

## Multivariate Rational Function Interpolation

```

1: Input: Modular black box  $B : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$  for rational function
    $\frac{ff(x_1, \dots, x_n)}{gg(x_1, \dots, x_n)}$  over  $\mathbb{Z}_p$ , where  $ff, gg \in \mathbb{Z}_p[x_1, \dots, x_n]$ ,  $\gcd(ff, gg) = 1$ ,
    $gg$  is monic, prime  $p$ , number of variables  $n$ , and list of variables  $vars$ .
2: Output:  $ff(x_1, \dots, x_n), gg(x_1, \dots, x_n)$  or FAIL.
3:  $Primes \leftarrow [2, 3, \dots, p_n] \in \mathbb{Z}_p^n$ 
4: Pick random vector  $\beta = [\beta_2, \dots, \beta_n] \in \mathbb{Z}_p^{n-1}$ 
5:  $num \leftarrow [], den \leftarrow []$ 
6:  $num\_points\_mqrfr \leftarrow 0$ 
7:  $numerator\_done \leftarrow \text{false}$ 
8:  $denominator\_done \leftarrow \text{false}$ 
9:  $T\_old \leftarrow 0$ 
10:  $T \leftarrow 4$ 
11:  $\sigma^0 \leftarrow [1, \dots, 1] \in \mathbb{Z}_p^n$ 
12:  $(f, g) \leftarrow \text{NDSA}(B, \sigma^0, \beta, p, T)$ 
13:  $num\_points\_mqrfr \leftarrow \deg(f) + \deg(g) + 2$ 
14: while true do
15:   for  $j \leftarrow 2T\_old$  to  $2T - 1$  do
16:      $\sigma^j \leftarrow [2^j, 3^j, \dots, p_n^j] \bmod p$ 
17:      $(f_j, g_j) \leftarrow \text{NDSA}(B, \sigma^j, \beta, p, num\_points\_mqrfr)$ 
18:     if not  $numerator\_done$  then
19:        $num.append(f_j(\sigma_1^j) \bmod p)$ 
20:     end if
21:     if not  $denominator\_done$  then
22:        $den.append(g_j(\sigma_1^j) \bmod p)$ 
23:     end if
24:   end for
   Construct minimum characteristic polynomials using Berlekamp-
   Massey algorithm
25:   if not  $numerator\_done$  then
26:      $\Lambda_{num}(z) \leftarrow \text{Berlekamp\_Massey}(num, p, z) \in \mathbb{Z}_p[z]$ 
27:      $s \leftarrow \deg(\Lambda_{num}(z))$ 
28:     Let  $roots_{num}$  be the distinct roots of  $\Lambda_{num}(z) \in \mathbb{Z}_p[z]$ .
29:   end if
30:   if not  $denominator\_done$  then
31:      $\Lambda_{den}(z) \leftarrow \text{Berlekamp\_Massey}(den, p, z) \in \mathbb{Z}_p[z]$ 
32:      $d \leftarrow \deg(\Lambda_{den}(z))$ 
33:     Let  $roots_{den}$  be the distinct roots of  $\Lambda_{den}(z) \in \mathbb{Z}_p[z]$ .
34:   end if
35:   if  $s = |roots_{num}|$  and  $s < T$  then
36:      $numerator\_done \leftarrow \text{true}$ 
37:   end if
38:   if  $d = |roots_{den}|$  and  $d < T$  then
39:      $denominator\_done \leftarrow \text{true}$ 

```

```

40:   end if
41:   if  $numerator\_done \wedge denominator\_done$  then
42:     break
43:   end if
44:    $T_{old} \leftarrow T$ 
45:    $T \leftarrow 2T$ 
46: end while
    Recover monomials from roots using trial division
47:  $N \leftarrow \text{get\_monomial}(roots_{num}, Primes, n, vars)$ 
48:  $D \leftarrow \text{get\_monomial}(roots_{den}, Primes, n, vars)$ 
49: if  $N = \text{FAIL}$  or  $D = \text{FAIL}$  then
50:   return FAIL
51: end if
52: Recover coefficients via Zippel Vandermonde solver
53:  $A \leftarrow \text{Zippel\_Vandermonde\_solver}(num, s, roots_{num}, \Lambda_{num}(z), p)$ 
54:  $B \leftarrow \text{Zippel\_Vandermonde\_solver}(den, d, roots_{den}, \Lambda_{den}(z), p)$ 
55:  $ff \leftarrow \sum_{m=1}^s A_m N_m, \quad gg \leftarrow \sum_{m=1}^d B_m D_m$ 
56: Let  $\mu$  be the leading coefficient of  $gg$  in grlex order where  $x_1 > \dots > x_n$ .
57:  $ff \leftarrow \mu^{-1} ff \bmod p, \quad gg \leftarrow \mu^{-1} gg \bmod p$ .
58: return  $ff, gg$ .

```

### Numerator Denominator Separation Algorithm (NDSA)

- 1: **Input:** Modular black box  $B$  for rational function  $\frac{ff(x_1, \dots, x_n)}{gg(x_1, \dots, x_n)}$  over  $\mathbb{Z}_p$ , prime  $p$ , where  $ff, gg \in K[x_1, \dots, x_n]$ ,  $\gcd(ff, gg) = 1$ ,  $\sigma \in \mathbb{Z}_p^n$ ,  $\beta \in \mathbb{Z}_p^{n-1}$ ,  $num\_points \in \mathbb{N}$ .
- 2: **Output:**  $f(x) = \frac{ff(x, \beta_2(x-\sigma_1)+\sigma_2, \dots, \beta_n(x-\sigma_1)+\sigma_n)}{c}$ ,  $g(x) = \frac{gg(x, \beta_2(x-\sigma_1)+\sigma_2, \dots, \beta_n(x-\sigma_1)+\sigma_n)}{c}$ , for some scalar  $c \in \mathbb{Z}_p^n$ .
- 3:  $t \leftarrow num\_points$
- 4: **while** true **do**
- 5:     Pick random vector  $\alpha = [\alpha_1, \dots, \alpha_t] \in \mathbb{Z}_p^t$
- 6:      $m(x) \leftarrow \prod_{k=1}^t (x - \alpha_k) \in \mathbb{Z}_p[x]$
- 7:      $\Phi \leftarrow [\phi(\alpha_1), \dots, \phi(\alpha_t)] \in \mathbb{Z}_p^{t \times n}$  such that:  $\phi(\alpha_k) \leftarrow [\alpha_k, \beta_2(\alpha_k - \sigma_1) + \sigma_2, \dots, \beta_n(\alpha_k - \sigma_1) + \sigma_n] \pmod p \forall 1 \leq k \leq t$
- 8:      $Y \leftarrow [B(\Phi(\alpha_1), p), \dots, B(\Phi(\alpha_t), p)] \in \mathbb{Z}_p^t$
- 9:      $u(x) \leftarrow \text{Interpolate}(\alpha, Y, x) \pmod p$
- 10:      $(f(x), g(x), deg\_q) \leftarrow \text{MQRFR}(m, u) \pmod p$
- 11:     **if**  $deg\_q > 1$  **then**
- 12:         **break**
- 13:     **else**
- 14:          $t \leftarrow 2t$
- 15:     **end if**
- 16: **end while**
- 17: **return**  $f, g$