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 $\mathbb{F}$, where

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

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 $\mathbb{R}$. One has to assume that the field characteristic is large enough, so that derivatives do not become zero. 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 $n - k - 1$.

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 (Nielsen ’01, Kopparty ’13, Guruswami-Wang ’14). For every $\epsilon > 0$, for sufficiently large $s$, univariate multiplicity codes are efficiently list decodable from fractional agreement $k ns + \epsilon$.

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 $\epsilon$. This was shown by Kopparty, Saraf, Ron-Zewi, and Wootters in 2018.

The fraction of agreement here is $k/s + \epsilon = \text{Rate} + \epsilon$. Compare this to what we had studied about Reed-Solomon codes, where we only had $\sqrt{\text{Rate}} (>> \text{Rate})$.

The remainder of this section is dedicated to the proof of this theorem; we shall look at the version due to Guruswami-Wang which gives a polynomial size list (instead of constant size).

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 $i \in [n]$, $Q(\alpha_i, Y_{0,i}, Y_{1,i}, \ldots, Y_{m,i}) = 0$; we want it to explain the top $m$ rows of the matrix.

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

$$Q(x, p(x), p^{(1)}(x), \ldots, p^{(m)}(x)) \equiv 0. \quad (1)$$
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 $\alpha_i$, then $R(\alpha_i) = 0$ \([\text{1}]\). The multiplicity constraint means that we also want the derivative of $R$ to be zero at $\alpha_i$. We have

$$\frac{dR}{dx} = A_0^{(1)} p + A_0 p^{(1)} + A_1^{(1)} p^{(1)} + A_1 p^{(2)} + \cdots + A_m^{(1)} p^{(m)} + A_m p^{(m+1)},$$

so if $m < s$,

$$0 = \frac{dR}{dx} \bigg|_{\alpha_i} = A_0^{(1)} (\alpha_i) Y_{0,i} + A_0 (\alpha_i) Y_{1,i} + A_1^{(1)} (\alpha_i) Y_{1,i} + A_1 (\alpha_i) Y_{2,i} + \cdots + A_m^{(1)} (\alpha_i) Y_{m,i} + A_m (\alpha_i) Y_{(m+1),i}.$$  

So, at each $i$, the aforementioned multiplicity constraints correspond to about $s - m - 1$ additional constraints of the above form. That is, for each $0 \leq \ell \leq s - m - 1$, we put the constraint

$$0 = \frac{d^\ell R}{dx^\ell} \bigg|_{\alpha_i} = \sum_{h=0}^{\ell} \left( A_0^{(\ell-h)} (\alpha_i) Y_{h,i} \right) + \sum_{h=0}^{\ell} \left( A_1^{(\ell-h)} (\alpha_i) Y_{h+1,i} \right) + \cdots + \sum_{h=0}^{\ell} \left( A_m^{(\ell-h)} (\alpha_i) Y_{h+m,i} \right).$$

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 $p(x)$ in $L$, the degree of $R(x)$ is at most $D + k - 1$. To ensure that $R$ is identically zero, we need that $t(s - m - 1) \geq D + k$. This is sufficient because our constraints imply that $\alpha_i$ is a root of $R(x)$ with multiplicity $s - m - 1$, for any $i \in T$. That means total $t(s - m - 1)$ roots for $R(x)$, which is more than the degree $D + k - 1$. So, we need

$$t > \frac{1}{s - m} (D + k) = \frac{n}{m} + \frac{k}{s - m} \Rightarrow \frac{t}{n} > \frac{k}{n(s - m)} + \frac{1}{m}.$$  

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

Finally, it remains to see if it is possible to find all low degree solutions $p$ to $Q(x, p, p^{(1)}, \ldots, p^{(m)}(x)) \equiv 0$. That is, given polynomials $A_0(x), A_1(x), \ldots, A_m(x)$, we wish to find $p(x)$ satisfying

$$A_0(x) p(x) + A_1(x) p^{(1)}(x) + \cdots + A_m(x) p^{(m)}(x) \equiv 0.$$  

Note that this condition gives us a set of linear equations in the coefficients of $p(x)$. One can show that the solution space is at most $m + 1$ dimensional.

For simplicity, let us look at just the trivariate case, with $Q(x, p, p') \equiv 0$. That is,

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

We may assume wlog that two of the $A_i$s 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 $A_2(\beta) \not\equiv 0$. We can assume wlog

\[1\] Stopping here would lead to unique decoding, by setting $m$ as $s$ or $s - 1$ or so.
that \( \beta = 0 \) by “shifting” the axis by \( \beta \) otherwise. Dividing by a constant, we can also assume that the constant term in \( A_2 \) is 1, so
\[
A_0(x)p(x) + A_1(x)p^{(1)}(x) + (1 + x\tilde{A}_2(x))p^{(2)}(x) \equiv 0.
\]
Let \( p \) we wish to find be of the form
\[
p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_{k-1} x^{k-1}.
\]
Plugging this into the previous equation, we have
\[
A_0(x)(p_0 + p_1 x + \cdots) + A_1(x)(p_1 + 2p_2 x + \cdots) + (1 + x\tilde{A}_2(x))(2p_2 + 3 \cdot 2p_3 x + \cdots) \equiv 0.
\]
Now, we argue that the solution space is only of 2-dimension. To see this, consider the degree-0 terms in the above expression.
\[
A_0,0 p_0 + A_{1,0} p_1 + 2p_2 = 0.
\]
This means that once we fix \( p_0 \) and \( p_1 \), the value of \( p_2 \) is uniquely determined. Now, let us consider the degree-1 terms.
\[
A_{0,1} p_0 + (A_{0,0} + A_{1,1}) p_1 + (A_{1,0} + A_{2,1}) 2p_2 + 6p_3 = 0.
\]
Once we have \( p_0, p_1, p_2 \) fixed, \( p_3 \) is also uniquely determined from the above equation. Hence, after fixing \( p_0, p_1, p_2 \), every other coefficient in \( p(x) \) is uniquely determined. This proves that the solution space is 2-dimensional.

In general, the solution space lives in an \((m + 1)\)-dimensional subspace. Because \( m \) depends on \( \epsilon \), we only need to check the elements of the subspace, which numbers about \(|F|^{1/\epsilon} \).