Polynomials in Algorithms: k-wise Independence, Reed-Solomon Codes

Tuesday, December 2, 2025 1:52 AM

k-wise independent hash functions from polynomials

Case $U = R = \mathbb{F}$, finite field $\mathbb{F}$

Sampling h:

① Sample random coefficients $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$

② Hash function is $h(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{k-1} x^{k-1}$.

To show: $\Pr[h(i_1) = a_1, h(i_2) = a_2, \dots, h(i_k) = a_k] = \frac{1}{|\mathbb{F}|^k}$.

$\iff$ there is a unique solution $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ s.t.

$$c_0 + i_1 c_1 + i_1^2 c_2 + \cdots + i_1^{k-1} c_{k-1} = a_1$$
$$c_0 + i_2 c_1 + i_2^2 c_2 + \cdots + i_2^{k-1} c_{k-1} = a_2$$
$$\vdots$$
$$c_0 + i_k c_1 + i_k^2 c_2 + \cdots + i_k^{k-1} c_{k-1} = a_k$$

k equations, k unknown variables.

If system is independent, then unique solution.

Matrix form:

$$\begin{bmatrix} 1 & i_1 & i_1^2 & i_1^3 & \cdots & i_1^{k-1} \\ 1 & i_2 & i_2^2 & i_2^3 & \cdots & i_2^{k-1} \\ & & \vdots & & & \\ 1 & i_k & i_k^2 & i_k^3 & \cdots & i_k^{k-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{k-1} \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix}$$

↑ Claim: the Vandermonde matrix is independent.

Proof: suffices to show columns are indep.

Suppose $b_0 \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} + b_1 \begin{bmatrix} i_1 \\ i_2 \\ \vdots \\ i_k \end{bmatrix} + \cdots + b_{k-1} \begin{bmatrix} i_1^{k-1} \\ i_2^{k-1} \\ \vdots \\ i_k^{k-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

Then $i_1, i_2, \dots, i_k$ are roots of the polynomial

$$b_0 + b_1 x + \cdots + b_{k-1} x^{k-1}$$

But a nonzero poly of degree $\le k-1$ has $\le k-1$ roots.

So zero polynomial $\Rightarrow b_0 = b_1 = \cdots = b_{k-1} = 0$.

Reed-Solomon Codes

Given integer k and finite field $\mathbb{F}_q$ where $q > k$

the Reed-Solomon Code is the mapping $\mathbb{F}_q^k \to \mathbb{F}_q^q$

defined by

$$(c_0, c_1, \dots, c_{k-1}) \in \mathbb{F}_q^k \longmapsto \big(p(0), p(1), \dots, p(q-1)\big) \in \mathbb{F}_q^q$$

where $p(x) = c_0 + c_1 x + \cdots + c_{k-1} x^{k-1}$

It is an error-correcting code in the following sense: given any $q-k$ erasures of a codeword, can uniquely recover the codeword.

To prove this, suppose for contradiction that two codewords $(p_1(0), \dots, p_1(q-1))$ and $(p_2(0), \dots, p_2(q-1))$ can both fill in $q-k$ erasures, i.e. they agree on the other k coordinates.

Then the difference of polynomials $p_1 - p_2$ has value 0 on k coordinates, and has degree $\le k-1$.

So $p_1 - p_2$ must be the zero polynomial, and $p_1 = p_2$.

The Reed-Solomon Code is also a linear operator: multiply the Vandermonde matrix with the coefficient vector.