Derandomization (VI)

Yijia Chen

Shanghai Jiao Tong University

December 23, 2012

Efficient Decoding

Theorem (Unique decoding for Reed-Solomon)

There is a polynomial time algorithm $\mathbb{A}$ *such that given a list* $(a_1, b_1), \ldots, (a_m, b_m)$ *of pairs of elements of a finite field* $\mathbb{F}$ *such that there is a* d*-degree polynomial* $G : \mathbb{F} \to \mathbb{F}$ *satisfying* $G(a_i) = b_i$ *for more than* $m/2 + d/2$ *many* $i \in [m]$*, the algorithm recovers* G*.*

Proof (1)

Consider the error locator polynomial

$$E(x) := \prod_{i \in [m] \text{ with } G(a_i) \neq b_i} (x - a_i),$$

which has degree $< m/2 - d/2$.
Then let

$$P(x) := G(x) \cdot E(x)$$

be a polynomial of degree $< m/2 + d/2$. Thus

$$P(a_i) = G(a_i) \cdot E(a_i) = b_i \cdot E(a_i)$$

for every $i \in [m]$

Proof (2)

Conversely, assume that there are two nonzero polynomials $P(x)$ and $E(x)$ such that

$$P(a_i) = b_i \cdot E(a_i)$$

for all $i \in [m]$, where $P(x)$ had degree $< m/2 + d/2$ and $E(x)$ has degree $< m/2 - d/2$.

We consider the polynomial

$$P(x) - G(x) \cdot E(x)$$

which has degree $< m/2 + d/2$. By assumption, it has more than $m/2 + d/2$ zeros, and hence is a zero polynomial.

We conclude

$$G(x) = \frac{P(x)}{E(x)}.$$

Proof (3)

The Berlekamp-Welch Procedure finds a pair $(P(x), E(x))$ by solving the linear equations

$$P(a_i) = b_i \cdot E(a_i)$$

for all $i \in [m]$. $\square$

Decoding concatenated codes

Let $E_1 : \{0,1\}^n \to \Sigma^m$ and $E_2 : \Sigma \to \{0,1\}^k$ be two error correcting codes, then

$$E_2 \circ E_1 : x \mapsto E_2(E_1(x)_1), \ldots, E_2(E_1(x)_m)$$

is an error correcting code from $\{0,1\}^n$ to $\{0,1\}^{m \cdot k}$.

Assume that we have a decoder for E_1 (respectively, E_2) that can handle ρ_1 (ρ_2, respectively) errors, then there is a decoder for $E_2 \circ E_1$ that can handle $\rho_1 \cdot \rho_2$ errors.

Local Decoding and Hardness Amplification

Definition

Let $E : \{0,1\}^n \to \{0,1\}^m$ be an error correcting code and $\rho > 0$. A *local decoder for* E *handling* ρ *errors* is a probabilistic algorithm $\mathbb{D}$ such that given random access to a string $y \in \{0,1\}^m$ with $\Delta(y, E(x)) < \rho$ for some (unknown) $x \in \{0,1\}^n$ and an index $j \in [n]$ the algorithm $\mathbb{D}$ runs in time $(\log m)^{O(1)}$ and output x_j with probability at least $2/3$.

Hardness amplification from local decoding

Theorem

Assume that there exists an error correcting code with polynomial time encoding algorithm and a local decoding algorithm handling ρ errors. If there is a function $f \in \mathbf{E}$ with

$$H_{\text{wrs}}(f)(n) \geq S(n)$$

for some function $S : \mathbb{N} \to \mathbb{N}$ with $S(n) \geq n$ for every $n \in \mathbb{N}$. Then there exists a function $\hat{f} \in \mathbf{E}$ with

$$H_{\text{avg}}^{1-\rho}(\hat{f})(n) \geq S(\varepsilon \cdot n)^{\varepsilon}$$

for some $\varepsilon > 0$.

Local decoder for Walsh-Hadamard

Theorem

Let $\rho < 1/4$. Then the Walsh-Hadamard code has a local decoder handling ρ errors, which only makes two queries for each input.

Proof (1)

Recall that the function $\mathrm{WH} : \{0,1\}^n \to \{0,1\}^{2^n}$ maps every string $x \in \{0,1\}^n$ into the string $z \in \{0,1\}^{2^n}$ satisfying

$$z_y = x \odot y = \sum_{i=1}^{n} x_i \cdot y_i \pmod 2$$

for every $y \in \{0,1\}^n$.

Proof (2)

Recall that the function $\mathrm{WH} : \{0,1\}^n \to \{0,1\}^{2^n}$ maps every string $x \in \{0,1\}^n$ into the string $z \in \{0,1\}^{2^n}$ satisfying

$$z_y = x \odot y = \sum_{i=1}^{n} x_i \cdot y_i \pmod 2$$

for every $y \in \{0,1\}^n$.

Input: $j \in [n]$, random access to a function $f : \{0,1\}^n \to \{0,1\}$ such that

$$\Pr_y[f(y) \neq x \odot y] \leq \rho < 1/4$$

and $x \in \{0,1\}^n$.

Output: A bit $b \in \{0,1\}$. (*Our goal*: $b = x_j$.)

Proof (3)

Algorithm: Let $e^j \in \{0,1\}^n$ be the string whose every bit is 0 except the j-th bit. The algorithm chooses $y \in \{0,1\}^n$ uniformly at random and then outputs

$$f(y) + f(y + e^j) \pmod 2,$$

where $y + e^j$ is obtained from y by flipping the j-th bit of y.

Proof (4)

Since both y and $y + e^j$ are uniformly distributed (although they are dependent), the union bound implies that with probability $1 - 2 \cdot \rho$ we have

$$f(y) = x \odot y \quad \text{and} \quad f(y + e^j) = x \odot (y + e^j).$$

Then

$$\begin{aligned} f(y) + f(y + e^j) &= x \odot y + x \odot (y + e^j) \\ &= 2 \cdot (x \odot y) + x \odot e^j \\ &= x \odot e^j = x_j \pmod{2} \end{aligned}$$

□

Thank you