^2 \\ &= \sum_i \left| \sum_j P_{ij} x_j \right|^2 \\ &\leq \sum_i \left| \sum_j P_{ij}^2 \right| \cdot \left| \sum_j |\alpha_j|^2 \right| \quad \text{(by Cauchy-Schwartz)} \\ &\leq \sum_i N = N^2. \end{aligned}$$

So $\|P\| \leq N$ and $\| P \|_{\mathrm{tr}} \leq N 2^{2m}$, and $\left\| \tilde{P} \right\|_{\mathrm{tr}} = \| P \|_{\mathrm{tr}} \leq N 2^{2m}$.

Further recall that a_t is the sum of the diagonal entries of $\tilde{P}$ corresponding to the eigenspace E_t. Therefore, $\sum_{t=0}^{k} |a_t| \leq \sum_j \left|\tilde{P}_{jj}\right| \leq 2^{2m} N$.

This bound allows us to drop all the terms $\lambda_{i,t}$ of degree larger than $O(m)$. Define

$$\tilde{p}(i) = \sum_{t=0}^{dm} a_t \lambda_{i,t},$$

where d is a large enough constant. (Taking $d = 3/\alpha$ suffices for our purposes. Here, α is the constant in the bound on the magnitude of $\lambda_{i,t}$.) Now $\tilde{p}(i)$ is a polynomial in i of degree at most dm. Moreover,

$$\begin{aligned}
|\tilde{p}(i) - p(i)| &\leq \sum_{t=dm+1}^{k} |a_t \lambda_{i,t}| \\
&\leq \sum_{t=dm+1}^{k} \frac{|a_t|}{N} \mathrm{e}^{-\alpha t} \\
&\leq \frac{\mathrm{e}^{-dm}}{N} \sum_{t>dm} |a_t| \\
&\leq 2^{2m} \mathrm{e}^{-dm} \leq \mathrm{e}^{-m}.
\end{aligned}$$

Thus, $\tilde{p}$ also approximates the logical NOR function.

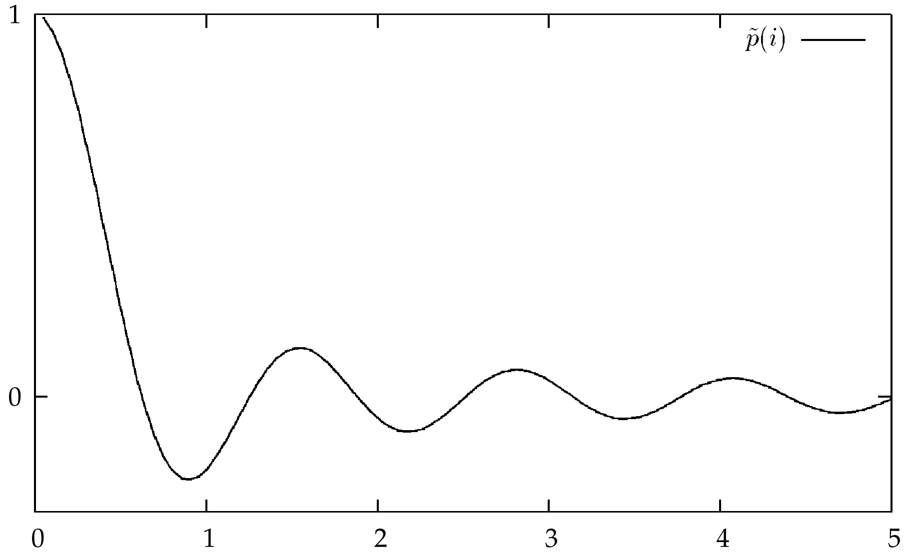

Figure 1: The approximating polynomial $\tilde{p}(i)$.

Fact : [Paturi'92] Any univariate polynomial $q(u)$ that is within ϵ of 1 at $u = 0$, and within ϵ of 0 at integer points $u = 1, 2, \ldots, k$, for a constant $\epsilon < 1/2$ has degree at least $\Omega(\sqrt{k})$.

Since $k = n/8$, $dm \geq \deg(\tilde{p}) \in \Omega(\sqrt{n})$, and $m \in \Omega(\sqrt{n})$. This is equivalent to saying that the rank of any matrix approximating M_f (in ℓ_∞) to within some constant (say $\frac{1}{3}$), is at least $2^{\Omega(\sqrt{n})}$. This concludes Razborov's proof of the set disjointness lower bound. □

2 Mixed States

We will now switch topics and study a bit of quantum cryptography. We start with some basic elements of quantum information theory that are required for this.

So far, we have considered qubit states given by superpositions. These are also called *pure* states. We may also consider a qubit system that is in a random superposition $|\phi_i\rangle$ picked according to a distribution $\{p_i\}$. Such a state is called a *mixed* state. These states arise naturally when one considers subsystems of qubits in a pure state.

As an example, take the EPR (Einstein-Podolsky-Rosen) pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, where the first qubit is with Alice, and the second with Bob. Consider the following scenarios

a) Alice measures her qubit in the basis $\{|0\rangle, |1\rangle\}$, leaving Bob's qubit in a mixed state $\left\{\left(\frac{1}{2}, |0\rangle\right), \left(\frac{1}{2}, |1\rangle\right)\right\}$.

b) Alice measures her qubit in the Hadamard basis $\left\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. In order to determine Bob's state, we apply the projectors corresponding to the outcome that Alice's experiment may have, yielding

$$\begin{aligned}(|+\rangle\langle+| \otimes I)\,\frac{|00\rangle + |11\rangle}{\sqrt{2}} &= \frac{|+\rangle\langle+|0\rangle|0\rangle + |+\rangle\langle+|1\rangle|1\rangle}{\sqrt{2}} \\ &= \frac{|+\rangle|0\rangle + |+\rangle|1\rangle}{\sqrt{2}} = \frac{|+\rangle|+\rangle}{2},\end{aligned}$$

with probability $\frac{1}{2}$. Similarly, the joint state is $\frac{|-\rangle|-\rangle}{2}$ with probability $\frac{1}{2}$. So Bob's (mixed) state is $\left\{\left(\frac{1}{2}, |+\rangle\right), \left(\frac{1}{2}, |-\rangle\right)\right\}$.

These are two different mixtures, but they are equivalent in a strong sense. For example, if we measure the mixtures in the standard basis, we get the same distribution on outcomes. This holds for any possible measurement that Bob may do.

Remark. In fact this property continues to hold regardless of which measurement Alice does at her end. This explains why instantaneous (therefore superluminal) signalling is not possible using entangled quantum states.

The above property is not captured in the probability distribution description of mixed states. We need a different representation of mixed states to capture this.

2.1 The Density Matrix

Let $\{p_i, |\phi_i\rangle\}$ be a mixed state, and $\{\Pi_j\}$ be a von Neumann measurement.

$$\begin{aligned}\Pr(\text{outcome } j) &= \sum_i p_i \,\| \Pi_j |\phi_i\rangle \|^2 \\ &= \sum_i p_i \langle\phi_i|\Pi_j|\phi_i\rangle \\ &= \sum_i p_i \mathrm{Tr}\left(\Pi_j |\phi_i\rangle\langle\phi_i|\right) \\ &= \mathrm{Tr}\left(\sum_i p_i \Pi_j |\phi_i\rangle\langle\phi_i|\right) \\ &= \mathrm{Tr}\left(\Pi_j \sum_i p_i |\phi_i\rangle\langle\phi_i|\right) \\ &= \mathrm{Tr}\left(\Pi_j \rho\right),\end{aligned}$$

where we define $\rho = \sum_i |\phi_i\rangle\langle\phi_i|$ to be the *density matrix* representing the mixed state $\{p_i, |\phi_i\rangle\}$. Note that the mixtures $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ and $\{(\frac{1}{2}, |-\rangle), (\frac{1}{2}, |+\rangle)\}$ have the same density matrix. Checking explicitly

$$\begin{aligned}
\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} &= \frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\frac{|-\rangle\langle -| + |+\rangle\langle +|}{2} &= \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Thus, they give rise to the same probability density on any measurement.

On any computation, a mixtures evolves as

$$\{p_i, |\phi_i\rangle\} \xrightarrow{U} \{p_i, U|\phi_i\rangle\}.$$

The new density matrix is

$$\sum_i p_i U|\phi_i\rangle\langle\phi_i|U^\dagger \quad = \quad U\left(\sum_i p_i|\phi_i\rangle\langle\phi_i|\right)U^\dagger,$$

so two mixed states with density matrix ρ result in the same density matrix $U\rho U^\dagger$. Thus the density matrix completely captures the physical behaviour of a mixed state. We will therefore identify a mixed state with its density matrix.

2.2 Purifications

Whenever we get a density matrix ρ by measuring part of a pure state $|\phi\rangle$, the state $|\phi\rangle$ is said to be a purification of ρ. The state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is a purification of the two mixtures $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ and $\{(\frac{1}{2}, |-\rangle), (\frac{1}{2}, |+\rangle)\}$. Formally,

Definition 1. *A state $|\phi\rangle \in \mathcal{H} \otimes \mathcal{K}$ is said to be a purification of a density matrix ρ over the space $\mathcal{K}$ (or of any mixed state that has this density matrix ρ) if*

$$\mathrm{Tr}_{\mathcal{H}}(|\phi\rangle\langle\phi|) = \rho.$$

The operation $\mathrm{Tr}_{\mathcal{H}}$ captures the measurement of the $\mathcal{H}$-part of the pure state, and is called *the partial trace over $\mathcal{H}$*. If we take $|\phi\rangle = \sum_h \alpha_h |h\rangle|\phi_h\rangle$ and measure the first subsystem in the basis $\{|h\rangle\}$, then we get the mixture $\{|\alpha_h|^2, |\phi_h\rangle\}$ with density matrix $\sum_h |\alpha|^2 |\phi_h\rangle\langle\phi_h|$. Note that

$$|\phi\rangle\langle\phi| = \sum_{h_1,h_2} \alpha_{h_1}\alpha^*_{h_2} |h_1\rangle\langle h_2| \otimes |\phi_{h_1}\rangle\langle\phi_{h_2}|$$

We can formally define the partial trace to be

$$\mathrm{Tr}_{\mathcal{H}}(|\phi\rangle\langle\phi|) = \sum_h \langle h| \otimes I(|\phi\rangle\langle\phi|)|h\rangle \otimes I.$$

As with the trace operation, the partial trace is independent of the basis $\{|h\rangle\}$ used to define it. We leave it to the reader to verify this fact.