

Input: \mathcal{P} : $\{p_j(\mathbf{x})\}_{i=0}^{m-1}$, m : Integer, n : Integer, n_1 : Integer
Result: A solution to the system \mathcal{P}
 PREPROCESS(\mathcal{P})
 $\ell \leftarrow n_1 + 1$
 $PotentialSolutions \leftarrow []$
foreach $k = 0, \dots$ **do**
 $A \leftarrow \text{MATRIX}(\ell, m)$
 $\tilde{\mathcal{P}}_k \leftarrow \{\sum_{j=0}^{m-1} A_{i,j} \cdot p_j(\mathbf{x})\}_{i=0}^{\ell-1}$
 $w \leftarrow (\sum_{i=0}^{\ell-1} \tilde{\mathcal{P}}_k.\text{degrees}()[i]) - n_1$
 $CurrPotentialSolutions \leftarrow \text{OUTPUT_POTENTIALS}(\tilde{\mathcal{P}}_k, n, n_1, w)$
 $PotentialSolutions[k] \leftarrow CurrPotentialSolutions$
 foreach $\hat{y} \in \{0, 1\}^{n-n_1}$ **do**
 if $CurrPotentialSolutions[\hat{y}][0] = 1$ **then**
 foreach $k_1 = 0, \dots k - 1$ **do**
 if
 $CurrPotentialSolutions[\hat{y}] = PotentialSolutions[k_1][\hat{y}]$
 then
 $sol \leftarrow \hat{y} \parallel CurrPotentialSolutions[\hat{y}]$
 if $\text{TEST_SOLUTION}(\mathcal{P}, sol)$ **then**
 return sol
 end
 end
 end
 end
 end
end

Algorithm 1: SOLVE(\mathcal{P} , m , n , n_1)

Input: $\tilde{\mathcal{P}}$: $\{r_i(\mathbf{x})\}_{i=0}^{\ell-1}$, n : Integer, n_1 : Integer, w : Integer
Result: A two-dimensional list of size $2^{n-n_1} \times (n_1 + 1)$ containing the z_i bits, y bits and $U_0(y)$ bit.
 $(V, ZV[0, \dots (n_1 - 1)]) \leftarrow \text{COMPUTE_U_VALUES}(\tilde{\mathcal{P}}, n, n_1, w)$
 $U_0 \leftarrow \text{MOB_TRANSFORM}(V[0 \dots |W_w^{n-n_1}| - 1], n - n_1)$
foreach $i = 1 \dots n_1$ **do**
 $U_i \leftarrow \text{MOB_TRANSFORM}(ZV[i][0, \dots, |W_{w+1}^{n-n_1}| - 1], n - n_1)$
end
 $Evals[0 \dots n_1][0 \dots 2^{n-n_1} - 1] \leftarrow \{0\}$
foreach $i = 0 \dots n_1$ **do**
 $Evals[i][0 \dots 2^{n-n_1} - 1] \leftarrow \text{MOB_TRANSFORM}(U_i.\text{as_array}(), n - n_1)$
end
 $Out[0 \dots 2^{n-n_1} - 1][0 \dots n_1] \leftarrow \{0\}$
foreach $\hat{y} \in \{0, 1\}^{n-n_1}$ **do**
 if $Evals[0][\hat{y}] = 1$ **then**
 $Out[\hat{y}][0] \leftarrow 1$
 foreach $i = 1 \dots n_1$ **do**
 $Out[\hat{y}][i] \leftarrow Evals[i][\hat{y}] + 1$
 end
 end
end
return Out

Algorithm 2: OUTPUT_POTENTIALS($\tilde{\mathcal{P}}$, n , n_1 , w)

Input: $\tilde{\mathcal{P}}$: $\{r_i(\mathbf{x})\}_{i=0}^{\ell-1}$, n_1 : Integer, w : Integer
Result: Lists V and ZV containing evaluations of $U_i(y), \forall i \in \{0, \dots n_1\}, \forall y \in \{y \mid y \in \{0, 1\}^{n-n_1}, hw(y) \leq w\}$
 $Sols[0 \dots L - 1] \leftarrow \text{BRUTEFORCE}(\mathcal{P}, n, n_1, w + 1)$
 $V[0 \dots |W_w^{n-n_1}| - 1] \leftarrow \{0\}$
 $ZV[0 \dots n_1][0 \dots |W_{w+1}^{n-n_1}| - 1] \leftarrow \{0\}$
foreach $s \in Sols$ **do**
 $\hat{y}, \hat{z} \leftarrow s[0 \dots n - n_1 - 1], s[n - n_1 \dots n - 1]$
 if $\text{HAMMING_WEIGHT}(\hat{y}) \leq w$ **then**
 $idx \leftarrow \text{INDEX_OF}(\hat{y}, n - n_1, w)$
 $V[idx]++$
 end
 foreach $i = 1 \dots n_1$ **do**
 if $z_i = 0$ **then**
 $idx \leftarrow \text{INDEX_OF}(\hat{y}, n - n_1, w + 1)$
 $ZV[i][idx]++$
 end
 end
end
return $V, ZV[1 \dots n_1]$

Algorithm 3: COMPUTE_U_VALUES($\tilde{\mathcal{P}}$, n , n_1 , w)

Input: For some polynomial p , the degree d , amount of variables n , and a sparsely filled truth-table S .
Result: The full truth-table of p , stored in R .
 $R[0 \dots 2^n - 1] \leftarrow \{0\};$
 $D \leftarrow \text{DICT}(\text{default: } 0);$
 $R[0], D[0] \leftarrow S[0], S[0];$
foreach $i = 1 \dots 2^n - 1$ **do**
 $Depth \leftarrow \min(\text{HAMMING_WEIGHT}(i), d);$
 $K \leftarrow \text{BITS}(i, Depth);$
 if $\text{HAMMING_WEIGHT}(i) > d$ **then**
 foreach $j = Depth \dots 1$ **do**
 $D[K_{0\dots j-1}] \leftarrow D[K_{0\dots j-1}] \oplus D[K_{0\dots j}];$
 end
 else
 $Q \leftarrow D[0];$
 $D[0] \leftarrow S[\text{GRAY}(i)];$
 foreach $j = 1 \dots Depth$ **do**
 if $j < Depth$ **then**
 $Tmp \leftarrow D[K_{0\dots j}];$
 end
 $D[K_{0\dots j}] \leftarrow D[K_{0\dots j-1}] \oplus Q;$
 if $j < Depth$ **then**
 $Q \leftarrow Tmp;$
 end
 end
 end
 $R[\text{GRAY}(i)] = D[0];$
end
return $R;$

Algorithm 4: FES_RECOVER(d , n , S)