Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 20: Application: Secret Sharing

October 12,2007

Lecturer: Atri Rudra *Scribe: Kanke Gao*

In the last lecture, we introduced the concept of secret sharing. Here we restate the formal definition of an (ℓ, m)-secret sharing scheme, where $m > \ell$.
Inputs are secret $s \in \mathbb{D}$, for some domain $\mathbb{D}$ and players $P_1, P_2, \ldots, P_n$ and outputs are shares s_i for each player $P_i (1 \le i \le n)$, such that

- (A) For every $S \subseteq [n]$, such that $|S| \ge m$, s can be computed from $\{s_i\}_{i \in S}$.
- (B) For every $S \subseteq [n]$, such that $|S| \le \ell$, s can not be computed from $\{s_i\}_{i \in S}$.

1 Shamir's secret sharing scheme

In the previous lecture, we saw a fairly simple secret sharing scheme with $\ell = n - 1$. In today's lecture we will consider some effective schemes. First, we will study Shamir's $(\ell, \ell + 1)$-secret sharing scheme [1].

Shamir's $(\ell, \ell + 1)$-secret sharing scheme

Consider $\mathbb{D} = \mathbb{F}_q$, where $q \ge n$

Step 1) Pick a random polynomial $P(x) \in \mathbb{F}_q(x)$ of degree $\le \ell$,$1 \le \ell \le n - 1$, such that $P(0) = s$.

Step 2) Choose distinct $x_1, x_2, \ldots, x_n \in \mathbb{F}_q$ and set $s_i = (P(x_i), x_i)$.

We now verify that Shamir's $(\ell, \ell + 1)$-secret sharing scheme satisfies two required conditions of secret sharing schemes.

- Property (A): Let $S \subseteq [n]$, such that $|S| \ge \ell+1$. At the output, we have shares $\{(P(x_i), x_i)\}_{i \in S}$, then we can recover $P(x)$ by polynomial interpolation as degree of P is at most of ℓ. Given $P(x)$, computing $s = P(0)$ is easy.
- Property (B): Let $S \subseteq [n]$, such that $|S| \le l$. At the output, we have shares $\{(P(x_i), x_i)\}_{i \in S}$. Consider coefficients of $P(x)$ as variables. Totally, we have $l + 1$ coefficients and $\le l$ values of $P(x)$. For every fixed value of $P(0)$, by polynomial interpolation one can obtain a different polynomial $P(x)$. So every value of s is equally likely, as desired.

Shamir's scheme seems to crucially use properties of Reed-Solomon codes. Next, we will see a generalization of Shamir's scheme to linear codes that satisfy certain properties.

2 A generic secret sharing scheme

(ℓ, m)-secret sharing scheme

Consider $\mathbb{D} = \mathbb{F}_q$, where $q \geq n$, and the parameters satisfy $l \leq d^{\perp}$, $m \geq n - d + 2$ for some d, $d^{\perp} \geq 1$. Let C be an $[n+1, k, d]_q$ code and $C^{\perp}$ be $[n+1, n+1-k, d^{\perp}]_q$ code.

Step 1) Pick a random codeword $(c_0, c_1, \ldots, c_n) \in C$ such that $c_0 = s$.

Step 2) Set $s_i = c_i$ for $1 \leq i \leq n$.

For step 1 to be valid, for starters for every $\alpha \in \mathbb{F}_q$, there needs to exist a codeword $(\alpha, c_2, \ldots, c_n) \in C$. For any linear code C, there exists a codeword $\mathbf{c}$ with $c_0 \neq 0$, which is equivalent to the condition that first column of generator matrix for C is not the all 0's vector[1]. By linearity, for all $\alpha \in \mathbb{F}_q$, $\alpha\mathbf{c} \in C$. So the first symbols in the vectors in $\{\alpha\mathbf{c}\}_{\alpha \in \mathbb{F}_q}$ is $\mathbb{F}_q$.
In Shamir's scheme, the code C, which is $RS[n+1, \ell+1]_q$, has distance $d = n - \ell + 1$. So we have $m \geq n - (n - \ell + 1) + 2 = \ell + 1$. Further, it is known that

Proposition 2.1. $RS[n,k]^{\perp} = RS[n, n-k]$

The proof is left as an exercise. One way to prove this result is by using hint in question $6(a)$ of homework.

By Proposition 2.1, $RS[n+1, \ell+1]_q^{\perp} = RS[n+1, n-\ell]_q$ and has distance $d^{\perp} = \ell$, as desired. We now check whether (ℓ, m)-secret sharing scheme above satisfies two conditions of secret sharing schemes.

- Property (A): Given $m \geq n - d + 2$ symbols of a codeword are known, then $n + 1 - (n - d + 2) = d - 1$ symbols of the codeword are unknown. Declare these symbols as erasures, then there are $\leq d - 1$ erasures. As C has distance d, we can uniquely recover the corresponding codeword $(c_0, c_1, \ldots, c_n)$ and in particular the secret c_0.

- Property (B): Follows from the claim below.

Claim 2.2. *Given $\leq d^{\perp} - 2$ symbols of a codeword $(c_0, c_1, \ldots, c_n) \in C$ (other than c_0), all values of c_0 are possible.*

Proof. (Sketch) Consider the known linear constraints on the c_i's. The only known constraints are of the form $\sum_{i=0}^{n} x_i c_i = 0$ for every $(x_0, x_1, \ldots, x_n) \in C^{\perp}$. In order to recover c_0, we need a constraint such that $x_0 \neq 0$ and $x_i = 0$, for every $i \notin S$. For sake of contradiction, there exists a dual codeword such that $x_0 \neq 0$ and $x_i = 0$, for every $i \notin S$. The weight of the dual codeword is $\leq d^{\perp} - 2 + 1 = d^{\perp} - 1$, which is a contradiction as $C^{\perp}$ has distance $d^{\perp}$. Finally all values of c_0 are

[1] We will assume this to be the case. Otherwise, we can drop the first symbol and not change any parameter of the code C other than decreasing the block length by one

possible as in the generator matrix of C, any $\leq d^{\perp} - 1$ columns are independent. This is because for any $C' = [n', k', d']_q$ code , d' is the smallest number of independent columns in parity check matrix of C'. $\square$

References

[1] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.