The STV worst-case to average-case reduction

Amnon Ta-Shma and Dean Doron

In this lecture we do the following:

- We explain the connection between local list-decoding and worst-case to average-case reductions for PSPACE.
- We prove that if there exists a language in PSPACE that is worst-case hard for SIZE(s), then there exists another language in PSPACE that has extreme average-case hardness for SIZE(s'), for s' slightly smaller than s.

1 Local list decoding and worst-case to average-case reductions

**Theorem 1.** Suppose \( f : \{0,1\}^n \to \{0,1\} \) is a function such that \( \text{Size}(f) > s(n) \). We also view \( f \) as \( f : [N = 2^n] \to \{0,1\} \) or alternatively as \( f : \{0,1\}^N \) (i.e., we represent the function by its truth table). Given \( \varepsilon > 0 \), let \( C \) be a \([N',N]\) binary code such that:

- \( C \) is a \((\varepsilon, L = \text{poly}(\log N, \frac{1}{\varepsilon}))\) locally list-decodable code, and,
- \( N' = \text{poly}(N, \frac{1}{\varepsilon}) \).

Define \( f' = C(f) \in \{0,1\}^{N'} \). Again we view \( f' \) as \([N'] \to \{0,1\} \) or equivalently as \( f' : \{0,1\}^{n'} \to \{0,1\} \) where \( N' = 2^{n'} \) (so we identify a function with its truth-table). Then, there exists a constant \( c \) such that \( \text{Size}_{\frac{1}{2} + \varepsilon}(f')(n') > \left( \frac{\varepsilon}{n} \right)^c \cdot s(n') \).

**Proof.** Let \( A' \) be the smallest circuit computing \( f' \) correctly on more than a \( \frac{1}{2} + \varepsilon \) fraction of the inputs of length \( n' \), and let \( n' \) be its size. Viewing \( f' \) as a word in \( \mathbb{F}_2^{N'} \), there exists \( j \in [L] \) such that with high probability, \( R^A(f', j, \cdot) = C(f) \) where \( R \) is the list-decoding algorithm for \( C \) guaranteed by Theorem 9 of Lecture 3.

Since the running time of \( R \) is \( t = \text{poly}(\log N', \frac{1}{\varepsilon}) \) oracle calls of \( A \), for every \( j \in [L] \) there exists a circuit \( M_j \) of size at most \( t \cdot s' \text{poly}(\frac{N}{\varepsilon}) \). Let \( M_{j_0} \) be the circuit that outputs \( f \) with high probability (we stress that getting \( f \) from the output \( C(f) \) is easy).

The circuit \( M_{j_0} \) uses randomness, however by standard amplification (thus paying in size) we can bring down the error to be exponentially-small so there exists a fixing of the random bits that is good for every input (prove it). The “derandomized” variant of \( M_{j_0} \) is of size \( O(n') \cdot \text{poly}(\frac{N}{\varepsilon}) \cdot s' \), and computes \( f \) exactly. Since, it must be at least \( s(n) \) we get a lower bound on \( s' \).

Plugging-in a small enough \( \varepsilon = s^{-\Omega(1)} \) and assuming \( \varepsilon < \frac{1}{n} \), we obtain:

**Corollary 2.** Suppose \( f : \{0,1\}^n \to \{0,1\} \) is a function that no circuit of size \( s(n) \) computes in the worst case. Then, there exists an explicit function \( f' = C(f) : \{0,1\}^{O(n)} \to \{0,1\} \) such that no circuit of size \( s' = \sqrt{s} \) computes \( f' \) correctly on more than a \( \frac{1}{2} + s^{-\Omega(1)} \) fraction of the inputs.
2 Worst-case to average case reductions for PSPACE

We next observe that if \( f \in \text{PSPACE} \) (as a function on an \( n \) bit input), and we choose \( C = \text{RM} \circ \text{Had} \) we used in Lecture 4, then \( f' = C(f) \), viewed as a function on \( n' \) bits, is also in \( \text{PSPACE} \).

**Proof.** View \( f \) as \( f : [N = 2^n] \to \{0, 1\} \) and let \( i \in \{0, 1\}^{n'} = [N'] \). Denote \( \text{RM} : \{0, 1\}^N \to \mathbb{F}_q^N \) with \( H = n, m = \frac{n}{\log n} \) and \( q = \text{poly}(n) \). Take \( \text{Had} : \{0, 1\}^{\log q} \to \{0, 1\}^q \). Then \( N' = N_0 \cdot q = \text{poly}(N) \), so \( n' = O(n) \). Write \( i = (a, b) \) where \( a \in [N_0] \) and \( b \in \mathbb{F}_q \), and recall that \( f'(i) = \text{Had}((\text{RM}(f))a)_b = \langle \text{RM}(f)_a, b \rangle_2 \).

It is then left to show how to compute a specific index of \( \text{RM}(f) \) in a space-efficient way (and using \( f \in \text{PSPACE} \)). \( \text{RM}(f) \) is viewed as a multivariate polynomial \( p : \mathbb{F}_q^m \to \mathbb{F}_q \) found by interpolation. We leave it as an exercise (do it!). Thus, \( f' \) is also in \( \text{PSPACE} \). \( \square \)

Clearly, a similar result holds for class above \( \text{PSPACE} \) (such as \( \text{E} \)).

We can therefore deduce the following strong worst-case to average-case reduction for \( \text{PSPACE} \):

**Theorem 3.** If there exists an \( f = \{f_n\} \in \text{PSPACE} \) such that \( \text{Size}(f) > s(n) \), then there exists another \( f' = \{f'_n\} \in \text{PSPACE} \) such that \( \text{Size}_{\frac{1}{2} + \Omega(1)}(f') > \sqrt{s(n)} \).