1 Encoding

- Represent the input m as a vector with $(k-1)$ components over $\mathbf{Z}_p$, where p is prime:

$$m = (a_{k-1}, \ldots, a_1);$$

- Choose the polynomial $P(x) = a_{k-1}x^{k-1} + \cdots + a_1 x$ (remark that $P(0) = 0$ - this property will be used for decoding);

- Encode m as the vector $y = (P(1), P(2), \ldots, P(n))$, where $n = k + 2s$,

$$y = (y_1, \ldots, y_n).$$

2 Decoding

- Suppose that the input z has at most s errors (i.e., $|\{i \in \{1, \ldots, n\} | z_i \neq y_i\}| \leq s$ -thus, $|\{i \in \{1, \ldots, n\} | z_i = y_i\}| \geq k + s$);

- Generate $A \subset \{1, \ldots, n\}$, with $|A| = k$, and compute the free coefficient as

$$fc = \sum_{i \in A} (z_i \cdot \prod_{j \in A \setminus \{i\}} \frac{j}{j-i});$$

- If $fc = 0$, determine the polynomial $P(x)$ as

$$\sum_{i \in A} (z_i \cdot \prod_{j \in A \setminus \{i\}} \frac{x-j}{i-j});$$

  We will have $P(x) = a_{k-1}x^{k-1} + \cdots + a_1 x$ and $m = (a_{k-1}, \ldots, a_1)$.

Example 1 Let $k = 3$, $s = 1$ ($n = 5$) and $p = 11$. The message $m = 29$ will be represented in base $p = 11$ as $m = (2, 7)_{11}$ ($a_2 = 2$, $a_1 = 7$). We will consider the polynomial $P(x) = 2x^2 + 7x$ over $\mathbf{Z}_{11}$ and we will obtain $y_1 = P(1) = 9$, $y_2 = P(2) = 0$, $y_3 = P(3) = 6$, $y_4 = P(4) = 5$, and $y_5 = P(5) = 8$. Thus, m will be encoded as $y = (9, 0, 6, 5, 8)$.

Suppose that $z = (9, 2, 6, 5, 8)$ (thus, $z_2 \neq y_2$ and $z_i = y_i$, for all $i \neq 2$). Then, for any subset A of $\{1, 3, 4, 5\}$ with 3 elements, we wil obtain $fc = \sum_{i \in A}(z_i \cdot \prod_{j \in A \setminus \{i\}} \frac{j}{j-i}) = 0$ and $P(x) = \sum_{i \in A}(z_i \cdot \prod_{j \in A \setminus \{i\}} \frac{x-j}{i-j}) = 2x^2 + 7x$. Thus, z will be decoded as $m = (2, 7)$.