Testing Interleaved Linear Codes

Testing Interleaved Linear Codes

DEFINITION 4.2 (INTERLEAVED CODE). *Let $L \subset \mathbb{F}^n$ be an $[n, k, d]$ linear code over $\mathbb{F}$. We let L^m denote the $[n, mk, d]$ (interleaved) code over $\mathbb{F}^m$ whose codewords are all $m \times n$ matrices U such that every row U_i of U satisfies $U_i \in L$. For $U \in L^m$ and $j \in [n]$, we denote by $U[j]$ the jth symbol (column) of U.*

Testing Interleaved Linear Codes

- **Oracle:** A purported L^m-codeword U. Depending on the context, we may view U either as a matrix in $\mathbb{F}^{m \times n}$ in which each row U_i is a purported L-codeword, or as a sequence of n symbols $(U[1], \ldots, U[n])$, $U[j] \in \mathbb{F}^m$.
- **Interactive testing:**
  (1) $\mathcal{V}$ picks a random linear combinations $r \in \mathbb{F}^m$ and sends r to $\mathcal{P}$.
  (2) $\mathcal{P}$ responds with $w = r^T U \in \mathbb{F}^n$.
  (3) $\mathcal{V}$ queries a set $Q \subset [n]$ of t random symbols $U[j]$, $j \in Q$.
  (4) $\mathcal{V}$ accepts iff $w \in L$ and w is consistent with U_Q and r. That is, for every $j \in Q$ we have $\sum_{i=1}^{m} r_j \cdot U_{i,j} = w_j$.

The following lemma follows directly from the linearity of L.

Lemma 4.1. *If $U \in L^m$ and $\mathcal{P}$ is honest, then $\mathcal{V}$ always accepts.*

Testing Interleaved Linear Codes

THEOREM 4.4. *Suppose Conjecture 4.1 holds. Let* e *be a positive integer such that* $e < d/3$. *Suppose* $d(U^*, L^m) > e$. *Then, for any malicious* $\mathcal{P}$ *strategy, the oracle* U^* *is rejected by* $\mathcal{V}$ *except with* $\leq (1 - e/n)^t + d/|\mathbb{F}|$ *probability.*

Testing Linear Constraints over Interleaved Reed-Solomon Codes

Test-Linear-Constraints-IRS

DEFINITION 4.5 (ENCODED MESSAGE). *Let* $L = \mathrm{RS}_{\mathbb{F},n,k,\eta}$ *be an RS code and* $\zeta = (\zeta_1, \ldots, \zeta_\ell)$ *be a sequence of distinct elements of* $\mathbb{F}$ *for* $\ell \leq k$. *For* $u \in L$ *we define the message* $\mathrm{Dec}_\zeta(u)$ *to be* $(p_u(\zeta_1), \ldots, p_u(\zeta_\ell))$, *where* p_u *is the polynomial (of degree* $< k$*) corresponding to* u. *For* $U \in L^m$ *with rows* $u^1, \ldots, u^m \in L$, *we let* $\mathrm{Dec}_\zeta(U)$ *be the length-*$m\ell$ *vector* $x = (x_{11}, \ldots, x_{1\ell}, \ldots, x_{m1}, \ldots, x_{m\ell})$ *such that* $(x_{i1}, \ldots, x_{i\ell}) = \mathrm{Dec}_\zeta(u^i)$ *for* $i \in [m]$. *Finally, when* ζ *is clear from the context, we say that* U encodes x *if* $x = \mathrm{Dec}_\zeta(U)$.

Test-Linear-Constraints-IRS

Test-Linear-Constraints-IRS$(\mathbb{F}, L = \mathrm{RS}_{\mathbb{F},n,k,\eta}, m, t, \zeta, A, b; U)$

- **Oracle:** A purported L^m-codeword U that should encode a message $x \in \mathbb{F}^{m\ell}$ satisfying $Ax = b$.
- **Interactive testing:**
  (1) $\mathcal{V}$ picks a random vector $r \in \mathbb{F}^{m\ell}$ and sends r to $\mathcal{P}$.
  (2) $\mathcal{V}$ and $\mathcal{P}$ compute

  $$r^T A = (r_{11}, \ldots, r_{1\ell}, \ldots, r_{m1}, \ldots, r_{m\ell})$$

  and, for $i \in [m]$, let $r_i(\cdot)$ be the unique polynomial of degree $< \ell$ such that $r_i(\zeta_c) = r_{ic}$ for every $c \in [\ell]$.

  (3) $\mathcal{P}$ sends the $k + \ell - 1$ coefficients of the polynomial defined by $q(\bullet) = \sum_{i=1}^{m} r_i(\bullet) \cdot p_i(\bullet)$, where p_i is the polynomial of degree $< k$ corresponding to row i of U.
  (4) $\mathcal{V}$ queries a set $Q \subset [n]$ of t random symbols $U[j]$, $j \in Q$.
  (5) $\mathcal{V}$ accepts if the following conditions hold:
    (a) $\sum_{c\in[\ell]} q(\zeta_c) = \sum_{i\in[m], c\in[\ell]} r_{ic} b_{ic}$.
    (b) For every $j \in Q$, $\sum_{i=1}^{m} r_i(\eta_j) \cdot U_{i,j} = q(\eta_j)$.

Test-Linear-Constraints-IRS

LEMMA 4.6. *Let e be a positive integer such that $e < d/2$. Suppose that a (badly formed) oracle U^* is e-close to a codeword $U \in L^m$ encoding $x \in \mathbb{F}^{m\ell}$ such that $Ax \neq b$. Then, for any malicious $\mathcal{P}$ strategy, U^* is rejected by $\mathcal{V}$ except with at most $((e+k+\ell)/n)^t + 1/|\mathbb{F}|$ probability.*

Testing Quadratic Constraints over Interleaved Reed-Solomon Codes

Testing Quadratic Constraints over Interleaved Reed-Solomon Codes

We want to check $x \odot y + a \odot z = b$ for some known $a, b \in \mathbb{F}^{m\ell}$, where $\odot$ denotes pointwise product. Letting $L = \mathrm{RS}_{\mathbb{E},n,k,\eta}$, $U_a = \mathsf{Enc}(a)$ and $U_b = \mathsf{Enc}(b)$, this reduces to checking that $U^x \odot U^y + U^a \odot U^z - U^b$ encodes the all- 0 message $0^{m\ell}$

Testing Quadratic Constraints over Interleaved Reed-Solomon Codes

Test-Quadratic-Constraints-IRS($\mathbb{F}, L = \mathsf{RS}_{\mathbb{F},n,k,\eta}, m, t, \zeta, a, b; U^x, U^y, U^z$)

- **Oracle:** Purported L^m-codewords U^x, U^y, U^z that should encode messages $x, y, z \in \mathbb{F}^{m\ell}$ satisfying $x \odot y + a \odot z = b$.
- **Interactive testing:**
  1. Let $U^a = \mathsf{Enc}_\zeta(a)$ and $U^b = \mathsf{Enc}_\zeta(b)$.
  2. $\mathcal{V}$ picks a random linear combinations $r \in \mathbb{F}^m$ and sends r to $\mathcal{P}$.
  3. $\mathcal{P}$ sends the $2k-1$ coefficients of the polynomial p_0 defined by $p_0(\bullet) = \sum_{i=1}^m r_i \cdot p_i(\bullet)$, where $p_i(\bullet) = p_i^x(\bullet) \cdot p_i^y(\bullet) + p_i^a(\bullet) \cdot p_i^z(\bullet) - p_i^b(\bullet)$, and where p_i^x, p_i^y, p_i^z are the polynomials of degree $< k$ corresponding to row i of U^x, U^y, U^z, and p_i^a, p_i^b are the polynomials of degree $< \ell$ corresponding to row i of U^a, U^b.
  4. $\mathcal{V}$ picks a random index set $Q \subset [n]$ of size t, and queries $U^x[j], U^y[j], U^z[j], j \in Q$.
  5. $\mathcal{V}$ accepts if the following conditions hold:
     (a) $p_0(\zeta_c) = 0$ for every $c \in [\ell]$.
     (b) For every $j \in Q$, it holds that

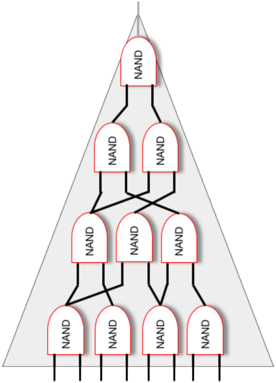
$$\sum_{i=1}^m r_i \cdot \left[U_{i,j}^x \cdot U_{i,j}^y + U_{i,j}^a \cdot U_{i,j}^z - U_{i,j}^b\right] = p_0(\eta_j).$$

Testing Quadratic Constraints over Interleaved Reed-Solomon Codes

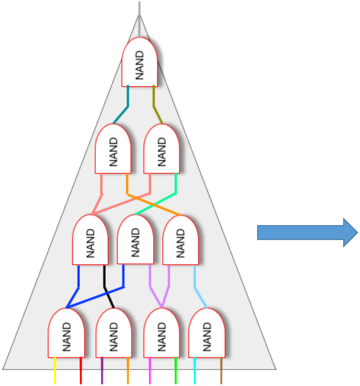
Suppose U^x, U^y, U^z *encode* x, y, z *such that* $x \odot y + a \odot z \neq b$. *Then, for any malicious* $\mathcal{P}$ *strategy,* (U^{x*}, U^{y*}, U^{z*}) *is rejected by* $\mathcal{V}$ *except with at most* $1/|\mathbb{F}| + ((e + 2k)/n)^t$ *probability.*

Summary

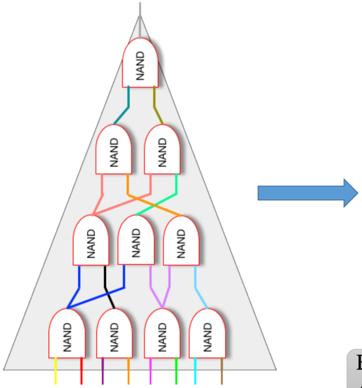
Summary

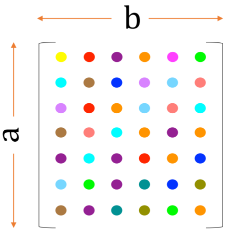


Summary



Summary

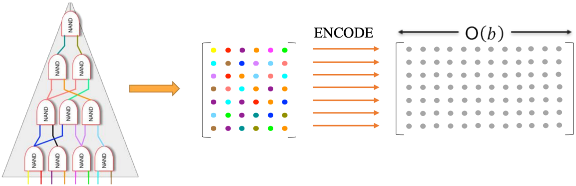




$$a \cdot b \geq X \cdot \#\text{gates}$$

Boolean: $X = 2$, AND/XOR
Arithmetic: $X = 3$, AND

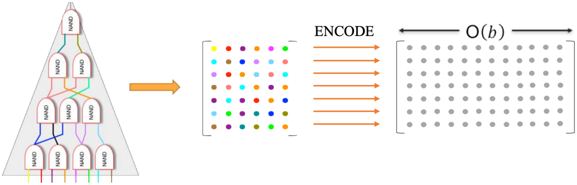
Summary



Prover

Verifier

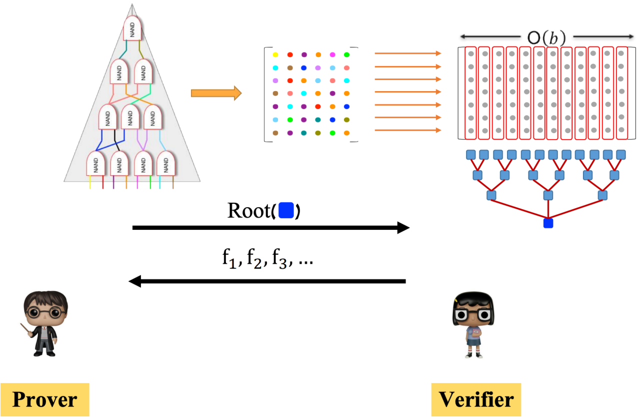
Summary



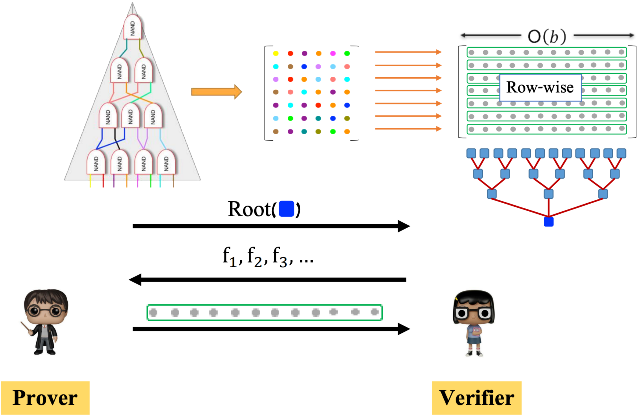
Prover

Verifier

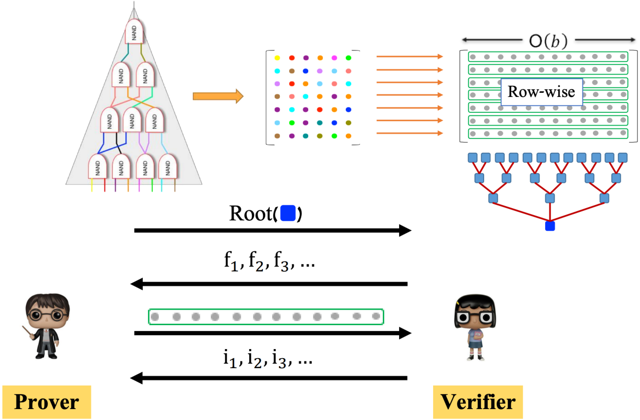
Summary



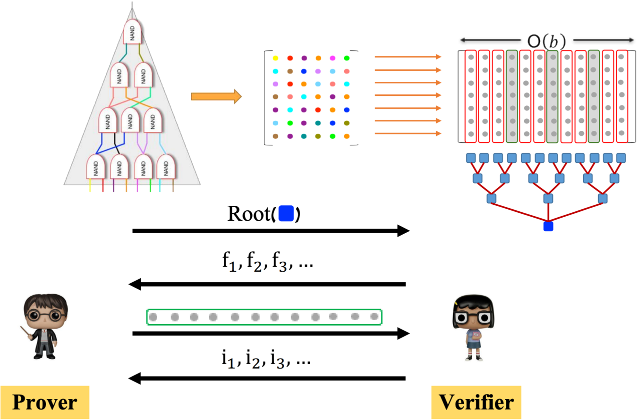
Summary



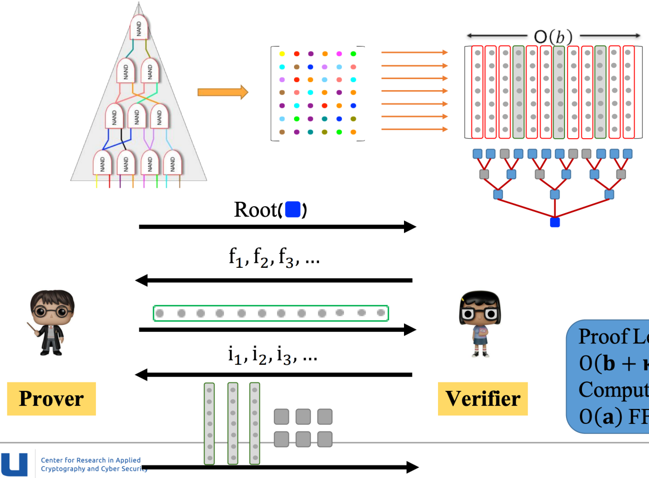
Summary



Summary



Summary



Proof Length:
$O(\mathbf{b} + \boldsymbol{\kappa} \cdot \mathbf{a})$
Computation:
$O(\mathbf{a})$ FFTs of $O(\mathbf{b})$

Idea

if we arrange the wire values on a 3-dimension matrix say $(a \times b \times c)$ which again their multiplication should be larger than the size of the circuit, say $(a \times b \times c) > 3C$, then we can have $a = b = c = C^{1/3}$ or we can play with them to achieve the best. This might allow us to have smaller value for $O(b + \kappa a)$, say $O(b' + \kappa a')$ which $a' := O(C^{1/3})$.

now the point is that the prover cannot encode each row of the matrix with a standard RS code, as we have three dimensions ... to cope with this issue I was interested to think about 2-dimension RS codes

Reading list for next week

- Two-dimensional generalized Reed-Solomon codes
- Ligero++