Shamir's Secret Sharing - Lagrange Interpolation

Anna Mouland

July 1, 2022

1 Degree-3 polynomial using normal numbers instead of a finite field

Given: $f(5) = 3$; $f(7) = 12$; $f(12) = 6$; $f(30) = 15$

Deltas:
$\delta_5(x)$ if $x == 5$ then 3, else 0
$\delta_7(x)$ if $x == 7$ then 2, else 0
$\delta_{12}(x)$ if $x == 12$ then 6, else 0
$\delta_{30}(x)$ if $x == 30$ then 15, else 0

$f(x) = \delta_5(x) + \delta_7(x) + \delta_{12}(x) + \delta_{30}(x)$

Abstraction 1: Multiply deltas by their desired value such that they return 1 or 0
$\delta_5(x)$ if $x == 5$ then 1, else 0
...
$f(x) = 5 \cdot \delta_5(x) + 2 \cdot \delta_7(x) + 6 \cdot \delta_{12}(x) + 15 \cdot \delta_{30}(x)$

Abstraction 2: let C be the set of all y points such that f(x) becomes a polynomial

$C = \{5, 7, 12, 30\}$
$\delta_i(x) =$ if $x \in Cx == i$ then 1, if $x \in Cx! = i$ then 0

then:
$\delta_5(x) = \frac{x-7}{5-7} \cdot \frac{x-12}{5-12} \cdot \frac{x-30}{5-30}$
...
so
$\delta_i(x) = \prod_(\frac{x-j}{i-j})$ for $j \in C$, $j! = i$

such that
$f(x) = \sum(f(i)\delta_i(x)$ for $i \in C$