

Zero-Knowledge Proof Systems with Distributed Proof Generation

No Author Given

No Institute Given

Abstract. Zero knowledge is an intriguing area of research from the prospect of theory as well as application, where a party, prover P , tries to convince verifier V that a statement x (instance of an NP language) is correct using a witness w such that $M(x, w) = 1$. Let C be the circuit representation of M and $|C|$ is the size of C i.e. the no. of gates in C . The work of Ligero in this problem proposed a solution where proof size is $O(|C|^{1/2})$. They solve the problem by converting a NP language to its corresponding circuit satisfiability problem. $w \in \mathbb{F}^{ml}$ be the extended witness which is the secret input to the prover. Prover P encodes w to a matrix U of size $m \times n$, where $m, n, l = O(\sqrt{|C|})$ and $n > l$. In Ligero's protocol first check is for to ensure that the matrix U is a correct encoding, that is done by testing interleaved. Then they check that all the outcomes of all the gates (addition and multiplication) are correct or not, and to do that they introduce two checks, linear constraint and quadratic constraint. We are using the same approach of Ligero, but our encoding is different. Instead of matrix we will encode w to a box (matrix of 3 dimensions), to keep the familiarity of notation we will consider $w \in \mathbb{F}^{pml}$ and the size of the box U is $p \times m \times n$, where $p, m, n, l = O(\sqrt[3]{|C|})$ and $n > l$. To encode w we are going to construct pm many polynomials (univariate) such that each of them has degree at most s , where s is some suitable number between l and n .

1 Introduction

- Motivation for proving knowledge of witness, shared across different parties. —
- Our contributions —
- Prior work in brief —

1.1 Overview

Overview of our work: the notion, techniques.

Distributed proof generation

Informal notion of Distributed Provers Zero Knowledge Protocol (P,V)

Need for homomorphic commitments (Oracle access for IOP).

Technical summary

2 Preliminaries

2.1 Codes

Reed-Solomon Code: For positive integers n, k , finite field \mathbb{F} , and a vector $\eta = (\eta_1, \dots, \eta_n) \in \mathbb{F}_n$ of distinct field elements, the code $RS_{\mathbb{F}, n, k, \eta}$ is the $[n, k, n - k + 1]$ linear code over \mathbb{F} that consists of all n -tuples $(p(\eta_1), \dots, p(\eta_n))$ where $p(\cdot)$ is a polynomial of degree $< k$ over \mathbb{F} .

[VD: 1. Have spaces between paragraphs even in Latex. The PDF generated by Latex is usually beautiful and readable. The tex file can't be beautiful but should atleast be as readable as the PDF.
 2. I have already told you many time, and I am not going to leave till you use it :) Use macro for any notation that you use more than two times throughout the paper. (You will realize the use of it the day we decide change some notation in the middle of writing a paper.. But it is also a good practice to do it in general).
 3. Use `\ldots` for ...
 4. You could use `subsection*` or `subsubsection*` instead of having a paragraph and using a `\textbf` inside. (try both, what looks better depends on the cls file you use).]

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 code words 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 j^{th} symbol (column) of U .

[VD: Have "th" in jth outside math mode.]

2.2 Interactive Oracle Proofs

The Interactive Oracle Proofs is the notion which combine both Interactive Proofs and Probabilistically Checkable Proofs, and also generalize the notion of the Interactive PCPs.

A k -round public-coin IOP has k rounds of interaction. In the i^{th} round of interaction, the verifier sends a uniformly random message m_i to the prover; then the prover replies with a message π_i to the verifier. After k rounds of interaction, the verifier makes some queries to the oracles it received and either accepts or rejects.

[VD: Have at least the main definitions in the Definition environment.]

An IOP system for a relation \mathcal{R} with round complexity k and soundness error ϵ is a pair (P, V) , where P, V are probabilistic algorithms, that satisfies the following properties:

Completeness: For every instance-witness pair (x, w) in the relation \mathcal{R} , $(P(x, w), V(x))$ is a $k(n)$ -round interactive oracle protocol with accepting probability 1.

Soundness: For every instance $x \notin \mathcal{L}(\mathcal{R})$ and unbounded malicious prover P^* , $(P^*, V(x))$ is a $k(n)$ -round interactive oracle protocol with accepting probability at most $\epsilon(n)$.

2.3 Zero-Knowledge

Interactive Argument Systems: A pair of PPT(Probabilistic Polynomial Time) interactive machines $\langle P, V \rangle$ is called an interactive proof system for a language \mathcal{L} if there exists a negligible function $\text{negl}(\cdot)$ such that the following two conditions hold:

[VD: 1. have space before a (or any other bracket.

2. Use `\langle \rangle` and `\rangle` instead of `\langle` and `\rangle` when using it as brackets. 3. You can have `\text{negl}` in `\mathsf{}`, it would look better (have a macro for this too!)]

- (1) *Completeness:* For every $x \in \mathcal{L}$ there exists a string w such that for every $z \in \{0, 1\}^*$, $\Pr[\langle P(x, w), V(x, z) \rangle = 1] \geq 1 - \text{negl}(|x|)$.
- (2) *Soundness:* For every $x \notin \mathcal{L}$, every interactive PPT machine P^* , and every $w, z \in \{0, 1\}^*$ $\Pr[\langle P^*(x, w), V(x, z) \rangle = 1] \leq \text{negl}(|x|)$

Zero Knowledge: Let $\langle P, V \rangle$ be an interactive proof system for some language \mathcal{L} . We say that $\langle P, V \rangle$ is computational zero-knowledge with respect to an auxiliary input if for every PPT interactive machine V^* there exists a PPT algorithm S , running in time polynomial in the length of its first input, such that $\{\langle P(x, w), V^*(x, z) \rangle\}_{x \in \mathcal{L}, w \in \mathcal{R}_x, z \in \{0, 1\}^*} \approx_c \{\langle S(x, z) \rangle\}_{x \in \mathcal{L}, z \in \{0, 1\}^*}$

2.4 Commitment schemes

Commitments: A non-interactive commitment scheme consists of a pair of probabilistic polynomial time algorithms $(Setup, Com)$. The setup algorithm $pp \leftarrow Setup(1^\lambda)$ generates public parameters pp for the scheme, for security parameter λ . The commitment algorithm Com_{pp} defines a function $M_{pp} \times R_{pp} \rightarrow C_{pp}$ for message space M_{pp} , randomness space R_{pp} and commitment space C_{pp} determined by pp . For a message $x \in M_{pp}$, the algorithm draws $\delta \in_R R_{pp}$ uniformly at random, and computes commitment $\mathbf{com} = Com_{pp}(x; \delta)$.

For ease of notation we write $Com = Com_{pp}$.

[VD: All algorithm names in `\mathsf` (macro for each). Eg. in the above paragraph, `Setup`, `Com`, ...]

Homomorphic Commitment: A homomorphic commitment scheme is a non-interactive commitment scheme such that M_{pp}, R_{pp} and C_{pp} are all abelian groups, and for all $x_1, x_2 \in M_{pp}, \delta_1, \delta_2 \in R_{pp}$, we have $Com(x_1; \delta_1) + Com(x_2; \delta_2) = Com(x_1 + x_2; \delta_1 + \delta_2)$

[VD: Hiding and binding are the core properties of a commitment scheme, i.e., a definition of a commitment scheme includes the properties of hiding and binding. So bring them first. And just mention “Hiding” and “Binding”.]

Hiding Commitment: A commitment scheme is said to be hiding if for all PPT adversaries \mathcal{A} there exists a negligible function $\mu(\lambda)$ such that

$$|Pr[b = b' | pp \leftarrow Setup(1^\lambda); (x_0, x_1) \in M_{pp}^2 \leftarrow \mathcal{A}(pp), b \in_R \{0, 1\}, \delta \in_R R_{pp}, \mathbf{com} = Com(x_b; \delta), b' \leftarrow \mathcal{A}(pp, \mathbf{com})] - \frac{1}{2}| \leq \mu(\lambda)$$

Binding Commitment: A commitment scheme is said to be binding if for all PPT adversaries \mathcal{A} there exists a negligible function μ such that

$$Pr[Com(x_0; \delta_0) = Com(x_1; \delta_1) \wedge x_0 \neq x_1 | pp \leftarrow Setup(1^\lambda), x_0, x_1, \delta_0, \delta_1 \leftarrow \mathcal{A}(pp)] \leq \mu(\lambda)$$

[VD: Have a subsection* with Pedersen commitment, and have the vector commitment also in the same part.]

Pedersen Commitment: $M_{pp}, R_{pp} = \mathbb{Z}_p, C_{pp} = \mathbb{G}$ of order p .

$Setup : g, h \in_R \mathbb{G}$

$Com(x, \delta) = (g^x h^\delta)$

Pedersen Vector Commitment: $M_{pp} = \mathbb{Z}_p^n, R_{pp} = \mathbb{Z}_p, C_{pp} = \mathbb{G}$ with \mathbb{G} of order p .

$Setup : \mathbf{g} = (g_1, \dots, g_n), h \in_R \mathbb{G}$

$Com(\mathbf{x} = (x_1, \dots, x_n); \delta) = h^r \mathbf{g}^{\mathbf{x}} = h^r \prod_i g_i^{x_i} \in \mathbb{G}$

3 Distributed Prover Zero Knowledge

3.1 Definition

Discussion Discussion on the definition.

3.2 Construction step 1: The introduction of homomorphic commitments

– some technical description of the techniques, and how “commitment oracle” helps in realizing DPZK

Note If we did not use homomorphic commitment we get $+poly(\text{secp}).N$ protocol.

4 DPZK with reduced proof size

An brief recall on how our paradigm enables any improvement in single prover ZK protocol directly translate to the DP version.

4.1 Construction step 2: Skewing the witness matrix

ZK with $O(n^{1/c})$ proof size and $O(n^{1-1/c})$ pub key operations for verifier. — Using skewed matrix and inner product arguments.

5 DPZKQuickVerify

$O(n^{1/c})$ proof with efficient verifier.

5.1 Non-interactive

IOP to NIROP

6 Instantiations

(For $c=3,4$)

- Instantiate $c=3,4$ with square-root inner product argument.
- Verifier even more efficient than (4).
- Low round complexity

7 Implementation and Evaluation

Prior content from below

8 Construction

Encoding: Let, $x \in \mathbb{F}^{pml}$ be the secret. We will encode x to $U \in \mathbb{F}^{pmn}$ in the following way.
Let

Construct polynomials $p_{ij}(\cdot)$ of degree $< s$ such that $p_{ij}(\zeta_k) = x_{ijk} \quad \forall i \in [p], j \in [m], k \in [l]$.

Define: U

$$U[i] = \begin{bmatrix} p_{i1}(\eta_1) & p_{i1}(\eta_2) & \cdots & p_{i1}(\eta_n) \\ p_{i2}(\eta_1) & p_{i2}(\eta_2) & \cdots & p_{i2}(\eta_n) \\ \vdots & & & \\ p_{im}(\eta_1) & p_{im}(\eta_2) & \cdots & p_{im}(\eta_n) \end{bmatrix}$$

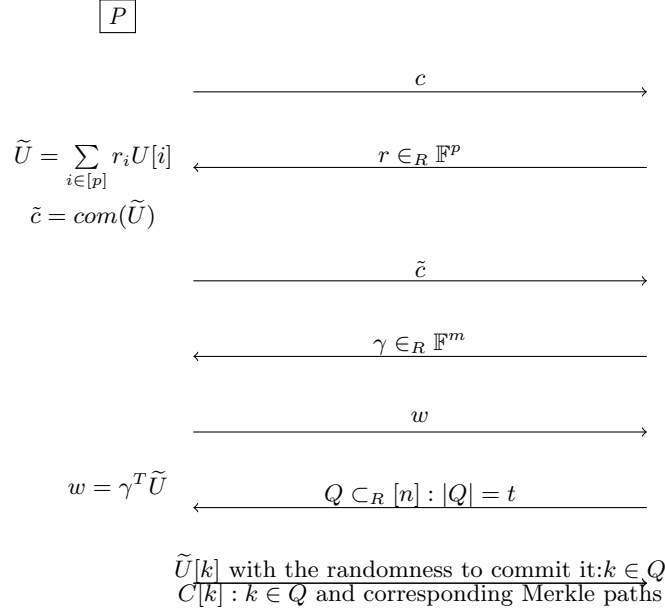
and $U = [U[1], U[2], \dots, U[p]]$.

So, U is a box with p slices and each slice has m rows and n columns.

Commitment: Let com be an homomorphic commitment scheme which commits a vector. Define:

$$com(U) = [c_1, c_2, \dots, c_p]^T = \begin{bmatrix} c[1, 1] & c[1, 2] & \cdots & c[1, n] \\ c[2, 1] & c[2, 2] & \cdots & c[2, n] \\ \vdots & & & \\ c[p, 1] & c[p, 2] & \cdots & c[p, n] \end{bmatrix} = C$$

where $c[i, k] = com([p_{i1}(\eta_k), p_{i2}(\eta_k), \dots, p_{im}(\eta_k)]^T)$ and let c is the Merkle tree root of C where leaves are entries of C .

**Fig. 1.** Protocol for Testing Interleaved

Protocol for Testing Interleaved: P and V does the following:

P and V follows the protocol in Figure 1 and then V checks the following:

- (a) Validation of $C[k]$ with respect to c .
- (b) $\tilde{c}_k = \sum_{i \in [p]} r_i c_{ik} \forall k \in Q$
- (c) $w \in L$, L is the set of codewords.
- (d) $\sum_{j \in [m]} \gamma_j \tilde{U}[j, k] = w_k \forall k \in Q'$
- (e) $\text{open}(\tilde{c}_k) = \tilde{U}[k] \forall k \in Q'$

Completeness: It is easy to see that if P has correct witness, for any choice of r, Q, γ, Q' of V , P can response for which V accepts.

Soundness: The following lemma ensures the soundness:

Lemma 1. Suppose $d(U^*, L^{mp}) > e$, where e is some positive integer such that $e < \frac{d}{3}$ ([what is the bound of e](#)), U^* is not a correct encoding then any adversarial prover strategy succeeds with probability at most $(1 - \frac{e}{2n})^\kappa + \frac{d}{|\mathbb{F}|} + \text{neg}(\kappa)$.

Proof. Let $\bar{U} = \sum_{i \in [p]} r_i U^*[i]$.

Then with probability $\geq 1 - \frac{d}{|\mathbb{F}|}$, \bar{U} satisfies $d(\bar{U}, L^m) > e$.

Let \bar{c} be the commitment for \bar{U} , that implies $\bar{c} = r^T \bar{C}$, by the homomorphic property of the commitment scheme, where \bar{C} is the commitment of \bar{U} .

Define: Let c, c' be two vectors, the distance between these two vectors is denoted by $d(c, c')$ and defined by the number of positions where c and c' differs.

case 1: $d(\bar{c}, \tilde{c}) \geq \frac{e}{2}$ where $\tilde{c} = r^T C$, where C is the commitment of U , nearest element of U^* in L^{mp} .

Prover's success probability $\leq \frac{\binom{n-e/2}{t}}{\binom{n}{t}} \approx (1 - \frac{e}{2n})^t \approx (1 - \frac{e}{2n})^k$ since $t = O(k)$

case 2: $d(\bar{c}, \tilde{c}) < \frac{e}{2}$.

Let, $\bar{\Delta} = \Delta(\bar{U}, L^m)$, positions where \bar{U} is different from the nearest correct code slice.

and let $\partial = \Delta(\bar{c}, \tilde{c})$

We have, $\bar{\Delta} > e$ and $\partial < \frac{e}{2}$, $\Rightarrow |\bar{\Delta} \setminus \partial| \geq \frac{e}{2}$.

Therefore, for $j \in \bar{\Delta} \setminus \partial$, $\bar{c}_j = \tilde{c}_j \Rightarrow \bar{U}[j] = \tilde{U}[j]$

Therefore probability of prover's success in the check (d) is $(1 - \frac{e}{2n})^t \approx (1 - \frac{e}{2n})^k$ since $t = O(k)$

So the soundness error is $(1 - \frac{e}{2n})^\kappa + \frac{d}{|\mathbb{F}|} + \text{neg}(\kappa)$.

Communication Complexity:

- Proof Size: constant size Merkle root, commitment vector with n components, with each component is of constant size, say λ , together $(n + 1)\lambda$, t many $C[j]$ and Merkle paths, size is $t(p\lambda + \log n)$, n sized vector w , t many $\tilde{U}[j]$ and randomness of total size $t(n + \alpha)$, where size of the randomness is α .
Therefore size of the proof is $\lambda(n + 1) + t(p\lambda + \log n) + n + t(n + \alpha) = O(\sqrt[3]{|C|})$
- Verifier's Complexity: $O(tm(M + E))$, where M is the cost of multiplication and E is the complexity of exponentiation. So, in this construction $O(\sqrt[3]{|C|})$ many cryptographic(elliptic curve) operations are required.
- Prover's complexity: To construct commitment matrix $|C|$ may exponentiation, to construct \tilde{U} , $|C|$ many multiplication, and to construct w , mn many multiplication.
So total complexity of the Prover is $mnM + |C|(M + E) = O(|C|(M + E))$

Protocol for checking Linear Constraint: x such that $Ax = b$

P and V does the following:

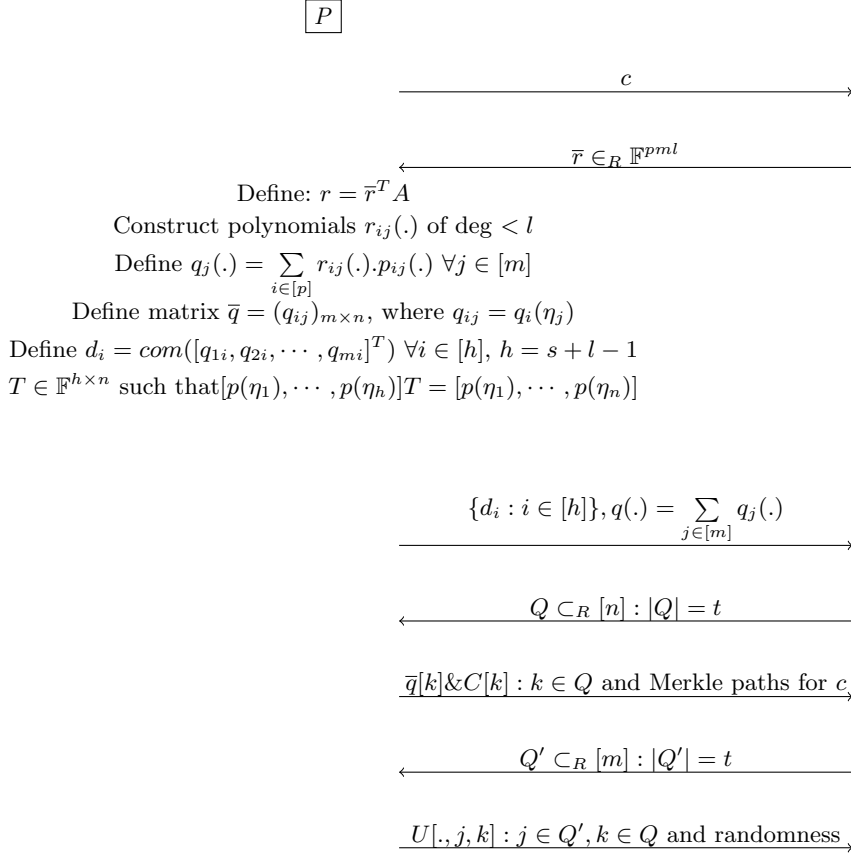
V checks that:

- (a) Validation of $C[k]$ with respect to c .
- (b) $\sum_{k \in [l]} q(\zeta_k) = \bar{r}^T b$
- (c) Check $q(\cdot)$ using $d_1, \dots, d_h: <1, \bar{q}[j']> = q(\eta_{j'}) \forall j' \in [h]$ as the inner product of the commitments should match with the commitment on the value $q(\eta_{j'})$. Using the idea of bullet proofs. Note that Verifier does not have $\bar{q}[j']$ for all $j' \in [h]$ but still this check is possible using the commitments d_1, \dots, d_h .
- (d) Reveal($\sum_{j' \in [h]} T_{j'k} d_{j'} = \bar{q}[k] \forall k \in Q$)
- (e) Check $U[., j, k]$ with respect to $C[k] \forall k \in Q, j \in Q'$: $<e_j, U[i, ., k]> = U[i, j, k]$
- (f) $\sum_{i \in [p]} r_{ij}(\eta_k) U[i, j, k] = \bar{q}[k]_j \forall k \in Q$ and $j \in Q'$

Completeness: If the prover encodes the correct x which satisfies $Ax = b$, then all the above checks will be passed, which ensures the completeness property.

Soundness: The following lemma ensures the soundness:

Lemma 2. *Let e be a positive integer such that $e < \frac{d}{3}$. Suppose that a malformed U^* is e -close to a codeword $U \in L^{mp}$ encoding $x \in \mathbb{F}^{pml}$ such that $Ax = b$. Then, for any malicious P strategy, U^* is rejected by V except with at most $((e + k + l)/n)^\kappa + 1/|\mathbb{F}| + \text{neg}(\kappa)$ probability.*

**Fig. 2.** Protocol for checking Linear Constraint

Proof. Since we assume that $Ax \neq b$, therefore $Pr_r[r^T Ax = r^T b]$ is at most $\frac{1}{|\mathbb{F}|}$.

Otherwise, P must have sent a wrong q' , instead of q . Since, degree of q' and q can be at most $k + l - 2$, as q' is fixed after fixing the matrix \bar{q} , which is fixed and ensured to the verifier by providing d_1, \dots, d_h . q and q' could be same in at most $k + l - 2$ many indices of η . Let, \bar{Q} is the set of indices where q' and q agree. and E be the set of indices where U and U^* are different. Therefore, in check (f), prover fails if $k \in Q$ such that $k \notin \bar{Q} \cup E$. Therefore

P can cheat with probability at most $\frac{\binom{e+k+l-2}{t}}{\binom{n}{t}} \approx \left(\frac{e+k+l}{n}\right)^t \approx \left(\frac{e+k+l}{n}\right)^\kappa$.

Therefore soundness error is $\left(\frac{e+k+l}{n}\right)^\kappa + \frac{1}{|\mathbb{F}|} + \text{neg}(\kappa)$, ($\text{neg}(\kappa)$ is due to the soundness probability of the commitment scheme).

Zero Knowledge:

Communication Complexity:

- Proof Size: First P sends Merkle root, which is of constant size, say λ , then sends $(k + l - 1)$ many commitments of constant size and $(k + l - 1)$ many coefficients of q , therefore, $(\lambda + 1) \times (k + l - 1)$. $t \times m$ to send t columns of \bar{q} and $t \times p\lambda$ for t columns of C , and for Merkle paths $t \times \log(pn)$. Finally t^2 many vectors from U including the randomness to commit P needs to send $t^2(p + \alpha)$. So, total size of the proof is $\sqrt[3]{|C|}$.
- Verifier's Complexity: l many polynomial evaluation of degree at most $(s + l - 1)$, for that number of multiplication is $O(l(s + l - 1))$,
 Checking commitments by IP using Bulletproofs, $(s + l - 1)\sqrt{m}$ many exponentiations.
 $t(s + l - 1)$ many multiplications.
 Checking commitments by IP using Bulletproofs, $t\sqrt{p}$ many exponentiations.

and finally tp many multiplications.

In total: $l(s+l-1) + t(s+l-1) + tp$ multiplications and $(s+l-1)\sqrt{m} + t\sqrt{p}$ many exponentiations

– Prover's Complexity:

Protocol for checking Quadratic Constraint: x, y, z suc that $x \odot y + a \odot z = b$

P and V does the following:

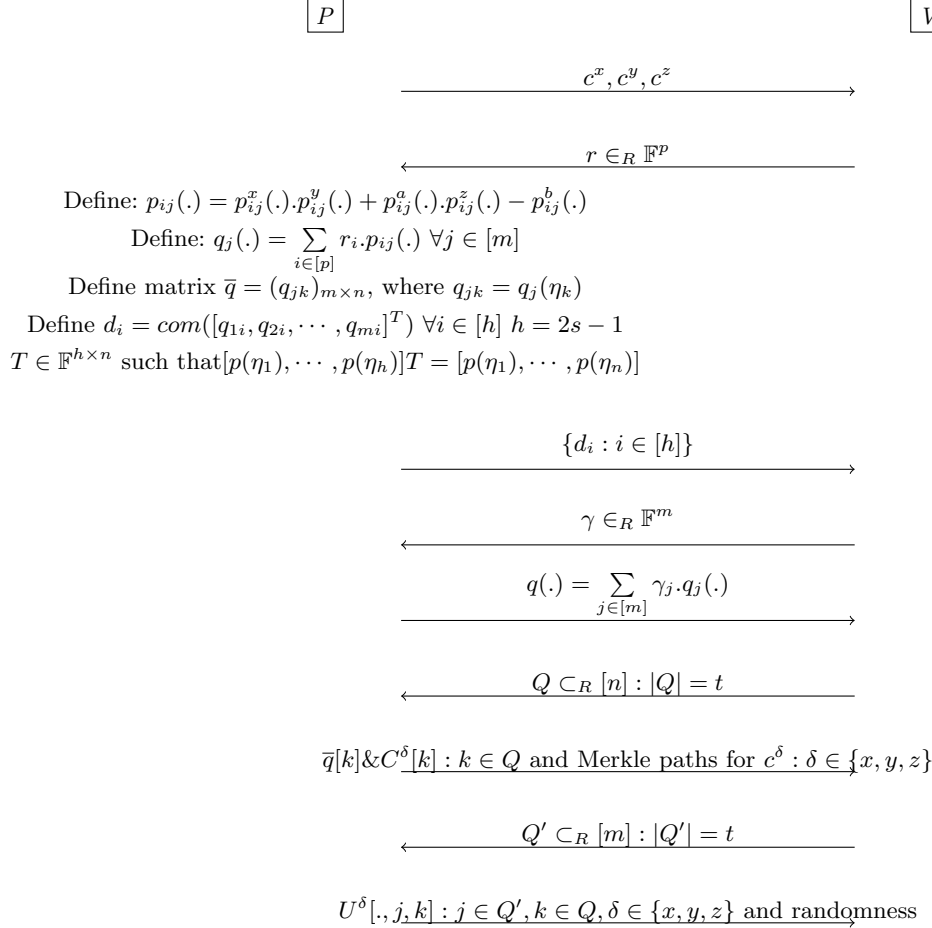


Fig. 3. Protocol for checking Quadratic constraint

V checks that:

- Validation of $C^\delta[k]$ with respect to c^δ , where $\delta \in \{x, y, z\}$.
- $\forall c \in [l], q(\zeta_c) = 0$
- Check $q(\cdot)$ using d_1, \dots, d_h : $\langle \gamma, \bar{q}[j'] \rangle = q(\eta_{j'}) \forall j' \in [h]$ as the inner product of the commitments should match with the commitment on the value $q(\eta_{j'})$. Using the idea of bullet proofs. Note that Verifier does not have $\bar{q}[j']$ for all $j' \in [h]$ but still this check is possible using the commitments d_1, \dots, d_h .
- Reveal($\sum_{j' \in [h]} T_{j'k} d_{j'} = \bar{q}[k] \forall k \in Q$)
- Check $U^\delta[., j, k]$ with respect to $C^\delta[k] \quad \forall k \in Q, j \in Q'$: $\langle e_j, U^\delta[i, ., k] \rangle = U^\delta[i, j, k]$, where $\delta \in \{x, y, z\}$.
- $\sum_{i \in [p]} r_i [U^x[i, j, k] \cdot U^y[i, j, k] + U^a[i, j, k] \cdot U^z[i, j, k] - U^b[i, j, k]] = \bar{q}[k]_j \quad \forall k \in Q \text{ and } j \in Q'$

Completeness: If the prover encodes the correct x, y, z which satisfy $x \odot y + a \odot z = b$, then all the above checks will be passed, which ensures the completeness property.

Soundness: The following lemma ensures the soundness:

Lemma 3.

Zero Knowledge:

Communication Complexity:

9 Multi-Prover Setting

Let, P_1, P_2, \dots, P_N provers are there. Let w be the extended witness which is additively distributed and w_ν is the share of the witness of the ν th party $\Rightarrow \sum_{\nu \in [N]} w_\nu = w$

P_ν encodes w_ν in the following way:

Let $w_\nu \in \mathbb{F}^{pml}$, then we can write

$$w_\nu = \begin{bmatrix} w_\nu[111] & w_\nu[112] & \cdots & w_\nu[11l] \\ w_\nu[121] & w_\nu[122] & \cdots & w_\nu[12l] \\ \vdots & \vdots & \ddots & \vdots \\ w_\nu[1m1] & w_\nu[1m2] & \cdots & w_\nu[1ml] \\ \vdots & \vdots & \ddots & \vdots \\ w_\nu[pm1] & w_\nu[pm2] & \cdots & w_\nu[pm l] \end{bmatrix}$$

Construct ' pm ' many polynomials of degree $< s$ such that $p_{ij}(\zeta_c) = w_\nu[i, j, c] \forall i \in [p] j \in [m] c \in [l]$

Define:

$$U^{w_\nu}[i] = \begin{bmatrix} p_{i1}^{w_\nu}(\eta_1) & \cdots & p_{i1}^{w_\nu}(\eta_n) \\ p_{i2}^{w_\nu}(\eta_1) & \cdots & p_{i2}^{w_\nu}(\eta_n) \\ \vdots & \ddots & \vdots \\ p_{im}^{w_\nu}(\eta_1) & \cdots & p_{im}^{w_\nu}(\eta_n) \end{bmatrix}$$

Define:

$$U^{w_\nu} = [U^{w_\nu}[1] \cdots U^{w_\nu}[p]]$$

Let $U = \sum_{\nu \in [N]} U^{w_\nu}$.

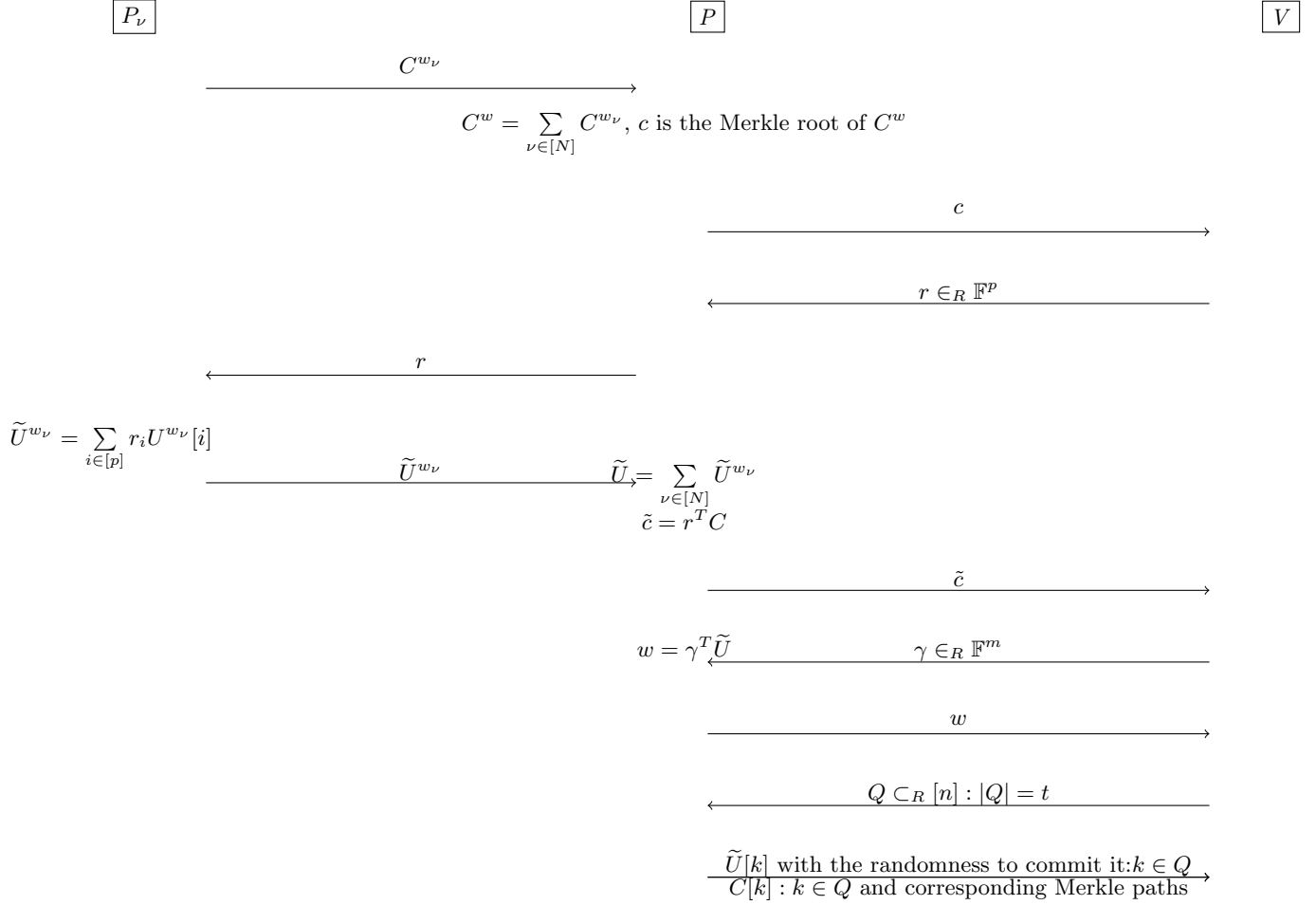
Note that U decodes to w . So let's call this U^w

Let C^{w_ν}, C^w be the commitment of U^{w_ν}, U^w respectively as mentioned in section 1. Therefore by the homomorphic property of the commitment scheme $C^w = \sum_{\nu \in [N]} C^{w_\nu}$.

Protocol for Testing Interleaved: $P \in \{P_1, \dots, P_N\}$ is arbitrarily chosen.

V checks that:

- (a) Validation of $C[k]$ with respect to the Merkle root c .
- (b) $\tilde{c}_k = \sum_{i \in [p]} r_i C_{ik} \forall k \in Q$
- (c) $w \in L$, L is the set of codewords of size \mathbb{F}^n
- (d) $\sum_{j \in [m]} \gamma_j \tilde{U}_{jk} = w_k \forall k \in Q$
- (e) $Open(\tilde{c}_k) = \tilde{U}[k] \forall k \in Q$

**Fig. 4.** Protocol for Testing Interleaved

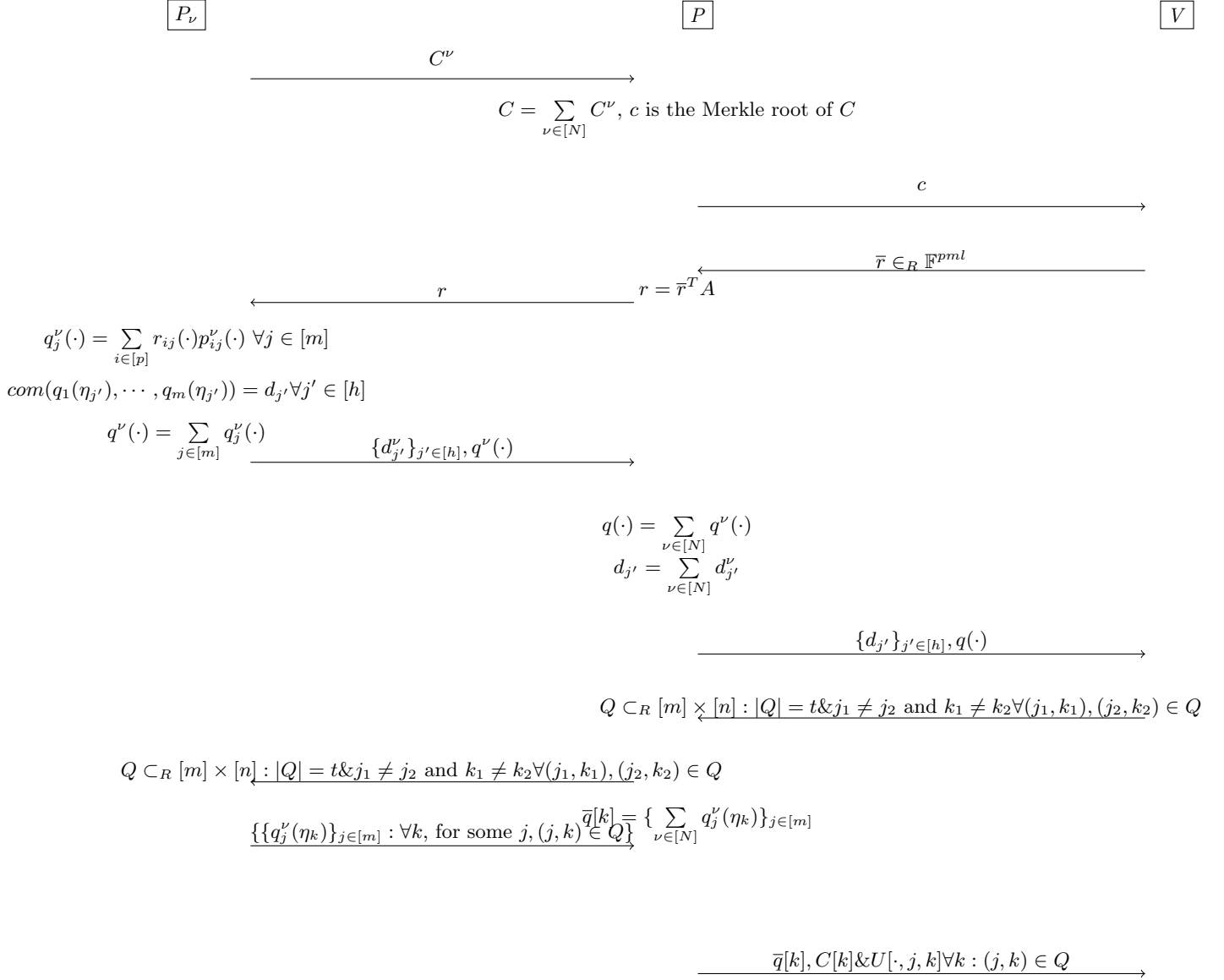
Protocol for Linear constraint: Let $Ax = b$, where $A \in \mathbb{F}^{pml \times pml}$ and $b \in \mathbb{F}^{pml}$ are publicly known and x is the secret which is additively distributed among the provers, say x_ν is the share of the ν th prover.

P_ν encodes x_ν to U^ν and C^ν is the commitment of U^ν .

$P \in \{P_1, \dots, P_N\}$ is arbitrarily chosen.

V checks that:

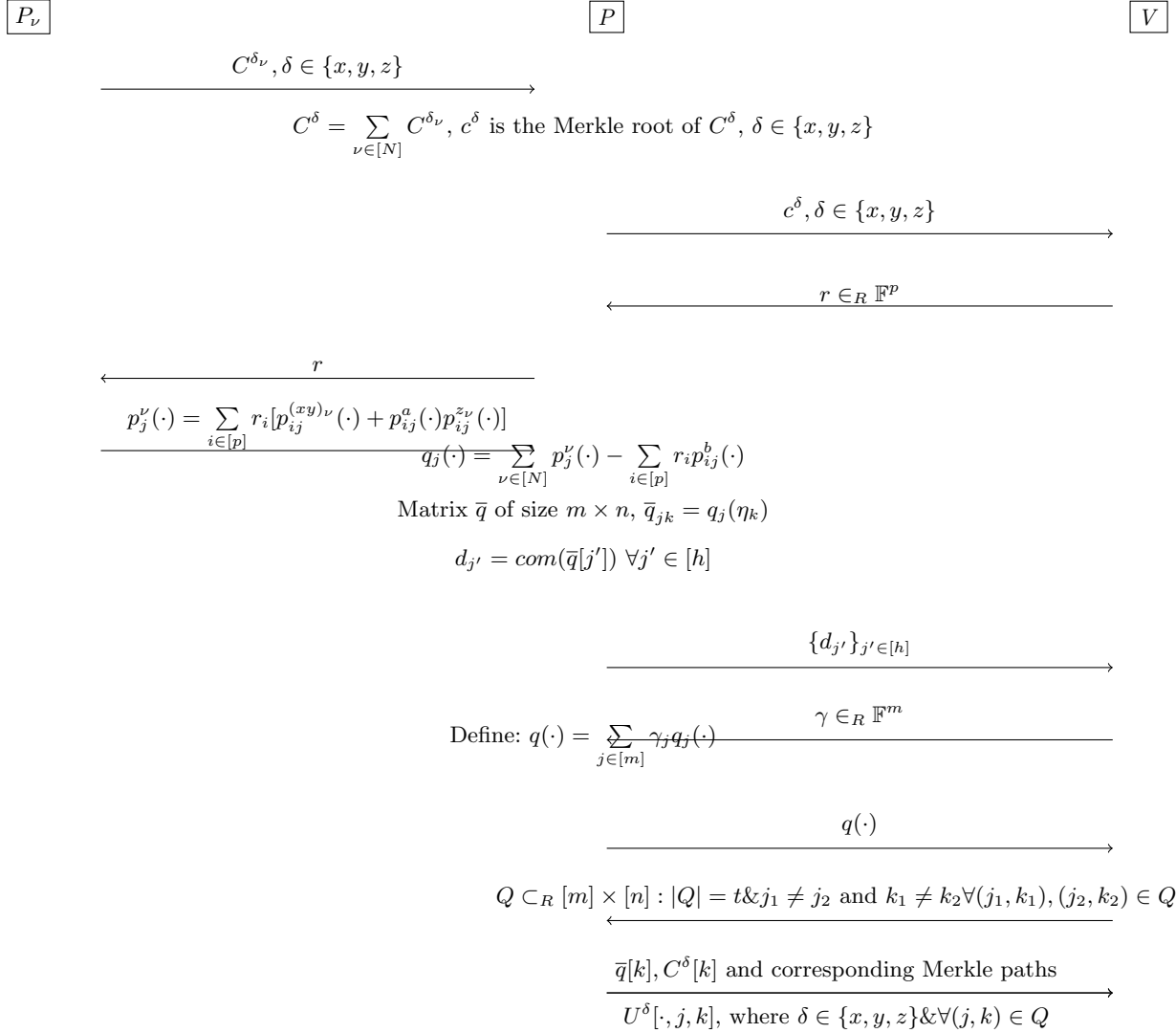
- (a) Validation of $C[k]$ with respect to the Merkle root c .
- (b) $\sum_{c \in [l]} q(\zeta_c) = \bar{r}^T b$.
- (c) Check $q(\cdot)$ using d_1, \dots, d_h by InnerProduct argument using Bullet Proofs: $\langle 1, \bar{q}[j'] \rangle = q(\eta_{j'}) \forall j' \in [h]$ where, commitment of $\bar{q}[j']$ is $d_{j'}$.
- (d) Reveal($\sum_{j' \in [h]} T_{j'k} d_{j'}$) = $q(\eta_k) \forall k \in [n]$, where T is a public matrix of dimension $n \times h$ such that $T([p(\eta_1), \dots, p(\eta_h)]^T) = ([p(\eta_1), \dots, p(\eta_h)]^T)$ for all polynomial of degree $< h$.
- (e) Check $U[\cdot, j, k]$ with respect to $C[k] \forall (j, k) \in Q$ by InnerProduct argument using Bullet Proofs: $\langle e_j, U[i, \cdot, k] \rangle = U[i, j, k]$.
- (f) $\sum_{i \in [p]} r_{ij}(\eta_k) U[i, j, k] = \bar{q}[k]_j \forall (j, k) \in Q$.

**Fig. 5.** Protocol for Linear Constraint

Protocol for quadratic constraint: Let $x \odot y + a \odot z = b$, where a, b are public and x, y, z are secrets. x_ν, y_ν, z_ν are the shares of P_ν . P_ν encodes x_ν, y_ν, z_ν to $U^{x_\nu}, U^{y_\nu}, U^{z_\nu}$ respectively and computes the corresponding commitments i.e. $com(U^{x_\nu}) = C^{x_\nu}, com(U^{y_\nu}) = C^{y_\nu}, com(U^{z_\nu}) = C^{z_\nu}$.

P_ν constructs ‘ pm ’ many polynomials $p_{ij}^{(xy)\nu}(\cdot)$ such that $p_{ij}^{(xy)\nu}(\cdot) = p_{ij}^{x_\nu}(\cdot) p_{ij}^{y_\nu}(\cdot)$. To do that use FFT and choose $\{\eta_1, \eta_2, \dots, \eta_n\}$ accordingly, in particular, n th roots of unity and set $n \geq 2s - 1$.

$P \in \{P_1, \dots, P_N\}$ is arbitrarily chosen.

**Fig. 6.** Protocol for Quadratic Constraint

V checks that:

- Validation of $C^\delta[k]$ with respect to c^δ , $\delta \in \{x, y, z\}$.
- $q(\zeta_c) = 0 \forall c \in [l]$.
- Check using d_1, \dots, d_h using Inner Product argument by Bullet Proofs: $\langle \gamma, \bar{q}[j'] \rangle = q(\eta_{j'}) \forall j' \in [h]$.
- Reveal($\sum_{j' \in [h]} T_{j'k} d_{j'}$) = $q(\eta_k) \forall k \in [n]$, where T is a public matrix of dimension $n \times h$ such that $T([p(\eta_1), \dots, p(\eta_h)]^T) = ([p(\eta_1), \dots, p(\eta_h)]^T)$ for all polynomial of degree $< h$.
- Check $U^\delta[\cdot, j, k]$ with respect to $C^\delta[k] \forall (j, k) \in Q$ by Inner Product argument using Bullet Proofs: $\langle e_j, U^\delta[i, \cdot, k] \rangle = U^\delta[i, j, k]$.
- $\sum_{i \in [p]} r_i [U^x[i, j, k] \cdot U^y[i, j, k] + U^a[i, j, k] \cdot U^z[i, j, k] - U^b[i, j, k]] = \bar{q}[k]_j \forall (j, k) \in Q$.

10 Proof of size $|C|^{\frac{1}{\alpha}}$

Here consider our extended witness $w \in \mathbb{F}^{pm_1m_2l}$. Encode it to U^w in the same way as above, where size of U is $p \times m_1m_2 \times n$. Let, $m = m_1m_2$

Protocol for Testing Interleaved: P and V does the following:

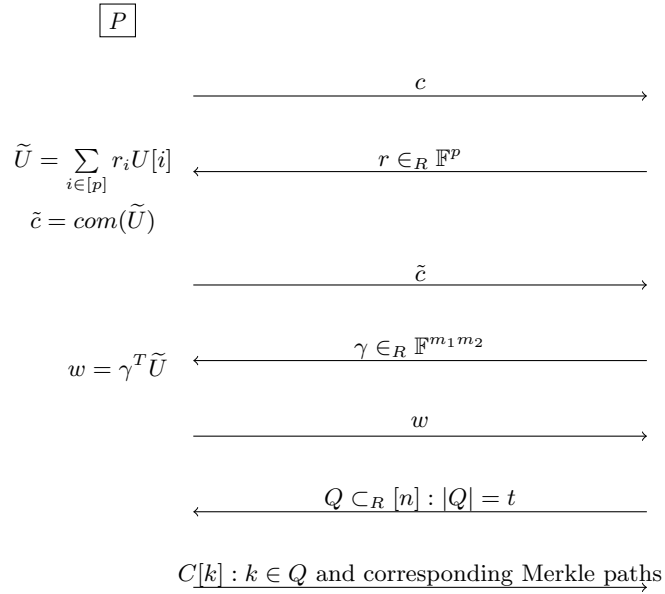


Fig. 7. Protocol for Testing Interleaved

P and V follows the protocol in Figure 1 and then V checks the following:

- Validation of $C[k]$ with respect to c .
- $\tilde{c}_k = \sum_{i \in [p]} r_i c_{ik} \ \forall k \in Q$
- $w \in L$, L is the set of codewords.
- $\sum_{j \in [m]} \gamma_j \tilde{U}[j, k] = w_k \ \forall k \in Q'$ Checking \tilde{U} with respect to its commitment and γ using inner product argument
i.e. $\langle \gamma, \tilde{U}[k] \rangle = w_k \ \forall k \in [n]$

Proof Size:

- constant size Merkle root
- n sized vector \tilde{c}
- n sized vector w
- t many p sized vector $C[k] : k \in Q$
- proof for inner product argument $O(\log(m))$

So total size of the proof is $O(|C|^{\frac{1}{4}})$.

Verifier's Complexity:

- Checking Merkle root
- p multiplications: pM

- Multiplication by the Parity check matrix: n^2M
- Inner Product check : $m.E$

So total $mE + pM + n^2M$

Prover's Complexity:

- Computing C , $|C|$ many exponentiation: $|C|.E$
- Computing Merkle root
- To compute \tilde{U} , $|C|.M$ and to compute \tilde{c} , $p.n.M$
- To compute w , $m.n.M$

So total $|C|.E + |C|.M + p.n.M + m.n.M + h$, where h is the complexit to compute the Merkle root.

Protocol for checking Linear Constraint: x such that $Ax = b$

P and V does the following:

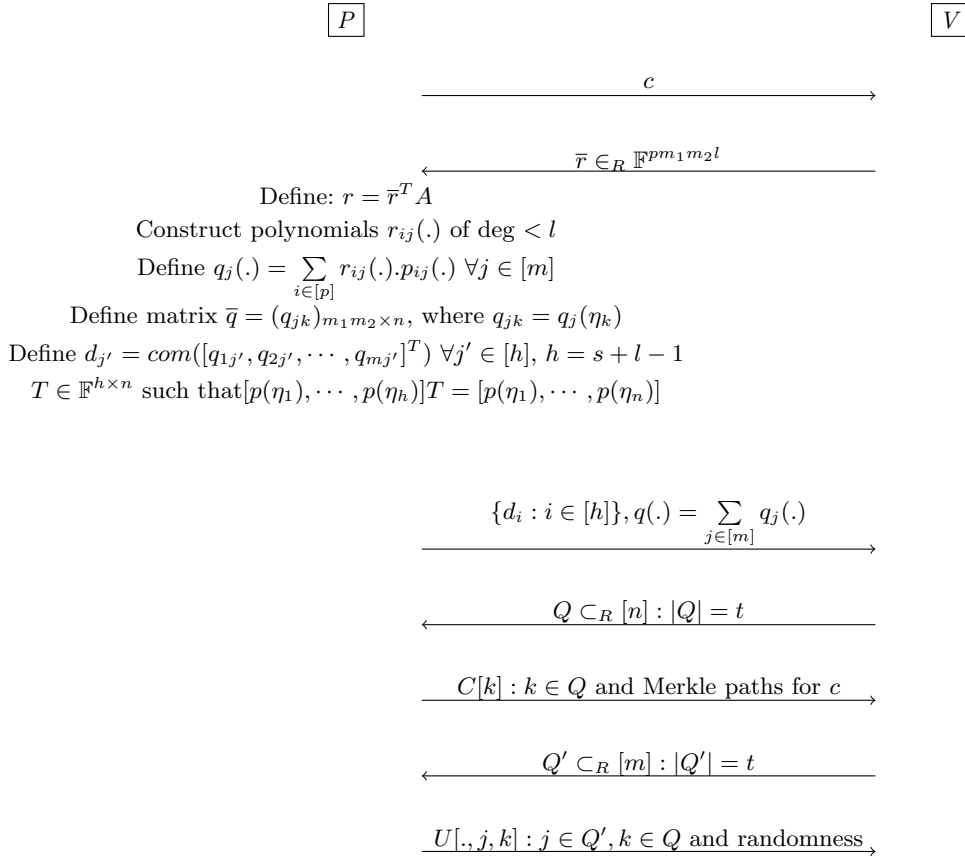


Fig. 8. Protocol for checking Linear Constraint

V checks that:

- (a) Validation of $C[k]$ with respect to c .

- (b) $\sum_{k \in [l]} q(\zeta_k) = \bar{r}^T b$
- (c) Check $q(\cdot)$ using d_1, \dots, d_h : $\langle 1, \bar{q}[j'] \rangle = q(\eta_{j'}) \forall j' \in [h]$ as the inner product of the commitments should match with the commitment on the value $q(\eta_{j'})$. Using the idea of bullet proofs. Note that Verifier does not have $\bar{q}[j']$ for all $j' \in [h]$ but still this check is possible using the commitments d_1, \dots, d_h .
- (d) Check $U[\cdot, j, k]$ with respect to $C[k] \forall k \in Q, j \in Q'$: $\langle e_j, U[\cdot, j, k] \rangle = U[i, j, k]$
- (e) V computes the value $\sum_{j' \in [h]} T_{j',k} d_{j'}$ which is the commitment of the vector $\bar{q}[k]$ and also computes $\sum_{i \in [p]} r_{ij}(\eta_k) U[i, j, k]$.
- Now use Inner Product argument i.e. $\langle e_j, \bar{q}[k] \rangle = \sum_{i \in [p]} r_{ij}(\eta_k) U[i, j, k] \forall j \in Q', k \in Q$.

Proof Size:

- Constant size Merkle root.
- h many constants for d_1, \dots, d_h and h coefficients for the polynomial, $O(h)$.
- t many $C[k]$ and corresponding Merkle paths, total size: $t.p + t \log(pn)$
- t many $U[\cdot, j, k]$ and randomness: $O(t.p)$.
- Proof for Inner Product argument $O(\log(m))$

In total $O(|C|^{\frac{1}{4}})$

Verifier's Complexity:

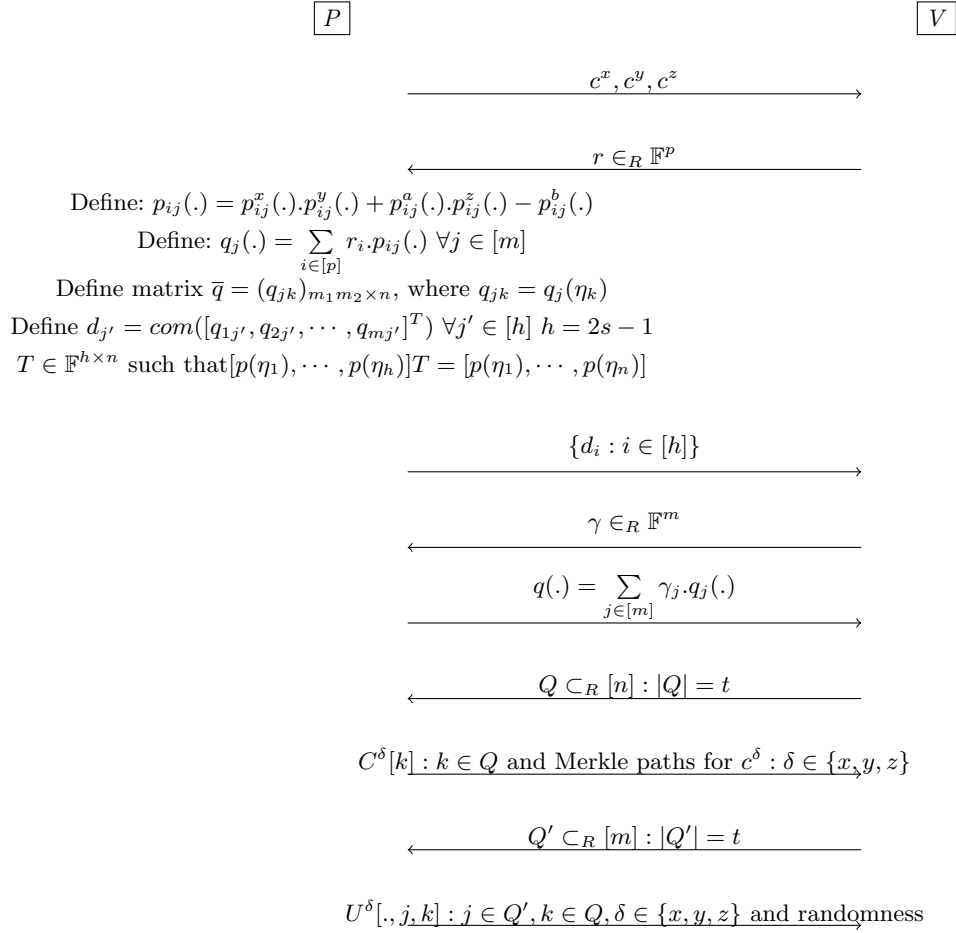
- Checking Merkle roots.
- l polynomial evaluations $(s + l - 1).l.M$
- Inner Product check by the verifier: $O(m.E)$
- $(s + l - 1).M + p.M + |C|.M + \log m.E$

So total $(s + l - 1).l.M + m.E + (s + l - 1).M + p.M + |C|.M + \log m.E$

Prover's Complexity: To compute C matrix, Prover needs to do $|C|$ many exponentiation and that is dominating term in his computation.

Protocol for checking Quadratic Constraint: x, y, z suc that $x \odot y + a \odot z = b$

P and V does the following:

**Fig. 9.** Protocol for checking Quadratic constraint

V checks that:

- Validation of $C^\delta[k]$ with respect to c^δ , where $\delta \in \{x, y, z\}$.
- $\forall k \in [l], q(\zeta_k) = 0$
- Check $q(\cdot)$ using d_1, \dots, d_h : $\langle \gamma, \bar{q}[j'] \rangle = q(\eta_{j'}) \forall j' \in [h]$ as the inner product of the commitments should match with the commitment on the value $q(\eta_{j'})$. Using the idea of bullet proofs. Note that Verifier does not have $\bar{q}[j']$ for all $j' \in [h]$ but still this check is possible using the commitments d_1, \dots, d_h .
- Check $U^\delta[., j, k]$ with respect to $C^\delta[k] \quad \forall k \in Q, j \in Q'$: $\langle e_j, U^\delta[i, ., k] \rangle = U^\delta[i, j, k]$, where $\delta \in \{x, y, z\}$.
- V computes the value $\sum_{j' \in [h]} T_{j'k} d_{j'}$, which is the commitment of the vector $\bar{q}[k]$ and also computes $\sum_{i \in [p]} r_i [U^x[i, j, k] \cdot U^y[i, j, k] + U^a[i, j, k] \cdot U^z[i, j, k] - U^b[i, j, k]] = R[i, j, k]$. Now use Inner Product argument i.e. $\langle e_j, \bar{q}[k] \rangle = R[i, j, k] \quad \forall j \in Q', k \in Q$.

Proof Size:

- Constant size Merkle root c .
- d_1, \dots, d_h : $O(h)$.
- To send the polynomial $q(\cdot)$, $2s - 1$ many coefficients are needed to be send.
- t many $C[k]$, $t \cdot p$

- t many $U[\cdot, j, k]$, $t.p$
- Proof for Inner product argument: $\log m$

In total $O(h + 2s - 1 + t.p + \log(m)) = O(|C|^{\frac{1}{4}})$

Verifier's Complexity:

- Checking Merkle roots.
- l polynomial evaluations: $(2s - 1).l.M$
- Checking using Inner Product arguments $O(m.E)$
- $(2s - 1).M + t.p.M$

So total complexity $O(|C|^{\frac{1}{2}}.E + |C|^{\frac{1}{2}}.M)$

Prover's Complexity: To compute C matrix, Prover needs to do $|C|$ many exponentiation and that is dominating term in his computation.

10.1 Zero-Knowledge:

We have three checks:

- Interleaved Testing
- Linear Check
- Quadratic Check

Note that during the interleaved testing, w is sent to the verifier, where w is the linear combination of all the rows of the encoding matrix, which verifier cannot compute on his own. So, it is required to blind the vector w by adding an additional vector which is a codeword.

For Linear check, verifier is receiving the polynomial $q(\cdot)$, and can evaluates in many points which he should not learn on his own, verifier should learn only $\sum_{c \in [l]} q(\zeta_c)$. To hide this, we will add a polynomial $q_{blind}(\cdot)$ such that $\sum_{c \in [l]} q_{blind}(\zeta_c) = 0$ and later $q_j(\eta_k)$ is opened to the verifier, hide this we need to add another polynomial to each $q_j(\cdot)$, say $q_{blind_j}(\cdot)$ such that $q_{blind_j}(\zeta_c) = 0 \forall c \in [l]$. To achieve this we will include one slice where each row but the $(m+1)th$ is encoding of zero vector. and in the $(m+1)th$ row is the encoding of a vector which sums to 0.

Similarly for quadratic also, we need to include one slice where each row is the encoding of zero vector.

10.2 Simulation based proof:

Let τ_1, τ_2, τ_3 be the transcripts of the interleaved check, linear check and quadratic check at the time of the execution of the protocol. where

$$\begin{aligned}\tau_1 &= \{r_1, \tilde{c}, \gamma_1, w, Q_1, C_{Q_1}, \tilde{U}_{Q_1}, \tilde{\delta}_{Q_1}, \tilde{v}_{Q_1}\} \\ \tau_2 &= \{r_2, d_{1[h]}, q_1(\cdot), Q_2, \bar{q}_{1Q_2}, C_{Q_2}, U_{Q_2}, \delta_{Q_2}, v_{Q_2}\} \\ \tau_3 &= \{r_3, d_{2[h]}, \gamma_2, q_2(\cdot), Q_2, \bar{q}_{2Q_2}, C_{Q_2}, U_{Q_2}, \delta_{Q_2}, v_{Q_2}\}\end{aligned}$$

Let \mathcal{S} be the simulator. Then \mathcal{S} randomly picks $r_1, r_2, r_3, \gamma_1, \gamma_2, Q = Q_1 \cup Q_2$, where size of Q is t such that Q_1 and Q_2 are disjoint. \mathcal{S} chooses a block \mathcal{B} corresponding to Q , i.e. \mathcal{S} chooses and fixes the complete matrix along the direction m and p , for the indices in Q . Once the block \mathcal{B} is fixed, for these block, U is fixed by the condition that, t slices along the direction m and p is fixed and l positions are fixed because of the encoding of the witness. So, using \mathcal{B} , \mathcal{S} generates $\tilde{c}, w, C_{Q_1}, \tilde{U}_{Q_1}, d_{1[h]}, d_{2[h]}, \bar{q}_{1Q_2}, \bar{q}_{2Q_2}, C_{Q_2}, U_{Q_2}$ and randomly picks $\tilde{\delta}_{Q_1}, \delta_{Q_2}, \tilde{v}_{Q_1}, v_{Q_2}$. Therefore the transcript generated by \mathcal{S} is indistinguishable from τ_1, τ_2, τ_3 .