Algorithm 1 MFR of finite field arithmetic circuits

Require: $Spec : f, buggy\ Impl : C$ modeled as a polynomial ideal $F = \{f_1 \ldots, f_s\}$ under $RTTO >$
Assume: C doesn't admit single-fix rectification //[*Rao. et al*, FMCAD'18]
Ensure: Rectification of C to match f

procedure $rectification$
  remainder = $verify(f, F + F_0)$ // Verification
  $O_a = analyze$(remainder) // Error Diagnosis
  $I_n = PotentialNets()$
  $m = 2$; rectified = $False$; $O_A = \emptyset$; $\mathcal{M}_i = \emptyset$; $\mathcal{F}_w = \emptyset$
  do
    $\{O_A\} = SetsOfUniquePartitions(O_a, m)$
    for each $O_A^i \in O_A$ **do**
      $\{\mathcal{M}_i\} = SetsOfIntersectionCovers(O_A^i)$
      for each $\mathcal{M}_i^j \in \mathcal{M}_i$ **do**
        $\{\mathcal{F}_w\} = SetsOfDistinctTargets(\mathcal{M}_i^j, m)$
        for each $f_w \in \mathcal{F}_w$ **do**
          $F', P_k(X) = MFRSetup(F, f_w)$ //MFR Notations
          if $MFRCheck(F') == 0$ **then** //MFR Check
            rectified = $True$
            U = $rectFunction()$ // Function Computation
            break out of all **for** loops
  while (!rectified && $(++m \leq |O_a|)$)
  return U