We interpolate the maximum possible terms of $f$ and use Chinese remaindering to recover the integer coefficients. We use a Kronecker substitution to reduce multivariate interpolation to a univariate interpolation.

Definition Let $f \in \mathbb{R}[x_1, x_2, \ldots, x_n]$, where $R$ is a ring and $d = \deg f$. Let $\ell$ denote the number of non-zero terms of $f$ and $\mathcal{T}(\ell)$ denote the maximum possible terms of $f$. $f$ is sparse if $\ell < \mathcal{T}(\ell) = \binom{n}{d}$. We interpolate $f$ modulo a set of primes $p_1, p_2, \ldots, p_n$ and use Chinese remaindering to recover the integer coefficients. We use a Kronecker substitution to reduce multivariate interpolation to a univariate interpolation.

Example Let $f(x, y, z) = 2x^3y^2z^4 + 2x^4 + 2x^2 + 2z^2 + 3$. Kronecker's algorithm is $(x \mod m_1, y \mod m_2, z \mod m_3)$.

Procedure Interpolate Exponents mod p-1:

**INPUT:** Black Box polynomial $g$ and a prime $p$.

**OUTPUT:** $E$ mod $p - 1$.

(1) Pick a generator $a \in Z_p^*$.

(2) For $1 \leq j \leq m - 1$ compute $e_j = g(a^j)$.

(3) Compute the roots of $(z \mod a) : a', a'', a''', \ldots (mod p)$. (4) Solve mod $p$ by taking the discrete logarithm: $\log_a(e^*) = e_j mod p - 1$.

**Modular Images**

$G \mapsto \left( E \mod m_1, E \mod m_2, E \mod m_3 \right)$

$\text{Sorted mod } E$:

$\text{Sort mod } E$:

The moduli we choose share a common divisor $\delta$. That is, for all $1 \leq i \leq n, p_i = \delta + i$. If we make $\delta$ large enough then the birthday paradox tells us

$\delta > \sqrt{n} \Rightarrow \text{Prob[unique exponents]} > 0$.

If the exponents are unique mod $\delta$ then the modular images are unique mod $\delta$, and therefore we can sort them mod $\delta$.

$\sum_{i=1}^{m} E \mod p_i - 1$ $\Rightarrow \left( e_1, e_2, e_3, \ldots e_n \right)$

$G \mapsto \left( e_1, e_2, e_3, \ldots e_n \right)$

We recover the exponents from their modular images, and therefore first need to pair up the modular images into sets that correspond to the right exponents. This is a challenge because their order is unknown.

**References**


