CS761 Derandomization and Pseudorandomness **2022-23 Sem I**

Lecture 14: 29-09-2022

Scribe: Amit Rajaraman *Lecturer: Rohit Gurjar*

Definition 14.1 (Multiplicity code)**.** *Let $\mathbb{F}$ be a finite field of size at least n, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. The message set is $\{f \in \mathbb{F}[x], \deg f < k\}$. We map f to the n-dimensional vector M over $\mathbb{F}^s$, where*

$$(M_i)_j = f^{(j)}(\alpha_i) = \frac{\partial^{j-1} f}{\partial x^{j-1}}(\alpha_i).$$

When talking about the derivative, we mean the *syntactic* derivative, which evaluates (on exponents of x) exactly the same as ordinary derivatives in functions over $\mathbb{R}$.
Note that the messages are encoded in $\mathbb{F}^s$, so errors mean errors anywhere in an entire vector of derivatives.

The rate of this code is approximately k/ns, which is worse than in Reed-Solomon codes. The distance however, jumps up to $n - \frac{k-1}{s}$!
A unique decoding algorithm for the multiplicity is very similar to Berlekamp-Welch, and we omit the details.

Note that in contrast to Reed-Solomon codes, we can allow the degree of the polynomial to be more than n.

Theorem 14.2 (Neilsen '01, Kopparty '13, Guruswami-Wang '14)**.** *For every $\epsilon > 0$, for sufficiently large s, univariate multiplicity codes are efficiently list decodable from fractional agreement $\frac{k}{ns} + \epsilon$.*

We can get arbitrarily close to the (hard) bound (!) – we cannot hope to get a degree k polynomial with fewer than k datapoints. Further, this can be done with a constant list size, with the constant depending on ϵ. This was shown by Kopparty, Saraf, Ron-Zewi, and Wootters in 2018.
The fraction of agreement here is $\frac{k}{sn} + \epsilon = \text{Rate} + \epsilon$. Compare this to what we had studied about Reed-Solomon codes, where we only had $\sqrt{\text{Rate}}$.

The remainder of this section is dedicated to the proof of this theorem; we shall look at the version due to Guruswami-Wang.

The input to the algorithm is an $s \times n$ matrix Y. We wish to find all polynomials p of degree at most k whose encoding has "large" agreement with Y. More precisely, there is a set $T \subseteq [n]$ of size greater than t such that for all $i \in T$ and $j \in [s]$,

$$p^{(j)}(\alpha_i) = Y_{ji}.$$

Denote by $\mathcal{L}$ the set of polynomials p such that the above is true. We want t to be as small as possible.
Sticking with the Welch-Berlekamp idea, the proof/algorithm go as follows.

1. Find a nonzero $(m+2)$-variate polynomial

   $$Q(x, z_0, z_1, \ldots, z_m) = z_0 A_0(x) + z_1 A_1(x) + \cdots + z_m A_m(x)$$

   such that

   - $\deg(A_i) < D$ for some D we shall fix later,
   - certain multiplicity constraints are satisfied, which we shall come up with later, and
   - Q "explains" the given data: for every $j \in [n]$, $Q(\alpha_i, Y_{0,i}, Y_{0,i}, \ldots, Y_{m,i}) = 0$; we want it to explain the top m rows of the matrix.

2. Show that for all $p \in \mathcal{L}$,

   $$Q(x, p(x), p^{(1)}(x), \ldots, p^{(m)}(x)) \equiv 0. \tag{1}$$

3. Find all low degree solutions to Q satisfying Equation (1). Note that we cannot rely on factoring for this, and it is more complicated.

Set $R(x)$ equal to the LHS of Equation (1) for some polynomial p, so it is

$$R(x) = A_0 p + A_1 p^{(1)} + \cdots + A_m p^{(m)}.$$

If Y and the encoding of p agree at α_i, then $R(\alpha_i) = 0$.[1] The multiplicity constraint means that we also want the derivative of R to be zero at α_i. We have

$$\frac{\mathrm{d}R}{\mathrm{d}x} = A_0^{(1)} p + A_0 p^{(1)} + A_1^{(1)} p^{(1)} + A_1 p^{(2)} + \cdots + A_m^{(1)} p^{(m)} + A_m p^{(m+1)},$$

so if $m < s$,

$$0 = \left.\frac{\mathrm{d}R}{\mathrm{d}x}\right|_{\alpha_i} = A_0^{(1)}(\alpha_i) Y_{0,i} + A_0(\alpha_i) Y_{1,i} + A_1^{(1)}(\alpha_i) Y_{1,i} + A_1(\alpha_i) Y_{2,i} + \cdots + A_m^{(1)}(\alpha_i) Y_{m,i} + A_m(\alpha_i) Y_{(m+1),i}.$$

So, at each i, the aforementioned multiplicity constraints correspond to about $s-m-1$ additional constraints of the above form.

Now, we would like to set D in the first step such that it has a solution. There are Dm variables and $n(s-m-1)$ constraints. So, we require $Dm \geq n(s-m-1)$. Set

$$D = \frac{n}{m}(s-m).$$

Let us now look at step 2. For a given polynomial in $\mathcal{L}$, the degree of R is at most $D+k-1$. To ensure that R is identically zero, we need that $t(s-m-1) \geq D+k$, since each point of agreement gives $(s-m-1)$ equations. That is, we need

$$\begin{aligned} t &> \frac{1}{s-m}(D+k) \\ &= \frac{n}{m} + \frac{k}{s-m} \\ \frac{t}{n} &> \frac{k}{n(s-m)} + \frac{1}{m}. \end{aligned}$$

Setting m as around $1/\epsilon$ and $s > 1/\epsilon^2$ does the job!

Finally, it remains to see if it is possible to find all low degree solutions p to $Q(x, p, p^{(1)}, \ldots, p^{(m)}(x)) \equiv 0$. Let us look at just the trivariate case, with $Q(x, p, p') \equiv 0$. That is, we wish to solve

$$A_0(x)p(x) + A_1(x)p^{(1)}(x) + A_2(x)p^{(2)}(x) \equiv 0.$$

Note that the space of all p satisfying this is a subspace of the space of all polynomials of degree $< k$. We may assume wlog that two of the A_i are nonzero, as the problem is not very interesting otherwise. Suppose that $A_2 \not\equiv 0$. This means that there exists some $\beta \in \mathbb{F}$ such that $A_2(\beta) \neq 0$. We can assume wlog that $\beta = 0$ by "shifting" the axis by β otherwise. Dividing by a constant, we can also assume that the constant term in A_2 is 1, so

$$A_0 p + A_1 p^{(1)} + (1 + \tilde{A}_2) p^{(2)} \equiv 0,$$

where $\tilde{A}_2$ has no constant term.
The p we wish to find is of the form

$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots p_{k-1} x^{k-1}.$$

[1] Stopping here would lead to unique decoding, by setting m as s or $s-1$ or so.

Plugging this into the previous equation, we have

$$A_0(p_0 + p_1 + \cdots) + A_1(p_1 + 2p_2x + \cdots) + (1 + \tilde{A}_2)(2p_2 + 3 \cdot 2p_3 + \cdots) \equiv 0.$$

This means that all the coefficients of the resulting polynomial is zero. This is just a linear system of equations, so we can solve it. It remains to argue that the number of solutions (the list size) is not too large. Note that the equation for the coefficient of degree k being 0 involves only the first $k + 2$ coefficients of p! Consequently, the solution space lives in a 3-dimensional subspace, so it is small. In general, it lives in an $(m+1)$-dimensional subspace. Because m depends on ϵ, we only need to check the elements of the subspace, which numbers about $|\mathbb{F}|^{1/\epsilon}$.