Algorithm 3 Multivariate rational function interpolation

Require: Black box for rational function $\frac{ff(x_1,x_2,\ldots,x_n)}{gg(x_1,x_2,\ldots,x_n)}$, p, where $ff, gg \in K(x_1, x_2, \ldots, x_n)$.

while true **do**
    $num \leftarrow [\ ]$
    $den \leftarrow [\ ]$
    $T \leftarrow 4$
    for $i \leftarrow 0$ to T **do**
        $\Sigma \leftarrow [[2^i, 3^i, \ldots, \Psi^i]]$, where $\sigma_i \leftarrow [2^i, 3^i, \ldots, \Psi^i] \in \mathbb{Z}_p^n$
        while true **do**
            $t \leftarrow T$
            Pick random vector $\alpha_i = [\alpha_{i1}, \ldots, \alpha_{it}] \in \mathbb{Z}_p^t$
            Pick random vector $\beta_i = [\beta_{i1}, \ldots, \beta_{i(n-1)}] \in \mathbb{Z}_p^{n-1}$
            $m_i(x) = \prod_{k=1}^{t}(x - \alpha_{ik})$, where $m_i(x) \in \mathbb{Z}_p[x]$.
            $[[\alpha_{ik}, \phi(\alpha_{ik})]]$ where $[\alpha_{ik}, \phi(\alpha_{ik})] \in \mathbb{Z}_p^n$ and $\phi(x) \leftarrow \beta_{ij}(x - \sigma_{i1}) + \sigma_{i(j+1)},\ \forall\ 1 \leq j \leq n-1$
            $Y_i \leftarrow [y_i, \ldots, y_{it}],$ where $y_{ik} \leftarrow B(\alpha_{ik}, \phi(\alpha_{ik}), p)\ \forall\ 1 \leq k \leq t$
            $u_i(x) \leftarrow Interpolate(\alpha_i, Y_i, x)$mod p
            $f_i(x), g_i(x), deg_q_i \leftarrow MQRFR(m_i, u_i)$mod p
            if $deg\_q_i > 1$ **then**
                $num.insert(f_i(\sigma_{i1}))$ mod p
                $den.insert(g_i(\sigma_{i1}))$ mod p
                break
            else
                $t \leftarrow 2t$
            end if
        end while
    end for
    Construct minimum characateristic polynomial using Berlekamp-Massey algorithm
    $\Lambda_n \leftarrow Berlekamp\_Massey(num, p)$
    $\Lambda_d \leftarrow Berlekamp\_Massey(den, p)$
    Find number of terms in denominator and numerator
    $terms_n \leftarrow$ degree(Λ_n)
    $terms_d \leftarrow$ degree(Λ_d)
    Factor $\Lambda_n(z)$ and $\Lambda_d(z)$ to find roots
    $roots_n \leftarrow$ ROOTS(Λ_n)
    $roots_d \leftarrow$ ROOTS(Λ_d)
    Check if number of terms and roots are equal
    if $terms_n \neq roots_n$ or $terms_d \neq roots_d$ **then**
        $T \leftarrow 2T$
    else
        break
    end if
end while
Recover monomials from roots using trial division
Recover coefficients via Zippel Vandermonde solver
$coeff_n \leftarrow$ Zippel_Vandermonde_solver($num, terms_n, Roots_n, \Lambda_n, p$)
$coeff_d \leftarrow$ Zippel_Vandermonde_solver($den, terms_d, Roots_d, \Lambda_d, p$)