Information and Coding Theory **Autumn 2014**

Lecture 14: November 13, 2014

Lecturer: Madhur Tulsiani Scribe: Behnam Neyshabur

1 A different definition of Reed-Solomon codes

Let $C : \mathbb{F}_q^k \to \mathbb{F}_q^n$ be a coding where $q \geq n$. Fix a subset $S \subseteq \mathbb{F}_q$ such that $|S| = n$, i.e. $S = \{a_1, \ldots, a_n\}$. For any $m_0, \ldots, m_{k-1}$, consider the following polynomial:

$$P(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-1} x^{k-1}$$

We define the coding C as

$$C(m_0, \ldots, m_{k-1}) = (P(a_1), P(a_2), \ldots, P(a_n))$$

Fix a subset $H \subseteq \mathbb{F}_q$ such that $|H| = k$. We treat the values of a polynomial P on H as the function $f : H \to \mathbb{F}_q$. Let P be the unique degree $k-1$ polynomial such that for all $\ell \in H$, $P(\ell) = f(\ell)$. We want to output $\{P(a_1), P(a_2), \ldots, P(a_n)\}$. This can be done by solving a set of k linear equation of the form $AX = b$.

The problem with Reed-Solomon codes is that q should be large ($q \geq n$). However, in practice we can only transmit only bits or symbols over a small alphabet. Reed-Muller introduced below help reduce the alphabet size to some extent. Moreover, they allow for a very interesting notion of decoding which we call "local decoding".

2 Reed-Muller codes

Fix $H \subseteq \mathbb{F}_q$ such that $|H| = h$. Let $C : \mathbb{F}_q^{h^m} \to \mathbb{F}_q^{q^m}$ be a coding where parameters q, h and m can be defined to get a reasonable performance. Given a list of h^m values in $\mathbb{F}_q$ as the input, we treat them as a function $f : H^m \to \mathbb{F}_q$. We want to find the unique polynomial $P \in \mathbb{F}_q[x_1, \ldots, x_m]$ such that for all i, $\deg_{x_i}(P) \leq h-1$ and for all $\ell_1, \ldots, \ell_m \in H$, we have that

$$P(\ell_1, \ldots, \ell_m) = f(\ell_1, \ldots, \ell_m)$$

and then output $\{P(z_1, \ldots, z_m)\}_{z_1, \ldots, z_m \in \mathbb{F}_q}$.

We need to prove two statements:

Exercise 2.1 *There exists a polynomial P such that:*

1. $\forall \ell_1, \ldots, \ell_m \in H, P(\ell_1, \ldots, \ell_m) = f(\ell_1, \ldots, \ell_m)$.
2. $\forall i, deg_{x_i}(P) \leq h-1$.

Exercise 2.2 *Such a polynomial P with properties defined in exercise 1 is unique.*

Proof: (of exercise 1)
Define the function δ as:

$$\delta(\ell_1, \ldots, \ell_m) = \prod_{i=1}^{m} \prod_{\ell'_i \in H \setminus \ell_i} \left(\frac{x_i - \ell'_i}{\ell_i - \ell'_i} \right)$$

As we indicated in previous lectures, it can be shown that the polynomial P is then nothing but:

$$P(x_1, \ldots, x_m) = \sum_{\ell_1, \ldots, \ell_m \in H} f(\ell_1, \ldots, \ell_m) \delta(\ell_1, \ldots, \ell_m)$$

■

We now prove the uniqueness of the polynomial P:

Proof: (of exercise 2)
Assume for contradiction that P_1 and P_2 are polynomials such that $\deg_{x_i}(P_1) \leq h-1$, $\deg_{x_i}(P_2) \leq h-1$ and

$$\forall \ell_1, \ldots, \ell_m, \quad P_1(\ell_1, \ldots, \ell_m) = P_2(\ell_1, \ldots, \ell_m) = f(\ell_1, \ldots, \ell_m)$$

Let $P' = P1 - P2$. It is clear that

- For any i, $\deg_{x_i}(P') \leq h - 1$.
- For all $\ell_1, \ldots, \ell_m \in H$, $P'(\ell_1, \ldots, \ell_m) = 0$.

P' can be written as:

$$\begin{aligned} P' &= \sum_{i_1, \ldots, i_m \leq h-1} c_{i_1, \ldots, i_m} x_1^{i_1} \ldots x_m^{i_m} \\ &= \sum_{i \leq h-1} x_1^i Q_i(x_2, \ldots, x_m) \end{aligned}$$

This is a univariate polynomial in x_1 that is zero for $\ell_2, \ldots, \ell_m$, i.e.

$$\forall \ell_2, \ldots, \ell_m, \forall i \in \{0, \ldots, h-1\}, \quad Q_i(\ell_2, \ldots, \ell_m) = 0$$

The proof is completed by induction on the polynomials Q_i and so on. ■

Exercise 2.3 *Show that Reed-Muller codes are linear.*

2.1 Distance of Reed-Muller Codes

A codeword of the Reed-Muller code $C : \mathbb{F}_q^{h^m} \to \mathbb{F}_q^{q^m}$ is a polynomial P in variables $z_1, \ldots, z_m$ evaluated on all points in $\mathbb{F}_q^m$. Thus, to compute the distance of the code, we are interested in lower bounding the number of points on which two polynomials must differ. Thus, given two polynomials P_1 and P_2, we are interested in a lower bound on the following probability:

$$\mathbb{P}_{x_1,\dots,x_m}[(P_1 - P_2)(x_1, \dots, x_m) \neq 0]$$

The following result, known as the Schwartz-Zippel gives a lower bound on this probability. Note that the result is stated in terms of the *total* degree of the polynomial. For the polynomial, we will have that the total degree is at most $m \cdot (h-1)$, since the degree in each variable is at most $h-1$.

Lemma 2.4 (Schwartz-Zippel Lemma [1, 2]) *Let $P \in \mathbb{F}_q[x_1, \dots, x_m]$ be a polynomial with total degree r, then*

$$\mathbb{P}_{z_1,\dots,z_m}[P(z_1, \dots, z_m) \neq 0] \;\geq\; \frac{1}{q^{\lfloor \frac{r}{q-1} \rfloor}} \left(1 - \frac{r \bmod (q-1)}{q}\right)$$

Thus, we can say that the distance is at least q^m times the lower bound given by the above lemma. An interesting special case is when $q - 1 > r$ and we get that

$$\mathbb{P}_{z_1,\dots,z_m}[P(z_1, \dots, z_m) \neq 0] \;\geq\; 1 - \frac{r}{q}\,.$$

Thus, when $q - 1 > r$, we get that $\Delta(C) \geq q^m \cdot \left(1 - \frac{r}{q}\right)$.

Exercise 2.5 *For the special case, when $q - 1 > r$, prove the Schwartz-Zippel lemma by induction on the number of variables in P.*

2.2 Local Correction of Reed-Muller codes

Let $\{P(z_1, \dots, z_m)\}_{z_1,\dots,z_m \in \mathbb{F}_q}$ be Reed-Muller codeword and assume that α fraction of the codeword is corrupted and instead we observe $\{g(z_1, \dots, z_m)\}_{z_1,\dots,z_m \in \mathbb{F}_q}$. Therefore, we have:

$$\mathbb{P}_{z_1,\dots,z_m \in \mathbb{F}_q}[P(z_1, \dots, z_m) = g(z_1, \dots, z_m)] \geq 1 - \alpha$$

Decoding the codeword would correspond to recovering the values $P(x_1, \dots, x_m)$ for all $x_1, \dots, x_m \in H$. However, suppose we are only interested in the value at *one* point $(x_1, \dots, x_m)$. Of course, decoding the full message would also give the value at the point of interest. However, the running time may be polynomial in q^m which is the length of the codeword.

Reed-Muller codes have the interesting property that for any point $(x_1, \dots, x_m)$, we can recover the value $P(x_1, \dots, x_m)$ (with high probability) in time $\mathrm{poly}(q, m)$. Note in particular that the dependence on m is polynomial instead of the exponential dependence we would get if we tried to recover the entire message. Also, we need to only to read the value of g at $O(q)$ randomly chosen points. Thus, we don't even read the entrire received word.

For simplicity, we illustrate this by an example.

Error Correction example:

Let $q \geq 5hm$. Therefore, we know that the distance is at least $\frac{4}{5}q^m$. Assume that $\alpha = \frac{1}{10}$ fraction of the code is corrupted. Given $z = (z_1, \dots, z_m)$ we want to find the value $P(z_1, \dots, z_m)$. Pick

$y \in \mathbb{F}_q^m$ at random where $y = (y_1, \dots, y_m)$ and define $\ell(t) = (1-t)z + ty$ where $t \in \mathbb{F}_q$. Note that $\ell(0) = z$.

Consider $P(\ell(t)) = Q(t)$. $Q(t)$ is a univariate polynomial with degree at most $(h-1)m$. We want to find $Q(0) = P(z)$ by looking at $\{g(\ell(0)), g(\ell(1)), \dots, g(\ell(q-1))\}$. If enough values are correct, this is Reed-Solomon code. Since at most $\frac{1}{10}$ of code words are corrupted, we have:

$$\forall t \neq 0, \quad \mathbb{P}_y [g(\ell(t)) \neq P(\ell(t))] \;\leq\; \frac{1}{10}$$

Therefore,

$$\mathbb{E}_y [|\{t \in \mathbb{F}_q \;\mid\; g(\ell(t)) \neq P(\ell(t))\}|] \;\leq\; \frac{q}{10}$$

By Markov's inequality, we can now bound the probability of having certain number of errors:

$$\mathbb{P}_y \left[|\{t \;\mid\; g(\ell(t)) \neq P(\ell(t))\}| \geq \frac{2q}{5} \right] \;\leq\; \frac{1}{4}$$

Thus, with probability at least $3/4$, the univariate polynomial Q is uncorrupted in at least $3q/5$ values. We can find Q using Reed-Solomon (unique) decoding and output $Q(0)$.

References

[1] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, October 1980.

[2] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, EUROSAM '79, pages 216–226, London, UK, UK, 1979. Springer-Verlag.