Multivariate Rational Function Interpolation

Input: Modular black box B for rational function $\frac{ff(x_1,\ldots,x_n)}{gg(x_1,\ldots,x_n)}$ over $\mathbb{Z}_p$, where $ff, gg \in K[x_1, \ldots, x_n]$ and $\gcd(ff, gg) = 1$
Output: $ff(x_1, \ldots, x_n), gg(x_1, \ldots, x_n)$ or **FAIL**
$\sigma \leftarrow [2, 3, \ldots, p_n] \in \mathbb{Z}_p^n$
Pick random vector $\beta = [\beta_2, \ldots, \beta_n] \in \mathbb{Z}_p^{n-1}$
$num \leftarrow [\,]$, $den \leftarrow [\,]$
$T \leftarrow 4$
$num\_points\_mqrfr \leftarrow 0$
$berlekamp\_failure \leftarrow$ true
$numerator\_failure \leftarrow$ true
$denominator\_failure \leftarrow$ true
$j\_init \leftarrow 2$, $t\_old \leftarrow 0$
while true **do**
  for $l \leftarrow t\_old$ to $2T - 1$ **do**
    $\sigma_l \leftarrow [2^l, 3^l, \ldots, p_n^l] \mod p$
  end for
  if $i == 1$ **then**
    $(f, g) \leftarrow \mathrm{NDSA}(B, \sigma_0, \beta, T)$
    $num\_points\_mqrfr \leftarrow \deg(f) + \deg(g) + 2$
  end if
  for $j \leftarrow j\_init$ to $2T - 1$ **do**
    $(f_j, g_j) \leftarrow \mathrm{NDSA}(B, \sigma_j, \beta, num\_points\_mqrfr)$
    if $numerator\_failure$ **then**
      $num.\mathrm{insert}(f_j(\sigma_{j1}) \mod p)$
    end if
    if $denominator\_failure$ **then**
      $den.\mathrm{insert}(g_j(\sigma_{j1}) \mod p)$
    end if
  end for
  Construct minimum characteristic polynomials using Berlekamp-Massey algorithm
  if $numerator\_failure$ **then**
    $\Lambda_n \leftarrow \mathrm{Berlekamp\_Massey}(num, p)$
    $s \leftarrow \deg(\Lambda_n)$
    $roots_n \leftarrow \mathrm{ROOTS}(\Lambda_n)$
  end if
  if $denominator\_failure$ **then**
    $\Lambda_d \leftarrow \mathrm{Berlekamp\_Massey}(den, p)$
    $d \leftarrow \deg(\Lambda_d)$
    $roots_d \leftarrow \mathrm{ROOTS}(\Lambda_d)$
  end if
  if $s == |roots_n|$ **then**

$numerator\_failure \leftarrow$ false
end if
if $d == |roots_d|$ **then**
$denominator\_failure \leftarrow$ false
end if
$berlekamp\_failure \leftarrow numerator\_failure \vee denominator\_failure$
if not $berlekamp\_failure$ **then**
break
end if
$i \leftarrow i + 1$
$T \leftarrow 2T$
$t\_old \leftarrow T$
$j\_init \leftarrow t\_old + 1$
end while
Recover monomials from roots using trial division
$N \leftarrow$ get_monomial$(roots_n, num, \sigma, n, vars)$
$D \leftarrow$ get_monomial$(roots_d, den, \sigma, n, vars)$
if N = FAIL or D = FAIL **then**
return FAIL
else
Recover coefficients via Zippel Vandermonde solver
$Ncoeff \leftarrow$ Zippel_Vandermonde_solver$(num, s, roots_n, \Lambda_n, p)$
$Dcoeff \leftarrow$ Zippel_Vandermonde_solver$(den, d, roots_d, \Lambda_d, p)$
return $\sum_{m=1}^{s} Ncoeff_m N_m, \quad \sum_{m=1}^{d} Dcoeff_m D_m$
end if

Numerator Denominator Separation Algorithm (NDSA)

Input: Modular black box B for rational function $\frac{ff(x_1,\ldots,x_n)}{gg(x_1,\ldots,x_n)}$ over $\mathbb{Z}_p$, prime p, where $ff, gg \in K[x_1,\ldots,x_n]$, $\gcd(ff,gg)=1$, $\sigma \in \mathbb{Z}_p^n$, $\beta \in \mathbb{Z}_p^{n-1}$, $num\_points \in \mathbb{N}$.

Output: $f(x) = \frac{ff(x,\beta_2(x-\sigma_1)+\sigma_2,\ldots,\beta_n(x-\sigma_1)+\sigma_n)}{c}$, $g(x) = \frac{gg(x,\beta_2(x-\sigma_1)+\sigma_2,\ldots,\beta_n(x-\sigma_1)+\sigma_n)}{c}$

$t \leftarrow num\_points$

while true **do**

  Pick random vector $\alpha = [\alpha_1,\ldots,\alpha_t] \in \mathbb{Z}_p^t$

  $m(x) \leftarrow \prod_{k=1}^{t}(x-\alpha_k) \in \mathbb{Z}_p[x]$

  $\Phi \leftarrow [\phi(\alpha_1),\ldots,\phi(\alpha_t)] \in \mathbb{Z}_p^{t\times n}$ such that: $\phi(\alpha_k) \leftarrow [\alpha_k, \beta_2(\alpha_k - \sigma_1)+\sigma_2,\ldots,\beta_n(\alpha_k-\sigma_1)+\sigma_n] \mod p \; \forall\, 1 \le k \le t$

  $Y \leftarrow [B(\phi(\alpha_1),p),\ldots,B(\phi(\alpha_t),p)] \in \mathbb{Z}_p^t$

  $u(x) \leftarrow \text{Interpolate}(\alpha, Y, x) \mod p$

  $(f(x), g(x), deg\_q) \leftarrow \text{MQRFR}(m,u) \mod p$

  if $deg\_q > 1$ **then**

    break

  else

    $t \leftarrow 2t$

  end if

end while

return f, g