Overview of the Goldreich-Levin List Decoder for Hadamard Codes

David Zuckerman, CS 395T notes

March 26, 2019

We view the GL decoder as a reduction from list-decoding to unique-decoding. Fix a linear polynomial $\mathbf{L} : \mathbb{F}_2^m \to \mathbb{F}_2$ within distance $\eta = \frac{1}{2} - \varepsilon$ from the received word $\mathbf{R} : \mathbb{F}_2^m \to \mathbb{F}_2$. Pick a random subspace $\mathbf{A}$ of dimension k. Assume that we guess the correct values of $\mathbf{L}$ on $\mathbf{A}$; in reality we will cycle over all 2^k possible values for $\mathbf{L}$ on $\mathbf{A}$. From these values, we can determine the value of $\mathbf{L}$ at any point $\mathbf{b} \in \mathbb{F}_2^n$.

To see how, consider the $k+1$ dimensional subspace $\mathbf{A'}$ spanned by $\mathbf{b}$ and the vectors in $\mathbf{A}$. The error rate is 0 on $\mathbf{A}$, because we assume our guess is correct. We use the received word $\mathbf{R}$ restricted to the affine space $\mathbf{b} + \mathbf{A}$ as our best guess for $\mathbf{L}$ on this affine space. The error rate on the affine space $\mathbf{b} + \mathbf{A}$ is roughly η, the error rate of $\mathbf{R}$, as picking a random subspace corresponds to picking pairwise independent points. One can use pairwise independence and Chebyshev's inequality to show that the probability that the error rate on this affine space is not less than $1/2$ is $O(\frac{1}{\varepsilon^2|A|})$.

Therefore, the overall error-rate on $\mathbf{A'}$ is likely to be the average of these, or $\eta/2 < \frac{1}{4}$. If the error rate is less than $1/4$, then we win, as this is within the unique decoding radius. We can correct the values on $\mathbf{A'}$ by unique decoding. This gives us $\mathbf{L}(\mathbf{b})$.

It's natural to choose $|\mathbf{A}| = Cm/\varepsilon^2$ for a large enough constant C. This will ensure that the error probability for recovering $\mathbf{L}(\mathbf{b})$ is at most $1/(3m)$ (say). We can then recover $\mathbf{L}$ at a basis for $\mathbb{F}_2^m$, and by the union bound the probability that there exists an error at a basis element is at most $m/3m = 1/3$. Once $\mathbf{L}$ is known on a basis, it is known everywhere. Note that the list size is the number of guesses for $\mathbf{L}$ restricted to $\mathbf{A}$. This is determined by the values of $\mathbf{L}$ on the k basis elements of $\mathbf{A}$, and hence the list size is $2^k = |\mathbf{A}|$.

It's even better to choose $|\mathbf{A}| = O(1/\varepsilon^2)$. Now the error probability for recovering $\mathbf{L}(\mathbf{b})$ is at most .1 (say). Instead of using an ordinary basis, we can use a robust version of a basis that can interpolate $\mathbf{L}$ even if a .1 fraction of points are wrong. Such robust interpolating sets are known, and this approach yields the tight list size of $O(\varepsilon^{-2})$.