Linearized polynomials and limits to Reed-Solomon decoding - sketch of lecture by Ariel Gabizon

December 9, 2013

notation: These notes are based on the Paper of Ben-Sasson, Kopparty and Radhakrishnan [1] Define $RS_{N,K}$ to be the set of degree K - Reed-Solomon words on $\mathbb{F}_N$ of degree K. (i.e., vectors of length N that are evaluations of a univariate polynomial of degree at most K on the points of $\mathbb{F}_N$).

Theorem 0.1. *Fix integers $u \leq v \leq m$, and a prime power q. Let $N = q^m$ and $K = q^u$. There is a set of $q^{(u+1)\cdot m - v^2}$ elements of $RS_{N,K}$ that all agree with some word $w \in \mathbb{F}_N$ on q^v points.*

Taking $u = \delta \cdot m$ and $v = \rho \cdot m$, we get a super-polynomial number of codewords whenever $\rho < \sqrt{\delta}$. This implies we need agreement $N^{\sqrt{\delta}}$ for efficient decoding. On the other direction, the Johnson bound implies agreement $N^{(1+\delta)/2}$ suffices.

Definition 1 (Subspace Polynomials)**.** *V is linear subspace of dimension v in $\mathbb{F}_{q^m}$. The* subspace polynomial *P_V is defined as follows.*

$$P_V(X) \triangleq \prod_{a \in V} (X - a)$$

Claim 0.2. *P_V is of the form*

$$X^{q^v} + \sum_{i=0}^{v-1} \alpha_i \cdot X^{q^i}$$

for $\alpha_i \in \mathbb{F}_{q^m}$.

Proof. (sketch) Look at functions $X, X^q, \ldots, X^{q^v}$ as $\mathbb{F}_q$-linear functions from V to $\mathbb{F}_{q^m}$. Show there is dependence over $\mathbb{F}_{q^m}$. □

Claim 0.3. *There is a set $\mathcal{U}$ of at least $q^{(u+1)\cdot m - v^2}$ subspace polynomials (of dimension v) that agree on the top coefficients $\alpha_{u+1}, \ldots, \alpha_{v-1}$.*

Proof. Number of subspaces of dimension v is at least $q^{(m-v)\cdot v}$. There are $q^{m\cdot(v-u-1)}$ choices for these top coefficients. An averaging argument concludes. □

Now, for this choice of $\alpha_{u+1}, \ldots, \alpha_{v-1}$ define

$$P^*(X) \triangleq X^{q^v} + \sum_{i=u+1}^{v-1} \alpha_i \cdot X^{q^i}$$

Define $\mathcal{L} \triangleq \{P^* - P_V | P_V \in \mathcal{U}\}$.
Note, for any $P \in \mathcal{L}$.

- P has degree at most q^u
- P and $P*$ agree on at least q^v points: Let $P = P^* - P_V$ Then

$$P^* - P = P^* - (P^* - P_V) = P_V$$

1 Observations on coefficients of subspace polynomials

Suppose n is prime.

Claim 1.1. *When choosing a random d-dimensional subspace V. All non-zero values of a given coefficient are obtained with same probability.*

Proof. For $a \in \mathbb{F}_{q^n}^*$ $a \in V \triangleq \{a{\cdot}v | v \in V\}$. $a{\cdot}V$ is a subspace of dim d different from V (when n is prime and $a \neq 1$). We can partition the subspaces of dimension d into orbits of the form $\{a \cdot V\}_{a \in \mathbb{F}_{2^n}}$. Call $c_0(V)$ the coefficient of X in P_V. Note $c_0(V) = \prod_{v \in V \setminus \{0\}} v$ So $c_0(a{\cdot}V) = \prod_{v \in V \setminus \{0\}} a{\cdot}v = a^{2^d-1}{\cdot}c_0(V)$. Note that raising to power $2^d - 1$ is a permutation of $\mathbb{F}_{2^n}^*$. The argument for the other coefficients c_i is similar, by noticing that they are always equal to a symmetric polynomial in the non-zero elements of the subspace. □

Claim 1.2. *Let $f(X) = X^{2^d} + \sum_{i=0}^{d-1} c_i \cdot X^{2^i}$ be a linearized polynomial with coefficients in F_{2^n}. Define an $n \times n$ matrix $A(f)$ where the first row are the coefficients of P. The i'th row is a circular shift of the $i-1$'th row, where all elements are also squared. Then f is a subspace polynomial if and only if the rank of the matrix $A(f)$ is exactly $n-d$ (it is always at least $n-d$).*

Corollary 1.3. *The subspace polynomials with $\{0,1\}$ coefficients are the linearized associates of the factors of $X^n - 1$.*

References

[1] Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace polynomials and limits to list decoding of reed-solomon codes. *IEEE Transactions on Information Theory*, 56(1):113–120, 2010.