Polynomial IOPs for Linear Algebra Relations

Alan Szepieniec
alan@nervos.org
Nervos Foundation

Yuncong Zhang
shjdzhangyuncong@sjtu.edu.cn
Shanghai Jiao Tong University

Abstract. This paper proposes new Polynomial IOPs for arithmetic circuits. They rely on the monomial coefficient basis to represent the matrices and vectors arising from the arithmetic constraint satisfaction system, and build on new protocols for establishing the correct computation of linear algebra relations such as matrix-vector products and Hadamard products. Our protocols give rise to concrete proof systems with succinct verification when compiled down with a cryptographic compiler whose role is abstracted away in this paper. Depending only on the compiler, the resulting SNARKs are either transparent or rely on a trusted setup.

Keywords: SNARK · Polynomial IOP · Zero-Knowledge · Succinct Verification

1 Introduction

Succinct Non-Interactive Arguments of Knowledge (SNARKs) enable a resource-constrained verifier to cryptographically verify the authentic computations of an untrusted prover. The technology is particularly well-suited to the cryptocurrency setting, where participants are typically anonymous, untrusted, and where the success of the network depends on the capability of lightweight nodes to verify the network's consensus (however that is defined). In this setting, there is a large monetary incentive for malicious behavior.

Despite the flurry of rapid related and unrelated developments by diverse parties, two trends are emerging as good practice in this domain.

1. *Functional separation in the compilation pipeline.* The compilation process for general purpose zero-knowledge proofs is separated into multiple steps with clear boundaries. At the input of this pipeline is a computation, represented either as program source code or as a circuit. A technique called arithmetization turns this computation into a constraint system involving native operations over a finite field. The next step transforms this constraint system into an abstract proof system between two parties, prover P and verifier V, that are interactive Turing machines with access to unrealistic or unrealizable resources such as PCP oracles. The abstract proof systems in this step typically achieve statistical or even perfect security. In the last step, the *cryptographic compilation*, the unrealistic resources are replaced by cryptographic approximations that achieve the same functionality at the expense of introducing computational hardness assumptions for security.

2. *Polynomial IOP formalism.* The abstract information-theoretical proof system in the step before cryptographic compilation could in principle rely on a variety of unrealistic resources, and build a sound proof system from their mathematical properties. However, for the purpose establishing soundness, the Schwartz-Zippel lemma is an indispensable tool. The strategy is to reduce the satisfaction of arithmetic constraints arising from the constraint system to series of identities of *low-degree polynomials*. By evaluating these polynomials in random points, their equality is tested probabilistically. If the left and right hand sides of an equation represent identical polynomials, they are identical everywhere, but if they are unequal they are different *almost* everywhere. The Schwartz-Zippel lemma provides an exact concrete quantification of the security lost due to this probabilistic approximation. A *Polynomial IOP* is the abstract proof system tailored to this strategy. In this formalism, the prover sends low degree polynomials to the verifier, and rather than reading the entire list of coefficients, the verifier queries these polynomials in a given point through an oracle interface. The cryptographic compiler uses a *polynomial commitment scheme* to simulate this unrealistic resource.

These trends are visible in the rise of universal SNARKs with universal and updatable structured reference strings (SRS's) such as Sonic [11], PLONK [8], and Marlin [7]. The common idea here is to use the cryptographic pairing-based mathematics only to realize *polynomial commitment scheme*, typically the KZG scheme [10]. Since the SRS is used only for the KZG scheme, it is independent of the preceding abstract proof system and the circuit it encodes; this independence is precisely what enables updates to the SRS and its adaptation to any circuit. PLONK and Marlin independently formalize this abstraction and introduce the terms *Polynomial Protocol* and *Algebraic Holographic Proof (AHP)*, respectively. This paper adopts the terminology of Bünz *et al.* [6], who introduce a new polynomial commitment scheme (and hence a cryptographic compiler) based on groups of unknown order and in the process explore the landscape of protocols it can apply to.

These trends are *also* visible in the rise of IOPs based on Reed-Solomon codes [1,4,3]. The underlying abstract protocols here are not explicitly Polynomial IOPs. However, their common feature is the reliance on Reed-Solomon codewords as the proof oracles. Since Reed-Solomon codewords are obtained by evaluating polynomials in a domain of points whose cardinality is larger than the polynomials' degree, these proof oracles uniquely identify the originating low-degree polynomials. As a result, a Reed-Solomon IOP is a Polynomial IOP in disguise.

Despite the spontaneous convergence onto Polynomial IOPs as a useful formalism, there seems to be little agreement about the optimal interface between Polynomial IOPs and the arithmetic constraint systems that they realize. Arithmetic constraint systems typically express constraints using matrix algebra: in terms of vectors, and matrix multiplication, but also *Hadamard products*, which is a fancy word for the element-wise products of pairs of equal-length vectors. The

set of operations that Polynomial IOPs natively offer are somewhat different. As a result, how the Polynomial IOP represents the objects in the arithmetic constraint system and how it simulates the equations that constrain them, are the key questions in the design process of Polynomial IOPs. The various answers to these questions are what set the various Polynomial IOPs for arithmetic circuits apart.

- Marlin and Aurora represent the objects of the arithmetic constraint system as the Reed-Solomon codewords of polynomials. Standard techniques establish the correct computation of a Hadamard product of such codewords. The computation of a linear transform applied to such a codeword is reduced to checking the sum of a related codeword.
- PLONK represents the vector of wire values as the values of a polynomial in a domain of points. A permutation argument establishes the assignment of wires to gates and the standard techniques for Reed-Solomon codewords establish the consistency of inputs and outputs to addition and multiplication gates.
- Sonic represents the vectors of left, right, and output wires of a series of multiplication gates as the coefficient vectors of three polynomials. The consistency of these multiplication gates, and of a linear transform, is established by checking several properties of bivariate polynomials. The paper furthermore explains under which conditions these bivariate polynomials can be simulated with univariate ones.

Contributions. In this paper we propose a collection of new Polynomial IOPs for arithmetic circuits called Claymore[1]. Succinct verification is achieved with an untrusted preprocessing phase. When compiled down using any polynomial commitment scheme, the result is a concrete zk-SNARK with universal updatable structured reference string, or transparent setup, depending only on the nature of the polynomial commitment scheme.

The arithmetic constraint system chosen to represent the arithmetic circuit is the Hadamard Product Relation (HPR), in which the witness consists of three vectors representing the left, right, and output wires of a list of multiplication gates. We note that Sonic realizes a similar constraint satisfaction relation by reducing both the multplication and linear constraints into one large equation. In Claymore, the multiplication gate consistency and linear consistency are achieved in two separate steps, both of which rely on a collection of subprotocols for linear algebra relations that we develop along the way. The separate steps are later merged as an explicit optimization.

While the concrete cryptographic compilation is abstracted away, it is possible to make arguments regarding the size of concrete proofs based on the communication complexity of the Polynomial IOP. In this respect, the dense variant of Claymore stands out as the number of polynomials transmitted in the online phase is only 4 – down 33.3% from the runner-up PLONK, whose number stands

[1] A type of Scottish sword.

at 6. As a result, if the number of polynomials in the transcript is the dominant factor of proof size, then Claymore will result in the smallest proofs.

There is a price to pay for this brevity: the degree of the largest-degree polynomial is much larger. For DenseClaymore this degree scales with roughly $O(n^2)$, where n is the size of the witness. Depending on the concrete cryptographic compiler, this behavior is either a minor inconvenience, or a complete blockade, for SNARKifying large enough circuits. Alternatives such as PLONK and Marlin achieve $O(n)$ scaling.

A question that arises when using the monomial coefficient basis, is whether this basis is equipped to deal with the sparse linear transformations that typically come from long-winded computations. We answer this question positively by providing methods for dealing with sparse linear algebra relations, culminating in a sparse variant of Claymore. This variant concretely outperforms Marlin in terms of the number of polynomials in the transcript. While this number is smaller still for PLONK, one notes that PLONK does not support arbitrary fan-in for linear constraints, whereas Marlin and Claymore (both variants) do.

Motivation and applications. The motivation for this work is chiefly theoretical. By studying the interface between arithmetic circuits and Polynomial IOPs in isolation of other constraints and demands, we develop a protocol that achieves its target functionality exactly. As a result of this focus, our protocol is arguably simpler than other protocols that achieve nominally the same thing. Complexity is the friend of mistakes, and our protocol may therefore be the preferred option for this reason even in circumstances where it is inferior in terms of performance. However, it is by no means clear that Claymore does perform worse in the general case, because this comparison is highly dependent on the parameters of the situation.

When used in combination with a cryptographic compiler whereby the number of polynomials in the transcript dominates the proof size, DenseClaymore yields in the smallest proofs. As a result, DenseClaymore should be the SNARK of choice in settings where the bandwidth is the most critical optimization target. Blockchains naturally satisfy this description when they have a fixed block rate and size.

Furthermore, the dense variant of Claymore performs extremely well for shallow arithmetic circuits, such as the verification circuits of lattice-based and MQ-based signature schemes, which typically involve operations on large matrices and vectors over a small finite field. As a result, a DenseClaymore-SNARK is an outstanding candidate for achieving post-quantum signature aggregation — or indeed, post-quantum signatures with various fancy properties that zero-knowledge proofs enable.

Using SNARKs in combination with other cryptographic tools points to a useful property that SNARKs frequently lack — they typically require a finite field with a particular structure, such as a large multiplicative subgroup of smooth order. Sonic, Marlin, and PLONK all have this property. Using the SNARK in combination with a different cryptosystem that requires an incompatible field, requires the SNARK to simulate the cryptosystem's field operations

using the arithmetic constraint system of the SNARK. In contrast, Claymore induces no such costly simulation overhead as it works for any finite field.

The protocols proposed here promote simplicity by adopting a modular approach. However, we observe that once the basic protocol has been composed, there are available optimizations that improve its characteristics at the cost of violating the boundaries between modules. This observation highlights the utility of separating *design* from *optimization* considerations. Note that it is only the optimized SparseClaymore protocol that outperforms Marlin in the target metric, number of polynomials. The unoptimized version is inferior in all respects. Furthermore, optimized Claymore admits a proof of zero-knowledge that is simpler and more straightforward than the equivalent for the unoptimized version. Lastly, the optimizations stand on their own, and can possibly improve other Polynomial IOPs beyond Claymore.

2 Preliminaries

2.1 Indexed Relations

Owing to their convenience, we use *indexed relations* [7]. An indexed relation is a set $\mathcal{R}$ of tuples $(\mathtt{i}, \mathtt{x}, \mathtt{w})$, whose three components are called the *index*, *instance*, and *witness*, respectively. The separation between index and instance captures the intuition that some properties of concrete proofs for $\mathcal{R}$ should be computable from $\mathtt{i}$ even before $\mathtt{x}$ is known. For instance, $\mathtt{i}$ can be the description of an arithmetic circuit, $\mathtt{x}$ the values of the output wires, and $\mathtt{w}$ an assignment of values to all wires that makes the all gates consistent. The projection $\{(\mathtt{i}, \mathtt{x}) \,|\, (\mathtt{i}, \mathtt{x}, \mathtt{w}) \in \mathcal{R}\}$ of triples in $\mathcal{R}$ onto the first two components is the *indexed language corresponding to* $\mathcal{R}$ and is denoted by $\mathcal{L}(\mathcal{R})$.

2.2 Constraint Systems

A constraint system is a representation of a computation in terms of equations with unknown variables. When there is an assignment to the unknown variables that satisfies all equations, we say the constraint system is *satisfiable*, and this assignment is the *witness*. The *index* determines all fixed constants in the equations, and the *instance* determines known variables that can vary independently of the index but are ultimately known by all parties involved.

The following constraint system is adapted from Bootle *et al.* [5].

Definition 1 (Hadamard Product Relation (HPR)). *Let $\mathbb{F}$ be a finite field. A triple $(\mathtt{i}, \mathtt{x}, \mathtt{w})$ where $\mathtt{i} = (m, n, M)$ with $m, n \in \mathbb{N}$, and $M \in \mathbb{F}^{m \times (1+3n)}$, where $\mathtt{x} = \mathbf{x} \in \mathbb{F}^m$, and where $\mathtt{w} = (\mathbf{w_l}, \mathbf{w_r}, \mathbf{w_o}) \in \mathbb{F}^n \times \mathbb{F}^n \times \mathbb{F}^n$; satisfies the* Hadamard Product Relation *iff both*

$$\mathbf{x} = M \begin{pmatrix} \frac{1}{\mathbf{w_l}} \\ \frac{\mathbf{w_r}}{\mathbf{w_o}} \end{pmatrix} \tag{1}$$

and

$$\mathbf{w_l} \circ \mathbf{w_r} = \mathbf{w_o} \ , \tag{2}$$

where $\circ$ *denotes the Hadamard (i.e., entry-wise) product; and in this case we write* $(\mathtt{i}, \mathbb{x}, \mathbb{w}) \in \mathcal{R}_{\mathsf{HPR}}$.

2.3 Interactive Proof Systems

Definition 2 (Interactive Proof System). *Let* $\mathcal{R}$ *be an indexed relation with corresponding relation language* $\mathcal{L}(\mathcal{R})$. *An* interactive proof system *is a pair* (P, V) *of stateful interactive Turing machines such that: the input to* P *is* $(\mathtt{i}, \mathbb{x}, \mathbb{w})$*, the input to* V *is* $(\mathtt{i}, \mathbb{x})$*;* P *and* V *exchange* $\mathsf{r} = \mathsf{r}(|\mathtt{i}|)$ *messages in total; and in the last step of the protocol* V *outputs a single bit* $b \in \{\top, \bot\}$. *The system satisfies two more properties:*

- Completeness — V *accepts members of* $\mathcal{L}(\mathcal{R})$*:* $(\mathtt{i}, \mathbb{x}) \in \mathcal{L}(\mathcal{R}) \Rightarrow b = \top$.
- Soundness *(with* soundness error σ*)* — V *rejects non-members of* $\mathcal{L}(\mathcal{R})$ *except with probability at most* σ *taken over the all random coins involved:* $\Pr[(\mathtt{i}, \mathbb{x}) \notin \mathcal{L}(\mathcal{R}) \Rightarrow b = \bot] \geq 1 - \sigma$.

Soundness becomes a moot point when for the given index $\mathtt{i}$ every instance $\mathbb{x}$ has a matching witness $\mathbb{w}$ such that $(\mathtt{i}, \mathbb{x}, \mathbb{w}) \in \mathcal{R}$. In this case a stronger notion called *knowledge soundness* [2] is preferred, which informally requires that any adversary that successfully convinces the verifier can be made to leak a witness by an extractor machine that has the same interface as the verifier but can additionally reset the adversary to an earlier point in time without forgetting the observed transcripts. In our context, all witnesses are encoded into oracles, and the prover displays knowledge of them simply by providing the oracles to the verifier. As a result, at our level of abstraction, knowledge soundness follows automatically from soundness. When the oracles are simulated by a concrete cryptographic tool, knowledge soundness becomes an important consideration that is not automatically satisfied. However, this cryptographic instantiation is beyond the scope of this paper.

A proof system is zero-knowledge [9] if, informally, an authentic transcript could have been produced by an adversary who is ignorant of the witness. More formally, the distribution of authentic transcripts must be sampleable with public information only.

Definition 3 (Honest-Verifier Zero-Knowledge). *Let* $\mathcal{R}$ *be an indexed relation and let* (P, V) *be a proof system for* $\mathcal{R}$*. Let* $tr \leftarrow \langle \mathsf{P}(\mathtt{i}, \mathbb{x}, \mathbb{w}), \mathsf{V}(\mathtt{i}, \mathbb{x}) \rangle$ *denote the assignment to the variable* tr *of the transcript arising from the interaction between* P *with input* $(\mathtt{i}, \mathbb{x}, \mathbb{w})$ *and* V *with input* $(\mathtt{i}, \mathbb{x})$*. The proof system* (P, V) *is* honest-verifier zero-knowledge *if there exists a polynomial-time Turing machine* S *such that the distribution* $\mathcal{D}_0$ *of authentic transcripts* $tr \leftarrow \langle \mathsf{P}(\mathtt{i}, \mathbb{x}, \mathbb{w}), \mathsf{V}(\mathtt{i}, \mathbb{x}) \rangle$*, is identical to the distribution* $\mathcal{D}_1$ *of simulated transcripts* $tr \leftarrow \mathsf{S}(\mathtt{i}, \mathbb{x})$*. When* $\mathcal{D}_0$ *and* $\mathcal{D}_1$ *are distinct, we consider the statistical distance and use the term* Statistical *Honest-Verifier Zero-Knowledge.*

2.4 Polynomial IOP

Informally, a Polynomial IOP is an abstract proof system, where the prover sends polynomials and the verifier, instead of reading the polynomials in their entirety, is allowed to query the polynomial as oracles in select points.

Definition 4 (Polynomial IOP). *Let $\mathcal{R}$ be an indexed relation with corresponding indexed language $\mathcal{L}(\mathcal{R})$, $\mathbb{F}$ some finite field, and $\mathsf{d} \in \mathbb{N}$ a degree bound. A* Polynomial IOP for $\mathcal{R}$ with degree bound d *is a pair of interactive machines (P, V), satisfying the following description.*

- (P, V) *is an interactive proof for $\mathcal{L}(\mathcal{R})$ with r rounds, and with soundness error σ.*
- P *sends polynomials $f_i(X) \in \mathbb{F}[X]$ of degree at most d to V.*
- V *is an oracle machine with access to a list of oracles, which contains one oracle for each polynomial it has received from the prover.*
- *When an oracle associated with a polynomial $f_i(X)$ is queried on a point $z_j \in \mathbb{F}$, the oracle responds with the value $f_i(z_j)$.*
- V *sends challenges $\alpha_k \in \mathbb{F}$ to P.*
- V *is public coin.*

In Appendix A we provide this alternative definition along with a transformation between definitions to establish their equivalence. This transformation does lose some generality: queries in $z_j = 0$ are not allowed and the soundness error increases by at most $q \cdot \frac{\mathsf{max}_i \mathsf{d}_i - \mathsf{min}_i \mathsf{d}_i}{|\mathbb{F}|-1}$, where q is the total number of queries. However, these restrictions are not significant for typical applications of Polynomial IOPs, where the field $\mathbb{F}$ is large.

With a minor extension, Polynomial IOPs can appropriately capture preprocessing. This extension introduces third machine, the *indexer* I. As its name suggest, I reads only $\mathtt{i}$, and it outputs a list of polynomials to which V has oracle access.

Definition 5 (Polynomial IOP with Preprocessing). *Let $\mathcal{R}$ be an indexed relation with corresponding language $\mathcal{L}(\mathcal{R})$. A* Polynomial IOP with Preprocessing *is a tuple of interactive machines $(\mathsf{I}, \mathsf{P}, \mathsf{V})$ such that (P, V) is a Polynomial IOP for $\mathcal{L}(\mathcal{R})$ and such that*

- I *takes $\mathtt{i}$ for input and outputs a list of polynomials of degree at most d;*
- V *has oracle access to these polynomials in addition to the polynomials it receives from P.*

Some of the Polynomial IOPs in this paper are designed for modular composition. As a result, V does not begin with an empty list of polynomial oracles. In order to define the relations that these Polynomial IOPs realize, we denote by $[f_i(X)]$ a polynomial $f_i(X)$ that was sent to V by I or P at some earlier stage and to which V has oracle access.

3 Dense Linear Algebra Relations

3.1 Inner Product

Bünz *et al.* [6] are the first to sketch a Polynomial IOP that realizes an inner product relation between two vectors. Our variant improves on this protocol as it involves one polynomial less. This optimization comes at the cost of doubling the maximum degree and increasing the number of points of evaluation. For odd order fields, the degree doubling can be avoided.

Formally, the relation realized by both protocols is

$$\mathcal{R}_{\text{ip}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = \mathsf{d} \\ \mathbb{x} = ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)], c) \\ \mathbb{w} = (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X)) \\ f_{\boldsymbol{a}}(X) = \sum_{i=0}^{\mathsf{d}} a_i X^i \\ f_{\boldsymbol{b}}(X) = \sum_{i=0}^{\mathsf{d}} b_i X^i \\ c = \sum_{i=0}^{\mathsf{d}} a_i b_i \end{array} \right\} . \tag{3}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{ip}})$
inputs: $\mathbb{i} : \mathsf{d}$
$\mathbb{x} : ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)], c)$
$\mathbb{w} : (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X))$
begin
- P computes $h(X) \leftarrow f_{\boldsymbol{a}}(X^2) \cdot f_{\boldsymbol{b}}(X^{-2}) \cdot X^{2\mathsf{d}} + f_{\boldsymbol{a}}(X^{-2}) \cdot f_{\boldsymbol{b}}(X^2) \cdot X^{2\mathsf{d}+1}$
- P computes $\bar{h}(X) \leftarrow h(X) \mod X^{2\mathsf{d}}$
- P sends $\bar{h}(X)$ of degree at most $2\mathsf{d}-1$ to V
- V samples $z \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and queries $([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)], [\bar{h}(X)])$ in (z^2, z^2, z) and in (z^{-2}, z^{-2}, z^{-1})
- V receives $y_a = f_{\boldsymbol{a}}(z^2)$, $y_a^* = f_{\boldsymbol{a}}(z^{-2})$, $y_b = f_{\boldsymbol{b}}(z^2)$, $y_b^* = f_{\boldsymbol{b}}(z^{-2})$, $y_h = \bar{h}(z)$, and $y_h^* = \bar{h}(z^{-1})$
- V tests $y_h + z^{2\mathsf{d}} \cdot c + z^{2\mathsf{d}+1} \cdot c + z^{4\mathsf{d}+1} \cdot y_h^* \stackrel{?}{=} y_a \cdot y_b^* \cdot z^{2\mathsf{d}} + y_a^* \cdot y_b \cdot z^{2\mathsf{d}+1}$

Protocol 1: InnerProduct

Theorem 1 (Security of InnerProduct). *Protocol* InnerProduct *of Protocol 2 is a Polynomial IOP for* $\mathcal{L}(\mathcal{R}_{\text{ip}})$ *with completeness and soundness with soundness error* $\sigma = \frac{4\mathsf{d}+1}{|\mathbb{F}|-1}$.

Proof. The protocol revolves around the symmetric polynomial identity

$$\bar{h}(X) + X^{2\mathsf{d}} \cdot c + X^{2\mathsf{d}+1} \cdot c + X^{4\mathsf{d}+1} \cdot \bar{h}(X^{-1}) = f_{\boldsymbol{a}}(X^2) \cdot f_{\boldsymbol{b}}(X^{-2}) \cdot X^{2\mathsf{d}} + f_{\boldsymbol{a}}(X^{-2}) \cdot f_{\boldsymbol{b}}(X^2) \cdot X^{2\mathsf{d}+1} \quad . \tag{4}$$

The verifier tests this identity by sampling left and right hand sides in a random point z. Since this is an identity whenever $c = \boldsymbol{a}^{\mathsf{T}}\boldsymbol{b}$, completeness follows. For soundness, consider when the test passes but the left and right hand sides of (4) are unequal. There are at most $4\mathsf{d}+1$ points z where left and right hand sides are equal, since both hands are bounded by this degree. By the Schwartz-Zippel lemma, the probability of a false accept is $\sigma = \frac{4\mathsf{d}+1}{|\mathbb{F}|-1}$. □

Note that for odd characteristic fields, it is possible to avoid interleaving the coefficients and rely instead on the simpler symmetric polynomial identity

$$\bar{h}(X) + X^{\mathsf{d}} \cdot 2 \cdot c + X^{2\mathsf{d}} \cdot \bar{h}(X^{-1}) = \\ f_{\boldsymbol{a}}(X) \cdot f_{\boldsymbol{b}}(X^{-1}) \cdot X^{\mathsf{d}} + f_{\boldsymbol{a}}(X^{-1}) \cdot f_{\boldsymbol{b}}(X) \cdot X^{\mathsf{d}} \quad . \quad (5)$$

We proceed in this paper with the interleaving variant in order to avoid loss of generality.

3.2 Batched Inner Product

We can batch multiple invocations of protocol InnerProduct into a single protocol that requires the prover to send only one polynomial oracle. Formally, the relation is given by

$$\mathcal{R}_{\text{bip}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \middle| \begin{array}{l} \mathbb{i} = (m, \mathsf{d}) \\ \mathbb{x} = \{([f_{\boldsymbol{a}_i}(X)], [f_{\boldsymbol{b}_i}(X)], c_i)\}_{i=1}^{m} \\ \mathbb{w} = \{(f_{\boldsymbol{a}_i}(X), f_{\boldsymbol{b}_i}(X))\}_{i=1}^{m} \\ f_{\boldsymbol{a}_i}(X) = \sum_{j=0}^{\mathsf{d}} a_{ij} X^i \\ f_{\boldsymbol{b}_i}(X) = \sum_{j=0}^{\mathsf{d}} b_{ij} X^i \\ c_i = \sum_{j=0}^{\mathsf{d}} a_{ij} b_{ij} \end{array} \right\} . \quad (6)$$

Theorem 2 (Security of BatchedInnerProduct). *Protocol* BatchedInnerProduct *of Protocol 2 is a Polynomial IOP for $\mathcal{L}(\mathcal{R}_{\text{bip}})$ with completeness and soundness with soundness error $\sigma = \frac{m+4\mathsf{d}+1}{|\mathbb{F}|-1}$.*

Proof. Let $H(X,Y) = \sum_{i=1}^{m} h_i(X) \cdot Y^{i-1}$ and $\bar{H}(X,Y) = H(X,Y) \bmod X^{2d}$. Note that $\bar{h}(X) = \bar{H}(X, \alpha)$.

The protocol revolves around the symmetric polynomial identity

$$\bar{H}(X,Y) + \sum_{i=1}^{m} (X^{2\mathsf{d}} \cdot c_i + X^{2\mathsf{d}+1} \cdot c_i) \cdot Y^{i-1} + X^{4\mathsf{d}+1} \cdot \bar{H}(X^{-1}, Y) = \\ \sum_{i=1}^{m} (f_{\boldsymbol{a}_i}(X^2) \cdot f_{\boldsymbol{b}_i}(X^{-2}) \cdot X^{2\mathsf{d}} + f_{\boldsymbol{a}_i}(X^{-2}) \cdot f_{\boldsymbol{b}_i}(X^2) \cdot X^{2\mathsf{d}+1}) \cdot Y^{i-1} \quad . \quad (7)$$

The verifier tests this identity by sampling left and right hand sides in a random point (z, α). Since this is an identity whenever $c_i = \boldsymbol{a}_i^{\mathsf{T}} \boldsymbol{b}_i$ for all i from 1

description: decides $\mathcal{L}(\mathcal{R}_{\text{bip}})$
inputs: $\mathbb{i} : (m, \mathsf{d})$
$\mathbb{x} : \{([f_{\boldsymbol{a}_i}(X)], [f_{\boldsymbol{b}_i}(X)], c_i)\}_{i=1}^m$
$\mathbb{w} : \{(f_{\boldsymbol{a}_i}(X), f_{\boldsymbol{b}_i}(X))\}_{i=1}^m$
begin
P computes $h_i(X) \leftarrow f_{\boldsymbol{a}_i}(X^2) \cdot f_{\boldsymbol{b}_i}(X^{-2}) \cdot X^{2\mathsf{d}} + f_{\boldsymbol{a}_i}(X^{-2}) \cdot f_{\boldsymbol{b}_i}(X^2) \cdot X^{2\mathsf{d}+1}$ for i from 1 to m
V samples $\alpha \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and sends α to P
P computes $\bar{h}(X) \leftarrow \sum_{i=1}^m h_i(X) \cdot \alpha^{i-1} \mod X^{2\mathsf{d}}$
P sends $\bar{h}(X)$ of degree at most $2\mathsf{d}-1$ to V
V samples $z \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and queries $(\{([f_{\boldsymbol{a}_i}(X)], [f_{\boldsymbol{b}_i}(X)])\}_{i=1}^m, [\bar{h}(X)])$ in $(\{z^2, z^2\}_{i=1}^m, z)$ and in $(\{z^{-2}, z^{-2}\}_{i=1}^m, z^{-1})$
V receives $y_{a,i} = f_{\boldsymbol{a}_i}(z^2)$, $y^*_{a,i} = f_{\boldsymbol{a}}(z^{-2})$, $y_{b,i} = f_{\boldsymbol{b}_i}(z^2)$, $y^*_{b,i} = f_{\boldsymbol{b}_i}(z^{-2})$ for i from 1 to m, and $y_h = \bar{h}(z)$, $y^*_h = \bar{h}(z^{-1})$
V tests $y_h + \sum_{i=1}^m (z^{2\mathsf{d}} \cdot c_i + z^{2\mathsf{d}+1} \cdot c_i) \cdot \alpha^{i-1} + z^{4\mathsf{d}+1} \cdot y^*_h \stackrel{?}{=} \sum_{i=1}^m (y_{a,i} \cdot y^*_{b,i} \cdot z^{2\mathsf{d}} + y^*_{a,i} \cdot y_{b,i} \cdot z^{2\mathsf{d}+1}) \cdot \alpha^{i-1}$

Protocol 2: BatchedInnerProduct

to m, completeness follows. For soundness, consider when the test passes but the left and right hand sides of (7) are unequal. For any $\bar{H}(X, Y)$, there are at most $m + 4\mathsf{d} + 1$ points (z, α) where left and right hand sides are equal, since both hands are bounded by this degree. By the (two-dimensional) Schwartz-Zippel lemma, the probability of a false accept is $\sigma = \frac{m+4\mathsf{d}+1}{|\mathbb{F}|-1}$. □

3.3 Modular Reduction

We start with a protocol that will be used as a subprotocol in the sequel. This protocol establishes that one polynomial, $r(X)$, is the remainder after division of a second polynomial $f(X)$, by a third, $d(X)$. This third polynomial is assumed to be known, but the protocol can be naturally amended to allow V only oracle access to $[d(X)]$. Formally, the relation is given by

$$\mathcal{R}_{\text{reduce}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (\mathsf{d}_f, \mathsf{d}_r) \\ \mathbb{x} = ([f(X)], [r(X)], d(X)) \\ \mathbb{w} = (f(X), r(X)) \\ \exists q(X) \in \mathbb{F}[X] \,.\, f(X) = q(X) \cdot d(X) + r(X) \\ \mathsf{deg}(f) \leq \mathsf{d}_f \\ \mathsf{deg}(r) \leq \mathsf{d}_r \end{array} \right\} . \tag{8}$$

Theorem 3 (Security of ModReduce**).** *Protocol* ModReduce *of Protocol 3 is a Polynomial IOP for* $\mathcal{L}(\mathcal{R}_{\text{reduce}})$ *with completeness and soundness with soundness error* $\sigma = \mathsf{d}_f/|\mathbb{F}|$.

Proof. completeness follows from construction: dividing $f(X)$ by $d(X)$ gives quotient $q(X)$ and remainder $r(X)$. Therefore, $f(X) = q(X) \cdot d(X) + r(X)$ is an

description: decides $\mathcal{L}(\mathcal{R}_{\text{reduce}})$
inputs: $\mathtt{i} : (\mathsf{d}_f, \mathsf{d}_r)$
$\mathbb{x} : ([f(X)], [r(X)], d(X))$
$\mathbb{w} : (f(X), r(X))$
begin
P computes q such that $f(X) = q(X) \cdot d(X) + r(X)$
P sends $q(X)$ of degree at most $\mathsf{d}_f - \mathsf{deg}(d)$ to V
V samples $z \xleftarrow{\$} \mathbb{F} \backslash \{0\}$ and queries $[f(X)]$, $[q(X)]$, and $[r(X)]$ in z
V receives $y_f = f(z)$, $y_q = q(z)$, and $y_r = r(z)$
V tests $y_f \stackrel{?}{=} y_q \cdot d(z) + y_r$

Protocol 3: ModReduce

identity of polynomials and guaranteed to hold everywhere including in the point z.

For soundness, observe that when $r(X) \not\equiv f(X) \bmod d(X)$ then $d(X)$ does not divide $f(X) - r(X)$. As a result, $f(X) \neq q(X) \cdot d(X) + r(X)$ is an inequality of polynomials with degree $\mathsf{deg}(d) + \mathsf{deg}(q) = \mathsf{d}_f$. Due to the Schwartz-Zippel lemma, the left and right hand sides can evaluate to the same value in at most d_f choices for z. The probability of V accepting when $r(X) \not\equiv f(X) \bmod d(X)$ is therefore $\sigma = \mathsf{d}_f / |\mathbb{F}|$.

What is left to argue is that P fails to convince V when the congruence $r(X) \equiv f(X) \bmod d(X)$ holds, but $r(X)$ is not equal to the remainder after division of $f(X)$ by $d(X)$. The representatives of the congruence class of $r(X)$ are apart by polynomials of degree at least $\mathsf{deg}(d)$, there is only one representative of degree at most $\mathsf{d}_r < \mathsf{deg}(d)$. The index value d_r therefore already constrains $r(X)$ to a unique polynomial. □

3.4 Matrix-Vector Product

The next protocol involves two polynomials that represent vectors in the monomial coefficient basis. It establishes that the one vector is the result of applying a linear transformation to the other. This linear transformation itself can be known and computed explicitly by the verifier. However, for succinct verifiers it is more appealing to encode this matrix into a polynomial oracle. Depending on the context, either the protocol's preprocessing phase produces this oracle, or another external protocol does.

Specifically Let $\boldsymbol{a} \in \mathbb{F}^n$ and $\boldsymbol{b} \in \mathbb{F}^m$ and $M \in \mathbb{F}^{m \times n}$ with the element in row i and column j (both indices starting at zero) indexed as $M_{[i,j]}$. These objects are represented as polynomials with $a_{[i]}$ being ith element of $\boldsymbol{a}$ and simultaneously the coefficient of the monomial X^i in $f_{\boldsymbol{a}}(X)$, and similarly for $\boldsymbol{b}, b_{[i]}$, and $f_{\boldsymbol{b}}(X)$. When encoded into polynomial form, the matrix is encoded in row-first order, specifically $f_M(X) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$. The protocol establishes that

$\boldsymbol{b} = M\boldsymbol{a}$. Formally, the relation is given by

$$\mathcal{R}_{\text{mvp}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (m, n, M) \\ \mathbb{x} = ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)]) \\ \mathbb{w} = (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X)) \\ f_{\boldsymbol{a}}(X) = \sum_{i=0}^{n-1} \boldsymbol{a}_{[i]} X^i \text{ for some } \boldsymbol{a} \in \mathbb{F}^n \\ f_{\boldsymbol{b}}(X) = \sum_{i=0}^{m-1} \boldsymbol{b}_{[i]} X^i \text{ for some } \boldsymbol{b} \in \mathbb{F}^m \\ \boldsymbol{b} = M\boldsymbol{a} \end{array} \right\} . \tag{9}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{mvp}})$
inputs: $\mathbb{i} : (m, n, M)$
$\mathbb{x} : ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)])$
$\mathbb{w} : (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X))$
// pre-processing
begin
  I computes $f_M(X) \leftarrow \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$
  I sends $f_M(X)$ of degree at most $mn - 1$ to P and V
begin
  V samples $\alpha \xleftarrow{\$} \mathbb{F}$ and sends α to P
  P computes $r(X) \leftarrow f_M(X) \bmod X^n - \alpha$
  P sends $r(X)$ of degree at most $n - 1$ to V
  P and V run ModReduce with $\mathbb{i}^{(1)} = (mn - 1, n - 1)$,
   $\mathbb{x}^{(1)} = ([f_M(X)], [r(X)], X^n - \alpha)$, and $\mathbb{w}^{(1)} = (f_M(X), r(X))$
  V queries $[f_{\boldsymbol{b}}(X)]$ in α and receives $y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}} = f_{\boldsymbol{b}}(\alpha)$
  P and V run InnerProduct with $\mathbb{i}^{(2)} = n - 1$, $\mathbb{x}^{(2)} = ([r(X)], [f_{\boldsymbol{a}}(X)], y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}})$,
   and $\mathbb{w}^{(2)} = (r(X), f_{\boldsymbol{a}}(X))$

Protocol 4: DenseMVP

Theorem 4 (Security of DenseMVP). *Protocol* DenseMVP *of Protocol 4 is a Polynomial IOP for* $\mathcal{L}(\mathcal{R}_{\text{mvp}})$ *with completeness and soundness with soundness error* $\sigma = \frac{mn+m+4n-5}{|\mathbb{F}|-1}$.

Proof. Let $\boldsymbol{\alpha}^\mathsf{T} = (\alpha^0, \alpha^1, \cdots)$ and $\boldsymbol{r}^\mathsf{T} = \boldsymbol{\alpha}^\mathsf{T} M$, and consider the equations

$$\boldsymbol{b} = M\boldsymbol{a} \tag{10}$$

$$\boldsymbol{\alpha}^\mathsf{T}\boldsymbol{b} = \boldsymbol{\alpha}^\mathsf{T} M\boldsymbol{a} \tag{11}$$

$$\sum_{i=0}^{m-1} \alpha^i b_{[i]} = \boldsymbol{r}^\mathsf{T}\boldsymbol{a} \tag{12}$$

$$f_{\boldsymbol{b}}(\alpha) = \sum_{i=0}^{n-1} r_{[i]} a_{[i]} \tag{13}$$

$$y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}} = \mathsf{coeffs}(r(X)) \cdot \mathsf{coeffs}(f_{\boldsymbol{a}}(X)) \tag{14}$$

$$(\mathbb{i}^{(2)}, \mathbb{x}^{(2)}) = (n-1, ([r(X)], [f_{\boldsymbol{a}}(X)], y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}})) \in \mathcal{L}(\mathcal{R}_{\text{ip}}) \ . \tag{15}$$

Furthermore, observe that the coefficient vector of $r(X)$ matches $\boldsymbol{r}$, by substituting X^n by α in the expression for $f_M(X)$:

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} M_{[i,j]} X^{in+j} \xrightarrow{X^n \mapsto \alpha} r(X) = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} M_{[i,j]} \alpha^i X^j \tag{16}$$

$$= \sum_{j=0}^{n-1} \left(\sum_{i=0}^{m-1} M_{[i,j]} \alpha^i \right) X^j \tag{17}$$

$$= \sum_{j=0}^{n-1} r_{[j]} X^j \ . \tag{18}$$

Completeness follows from the implications (10) $\Rightarrow$ (11) $\Leftrightarrow$ (12) $\Leftrightarrow$ (13) $\Rightarrow$ (14) $\Rightarrow$ (15).

For soundness, there are 3 events that can cause V to accept despite $\boldsymbol{b} \neq M\boldsymbol{a}$:

1. (10) $\not\Leftarrow$ (11). The probability of this event is at most $\frac{m-1}{|\mathbb{F}|-1}$ due to the Schwartz-Zippel lemma.
2. (13) $\not\Leftarrow$ (14) because $r(X)$ is not the remainder of $f_M(X)$ after division by $X^n - \alpha$. The probability of this event is at most $\frac{mn-1}{|\mathbb{F}|}$, the soundness error of $\mathsf{ModReduce}$.
3. (14) $\not\Leftarrow$ (15), because $y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}}$ is not the inner product of the coefficient vectors of $r(X)$ and $f_{\boldsymbol{a}}(X)$. The probability of this event is at most $\frac{4n-3}{|\mathbb{F}|}$, the soundness error of $\mathsf{InnerProduct}$.

By the union bound, the soundness error of $\mathsf{DenseMVP}$ is bounded by $\sigma = \frac{mn+m+4n-5}{|\mathbb{F}|-1}$. □

Note that after unrolling, the verifier the $\mathsf{DenseMVP}$ protocol tests two polynomial identities. One arises from expanding $\mathsf{ModReduce}$, and the other arises from $\mathsf{InnerProduct}$. Both polynomial identities involve the polynomial $r(X)$, and as a result it can be eliminated and the identities merged. We present the unrolled and optimized version in Appendix C.1.

To see that this merger has no effect on soundness, observe that the inequality $lhs_1 \neq lhs_2$ implies $r(X) \neq lhs_1$ or $r(X) \neq lhs_2$. The verifier therefore accepts this false instance with a probability bounded by the same soundness error as the unoptimized protocol. This optimization strategy translates more generally to (some) other Polynomial IOPs: to eliminate a polynomial that is common to two identities, move it to the right hand side and then equate both left hand sides.

3.5 Hadamard Product

The next protocol establishes that the Hadamard (or component-wise) product of two vectors is equal to a third. These vectors are represented as the coefficient vectors of polynomials $f_{\boldsymbol{a}}(X)$, $f_{\boldsymbol{b}}(X)$, and $f_{\boldsymbol{c}}(X)$ such that $\boldsymbol{c} = \boldsymbol{a} \circ \boldsymbol{b}$ and $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{F}^{\mathsf{d}+1}$. The protocol relies on the fact that $\boldsymbol{c} = \boldsymbol{a} \circ \boldsymbol{b}$ implies $\boldsymbol{\alpha}^{\mathsf{T}}(\boldsymbol{a} \circ \boldsymbol{b}) = \boldsymbol{\alpha}^{\mathsf{T}}\boldsymbol{c}$ for all vectors $\boldsymbol{\alpha}$. In other words, one can simply sample a random scalar $\alpha \xleftarrow{\$} \mathbb{F}$, and check the inner product of $\boldsymbol{\alpha} \cdot \boldsymbol{a}$ with $\boldsymbol{b}$ against the inner product $\boldsymbol{\alpha}^{\mathsf{T}}\boldsymbol{c}$. Note that the right hand side of this check amounts to $f_{\boldsymbol{c}}(\alpha)$ and the operands in the left hand side amount to the coefficient vectors of $f_{\boldsymbol{a}}(\alpha X)$ and $f_{\boldsymbol{b}}(X)$, respectively. Formally, the relation is given by

$$\mathcal{R}_{\text{hadamard}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = \mathsf{d} \\ \mathbb{x} = ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)], [f_{\boldsymbol{c}}(X)]) \\ \mathbb{w} = (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X), f_{\boldsymbol{c}}(X)) \\ \forall i \in \{0, \ldots, \mathsf{d}\} \,.\, a_i b_i = c_i \end{array} \right\} \,. \tag{19}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{hadamard}})$
inputs: $\mathbb{i}$: d
$\mathbb{x}$: $[f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)], [f_{\boldsymbol{c}}(X)]$
$\mathbb{w}$: $f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X), f_{\boldsymbol{c}}(X)$
begin
V samples $\alpha \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and sends α to P
P evaluates $y \leftarrow f_{\boldsymbol{c}}(\alpha)$
V queries $[f_{\boldsymbol{c}}(X)]$ in α and receives $y = f_{\boldsymbol{c}}(\alpha)$
P and V run InnerProduct with $\mathbb{i}^{(1)} = \mathsf{d}$, $\mathbb{x}^{(1)} = ([f_{\boldsymbol{a}}(\alpha X)], [f_{\boldsymbol{b}}(X)], y)$, $\mathbb{w}^{(1)} = (f_{\boldsymbol{a}}(\alpha X), f_{\boldsymbol{b}}(X))$, where V simulates $[f_{\boldsymbol{a}}(\alpha X)]$ using $[f_{\boldsymbol{a}}(X)]$ and the scalar α

Protocol 5: Hadamard

Theorem 5 (Security of Hadamard). *Protocol* Hadamard *of Protocol 9 is a Polynomial IOP for* $\mathcal{L}(\mathcal{R}_{\text{hadamard}})$ *with completeness and soundness with soundness error* $\sigma = (5\mathsf{d} + 1)/(|\mathbb{F}| - 1)$.

Proof. Consider the following sequence of equations.

$$\boldsymbol{a} \circ \boldsymbol{b} = \boldsymbol{c} \tag{20}$$

$$\boldsymbol{\alpha}^{\mathsf{T}} \cdot (\boldsymbol{a} \circ \boldsymbol{b}) = \boldsymbol{\alpha}^{\mathsf{T}} \cdot \boldsymbol{c} \tag{21}$$

$$\sum_{i=0}^{\mathsf{d}} (\alpha^i \boldsymbol{a}_{[i]}) \boldsymbol{b}_{[i]} = \sum_{i=0}^{\mathsf{d}} \alpha^i \boldsymbol{c}_{[i]} \tag{22}$$

$$\mathsf{coeffs}(f_{\boldsymbol{a}}(\alpha X)) \cdot \mathsf{coeffs}(f_{\boldsymbol{b}}(X)) = f_{\boldsymbol{c}}(\alpha) \tag{23}$$

$$\mathsf{coeffs}(f_{\boldsymbol{a}}(\alpha X)) \cdot \mathsf{coeffs}(f_{\boldsymbol{b}}(X)) = y \tag{24}$$

$$(\mathbb{i}, \mathbb{x}) = (\mathsf{d}, ([f_{\boldsymbol{a}}(\alpha X)], [f_{\boldsymbol{b}}(X)], y)) \in \mathcal{L}(\mathcal{R}_{\mathsf{InnerProduct}}) \tag{25}$$

Completeness follows from the sequence of implications (20) $\Rightarrow$ (21) $\Leftrightarrow$ (22) $\Leftrightarrow$ (23) $\Leftrightarrow$ (24) $\Rightarrow$ (25).

For soundness, consider when the reverse implications fail.

- (20) $\not\Leftarrow$ (21). This event happens with probability at most $\mathsf{d}/(|\mathbb{F}| - 1)$ due to the Schwartz-Zippel lemma.
- (24) $\not\Leftarrow$ (25). This event happens with probability at most $(4\mathsf{d}+1)/(|\mathbb{F}| - 1)$, the soundness error of $\mathsf{InnerProduct}$.

Therefore, the probability that V accepts even though $\boldsymbol{a} \circ \boldsymbol{b} \neq \boldsymbol{c}$ is bounded by $\sigma = (5\mathsf{d} + 1)/(|\mathbb{F}| - 1)$. □

4 Sparse Linear Algebra Relations

The purpose of this section is to present an analogue of the $\mathsf{DenseMVP}$ Polynomial IOP but that works when the matrix M is represented sparsely, *i.e.*, as a list of nonzero coefficients and their coordinates. The full, formal presentation of this protocol is rather lengthy, and so we defer it to Appendix B. Here we present an intuitive, high-level overview with just enough detail so that the reader could reconstruct the deferred formal presentation.

4.1 High-Level Overview

Let $M \in \mathbb{F}^{m \times n}$ be a matrix with only K nonzero elements, such that it can be represented as $M = \sum_{k=0}^{K-1} \mathbf{e}_{\mathsf{row}(k)} \mathbf{e}_{\mathsf{col}(k)}^{\mathsf{T}} \cdot \mathsf{val}(k)$, where $\mathbf{e}_i$ is the ith unit vector, where $\mathsf{row}, \mathsf{col} : \mathbb{N} \to \mathbb{N}$ indicate the column and row of the kth element, and where $\mathsf{val} : \mathbb{N} \to \mathbb{F}$ indicates its value. We detail a protocol to establish that $\mathbf{y} = M\mathbf{x}$. We first explain the steps from a high level point of view.

From MVP to *bivariate polynomial evaluation.* A key component of the dense matrix-vector multiplication protocol is the evaluation of $(f_M(X) \mod X^n - \alpha)$ at the point z, where $f_M(X)$ is the polynomial associated with the matrix

M, *i.e.*, $f_M(X) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$. This step can equivalently be interpreted as the evaluation of the bivariate polynomial $f_M(X,Y) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^i Y^j$ in the point (α, z). In other words, if we can achieve sparse bivariate polynomial evaluation, then we can achieve sparse matrix-vector products.

From *bivariate polynomials* to *univariate monomial vectors*. The reduction goes one step further: it is possible to achieve sparse bivariate polynomial evaluation given a procedure that establishes that the vector of coefficients of a dense polynomial is the same as the vector of monomials of a sparse univariate polynomial when evaluated in a given point. To see this, observe that a sparse bivariate polynomial $f(X,Y) = \sum_{k=0}^{K-1} c_k X^{a_k} Y^{b_k}$ can be evaluated in a point (x,y) using the polynomials $f_c(Z) = \sum_{k=0}^{K-1} c_k X^k$, $f_x(X) = \sum_{k=0}^{K-1} x^{a_k} X^k$, and $f_y(X) = \sum_{k=0}^{K-1} y^{b_k} X^k$, simply by performing one Hadamard and one InnerProduct subprotocol. This reduction does introduce a problem, namely $f_x(X)$ and $f_y(X)$ cannot be known before V supplies x and y. So how does P commit to them, and how does V verify that the received oracles match with the commitment?

From *univariate monomial vector* to *bit matrix*. Let's focus on $f_x(X)$, as $f_y(X)$ proceeds analogously. This polynomial can be represented by a bit matrix B, which takes the value 1 in cells (a_k, k) and 0 elsewhere. Let $H = \max_k a_k$, $\mathbf{x} = (x^0, x, x^2, \ldots, x^{H-1})^\mathsf{T}$, and $z = (z^0, z, z^2, \ldots, z^{K-1})^\mathsf{T}$. Then B represents the polynomial $f_x(X)$ since $f_x(z) = \mathbf{x} B \mathbf{z}$.

From *bit matrix* to *Lagrange and Vandermonde* matrices. The idea is to decompose the matrix $B \in \mathbb{F}^{H \times K}$ as the product of two matrices, $L \in \mathbb{F}^{H \times H}$ and $R \in \mathbb{F}^{H \times K}$. Let $\mathcal{H} \subset \mathbb{F}$ be a set of H distinct elements of $\mathbb{F}$ and $\varphi : \mathbb{N} \to \mathcal{H}$ a canonical mapping from $\{0, \ldots, H-1\}$ to $\mathcal{H}$. L is the Lagrange matrix, whose hth row is the coefficient vector of $\mathcal{L}_h(X)$, which is the Lagrange polynomial taking the value 1 in $\varphi(h)$ and 0 in all other points of $\mathcal{H}$. Symbolically:

$$\mathcal{L}_h(X) = \sum_{i=0}^{H-1} L_{[h,i]} X^i = \prod_{\substack{i=0 \\ i \neq h}}^{H-1} \frac{X - \varphi(i)}{\varphi(h) - \varphi(i)} \ . \tag{26}$$

R is the Vandermonde matrix, whose rows are the (Hadamard) powers of $(\varphi(a_k))_{k=0}^{K-1}$. Specifically:

$$R = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varphi(a_0) & \varphi(a_1) & \cdots & \varphi(a_{K-1}) \\ \varphi(a_0)^2 & \varphi(a_1)^2 & \cdots & \varphi(a_{K-1})^2 \\ \vdots & \vdots & \cdots & \vdots \\ \varphi(a_0)^{H-1} & \varphi(a_1)^{H-1} & \cdots & \varphi(a_{K-1})^{H-1} \end{pmatrix} \ . \tag{27}$$

To verify that $LR = B$, observe that the inner product between $L_{[h,:]}$ and $R_{[:,k]}$ is equal to $\mathcal{L}_h(\varphi(a_k))$. When V provides (x, z) hoping to obtain $\mathbf{x}^\mathsf{T} B \mathbf{z}$, P will respond with $[\mathbf{x}^\mathsf{T} L]$ and $[R\mathbf{z}]$ (in polynomial form), and both proceed to an $\mathsf{InnerProduct}$ protocol. We will refer to these vectors as the Lagrange and Vandermonde vectors, respectively. The next question is, how and against what does V verify them?

Verifying the Lagrange vector. After sending x and receiving the vector (encoded as a polynomial oracle) $[\mathbf{x}^\mathsf{T} L]$, V sends γ to P, who responds with the vector $[L\boldsymbol{\gamma}]$, where $\boldsymbol{\gamma} = (1, \gamma, \gamma^2, \ldots, \gamma^{H-1})^\mathsf{T}$. Let $Z_{\mathcal{H}}(X)$ be the unique monic polynomial of degree degree $H-1$ that vanishes on $\mathcal{H}$. By repeating the equation

$$\mathcal{L}_h(\gamma) \cdot (\gamma - \varphi(h)) = \frac{Z_{\mathcal{H}}(\gamma)}{\prod_{\substack{i=0 \\ i \neq h}}^{H-1} (\varphi(h) - \varphi(i))} \tag{28}$$

for every h, V can check $L\boldsymbol{\gamma}$ using a $\mathsf{Hadamard}$ subprotocol, assuming that P or I previously committed to oracles for $f_\varphi(X) = \sum_{h=0}^{H-1} \varphi(h) X^h$ and $f_{\mathcal{H}}(X) = \sum_{h=0}^{H-1} \left(\prod_{i \in \{0 \ldots H-1\} \setminus \{h\}} (\varphi(h) - \varphi(i)) \right)^{-1} \cdot X^h$. The next step is to query the oracles $[\mathbf{x}L]$ and $[L\boldsymbol{\gamma}]$ in γ and x, respectively and verify that the responses match.

Verifying the Vandermonde Vector. A similar technique allows V to verify the Vandermonde vector. After sending z and receiving $[R\mathbf{z}]$ back, V sends δ, and P responds with $[\boldsymbol{\delta}^\mathsf{T} R]$. Next, V checks that for every $k \in \{0, \ldots, K-1\}$,

$$\left(\sum_{i=0}^{H-1} (\delta \cdot \varphi(a_k))^i \right) \cdot (\delta \varphi(a_k) - 1) = (\delta \varphi(a_k))^H - 1 \tag{29}$$

using another $\mathsf{Hadamard}$ protocol and the precommitted oracle $f_a(X) = \sum_{k=0}^{K-1} \varphi(a_k) X^k$. Lastly, V queries $[R\mathbf{z}]$ in δ to see if the response matches with $[\boldsymbol{\delta} R]$ when queried in z.

Batching Lagrange and Vandermonde Vectors. In order to establish the correct evaluation of the bivariate polynomial, the prover must establish the correct production of two univariate monomial vectors. A naïve implementation invokes the Lagrange vector and the Vandermonde vector procedure twice. However, it turns out to be possible to merge these two invocations, and save a total of 4 polynomials. We treat this optimization explicitly in Appendix C.

5 A Polynomial IOP for Arithmetic Circuits

5.1 The Protocol

The next protocol, Protocol 6 puts many of the previously developed tools together into a Polynomial IOP (with preprocessing) for arithmetic circuits as

captured by the HPR. To differentiate our protocol from other similar ones, we name it Claymore.

description: realizes $\mathcal{R}_{\text{hpr}}$
inputs: $\mathbb{i}$: (m, n, M) with $M \in \mathbb{F}^{m \times (3n+1)}$
$\mathbb{x}$: $\mathbf{x} \in \mathbb{F}^n$
$\mathbb{w}$: $(\mathbf{w_l}, \mathbf{w_r}, \mathbf{w_o}) \in \mathbb{F}^n \times \mathbb{F}^n \times \mathbb{F}^n$
// preprocessing
begin
  I runs MVP.I on $\mathbb{i}^{(1)} = (m, 3n+1, M)$
// online
begin
  P computes $f_{wl} \leftarrow \sum_{j=0}^{n-1} \mathbf{w_l}_{[j]} X^j$, $f_{wr} \leftarrow \sum_{j=0}^{n-1} \mathbf{w_r}_{[j]} X^j$, and $f_{wo} \leftarrow \sum_{j=0}^{n-1} \mathbf{w_o}_{[j]} X^j$
  P sends $f_{wl}(X)$, $f_{wr}(X)$, and $f_{wo}(X)$, all of degrees at most $n-1$, to V
  P computes $f_{1w}(X) \leftarrow 1 + X f_{wl}(X) + X^{n+1} f_{wr}(X) + X^{2n+1} f_{wo}(X)$
  P computes $f_x(X)$, whose coefficient vectors correspond to $\mathbf{x} = M\,(1|\mathbf{w_l}^\mathsf{T}|\mathbf{w_r}^\mathsf{T}|\mathbf{w_o}^\mathsf{T})^\mathsf{T}$
  P and V run MVP with $\mathbb{i}^{(1)} = (m, 3n+1, M)$, $\mathbb{x}^{(1)} = ([f_{1w}(X)], [f_x(X)])$, $\mathbb{w}^{(1)} = (f_{1w}(X), f_x(X))$ where V simulates $[f_{1w}(X)]$ using $f_{1w}(X) = 1 + X f_{wl}(X) + X^{n+1} f_{wr}(X) + X^{2n+1} f_{wo}(X)$, $[f_{wl}(X)]$, $[f_{wr}(X)]$, and $[f_{wo}(X)]$; and where V computes $[f_x(X)]$ locally using $\mathbf{x} = \mathbb{x}$
  P and V run Hadamard with $\mathbb{i}^{(2)} = n-1$, $\mathbb{x}^{(2)} = ([f_{wl}(X)], [f_{wr}(X)], [f_{wo}(X)])$, $\mathbb{w}^{(2)} = (f_{wl}(X), f_{wr}(X), f_{wo}(X))$

Protocol 6: Claymore

Theorem 6 (Security of Claymore). *Protocol Claymore of Protocol 6 is a Polynomial IOP for $\mathcal{R}_{\text{HPR}}$ with completeness and soundness error $\sigma \leq \sigma_{\mathsf{Hadamard}} + \sigma_{\mathsf{MVP}}$.*

Proof. Completeness follows from construction. Since the arguments are computed honestly, the subprotocols succeed and guarantee equalities (1) and (2), respectively.

Soundness. If the HPR instance is a false instance, then $\mathbf{x} \neq M(1|\mathbf{w_l}^\mathsf{T}|\mathbf{w_r}^\mathsf{T}|\mathbf{w_o}^\mathsf{T})^\mathsf{T}$ or $\mathbf{w_l} \circ \mathbf{w_r} \neq \mathbf{w_o}$. As a result either the Hadamard protocol succeeds despite being run on a false instance, or the MVP protocol succeeds despite being run on a false instance. The probabilities of these events are respectively at most $\sigma_{\mathsf{Hadamard}}$ and at most σ_{MVP}. □

5.2 The Role of Preprocessing

The preprocessing phase can be omitted. In this case, V must compute $f_M(X)$ locally. This task requires $O(mn)$ work, or only $O(K)$ if the matrix M has only

K nonzero elements and is represented as such. When this phase is omitted, Claymore should be compared to the Polynomial IOP underlying Aurora [4].

When used with preprocessing, Claymore achieves fast verification. Specifically, the matrix M which determines the circuit being proved, is processed by the indexer. For long and drawn-out computations, this matrix is typically sparse and the SparseMVP is suitable. However, for short and especially shallow computations, DenseMVP is the better option. Depending on the choice of MVP protocol, the matching soundness error should be considered.

5.3 Optimizations

Batch the Inner Product Protocols. Note that the unrolled SparseClaymore protocol consists of 10 invocations of InnerProduct protocol. We can replace these InnerProduct protocols by the BatchedInnerProduct protocol presented in Protocol 2. To see that this replacement does not affect the soundness, note that the InnerProduct subprotocols do not involve any verifier randomness and we can safely postpone them to the end of the Claymore protocol. Next, we replace them with a BatchedInnerProduct, unifying the degrees by the maximal degree of these polynomials. The prover passes the original InnerProduct protocols with high probability if and only if the prover passes the BatchedInnerProduct protocol with high probability.

Batch the Sparse Vector Protocols. We also present an alternative version of SparseBiEval by batching the two instances of VandermondeVector and the two LagrangeVector protocols. This optimization eliminates four polynomial oracles at the cost of doubling the polynomial degrees. We present the protocol details and security proofs in Appendix C.2.

Concatenate Left and Right Wire Vectors Instead of sending three witness polynomials $(f_{wl}(X), f_{wr}(X), f_{wo}(X))$, the prover can get away with sending only two: $(f_{wi}(X), f_{wo}(X))$ where $f_{wi}(X) = f_{wl}(X) + X^n \cdot f_{wr}(X)$. This concatenation is already implicit in the matrix-vector product subprotocol. The input to the Hadamard subprotocol should be $\mathbb{x} = ([f_{wi}(X)], [X^n \cdot f_{wi}(X)], [X^n \cdot f_{wo}(X)])$. The subprotocol then establishes that

$$\left(\begin{array}{c}\mathbf{w_l}\\\hline\mathbf{w_r}\\\hline\mathbf{0}_n\end{array}\right) \circ \left(\begin{array}{c}\mathbf{0}_n\\\hline\mathbf{w_l}\\\hline\mathbf{w_r}\end{array}\right) = \left(\begin{array}{c}\mathbf{0}_n\\\hline\mathbf{w_o}\\\hline\mathbf{0}_n\end{array}\right) \quad , \tag{30}$$

which is clearly equivalent to the original Hadamard relation. With this technique, the polynomials are degree $3n-1$, and so the soundness error is $(15n-4)/(|\mathbb{F}|-1)$ instead of $(5n-4)/(|\mathbb{F}|-1)$.

This optimization also preserves zero knowledge. To see this, observe that any distinguisher D that uses $f_{wi}(X)$ can be simulated with a distinguisher D' that uses $f_{wl}(X)$ and $f_{wr}(X)$. As a result, the optimized protocol lacks zero knowledge only if the protocol before applying the optimization also lacks it.

6 Zero-Knowledge

The strategy for achieving zero-knowledge consists of appending q randomizers to the initial wire vectors $\mathbf{w_l}$, $\mathbf{w_r}$, and $\mathbf{w_o}$. The randomizers will make the witness polynomials q-wise independent, meaning that no distinguisher restricted to at most q queries will obtain any infomation about the witness.

description: realizes $\mathcal{R}_{\text{HPR}}$
inputs: $\mathbb{i}$: (m, n, M) with $M \in \mathbb{F}^{m \times n}$
$\mathbb{x}$: $\mathbf{x} \in \mathbb{F}^n$
$\mathbb{w}$: $(\mathbf{w_l}, \mathbf{w_r}, \mathbf{w_o}) \in \mathbb{F}^n \times \mathbb{F}^n \times \mathbb{F}^n$
additional parameters: q
offline preprocessing:
V runs Claymore.I on $\mathbb{i}^{(1)} = (m, n+q, M' =$
$\left(M_{[:,0:(n+1)]} | 0_{m \times q} | M_{[:,(n+1):(2n+1)]} | 0_{m \times q} | M_{[:,(2n+1):(3n+1)]} | 0_{m \times q}\right))$
online phase:
// compute witness polynomial with randomizers
P samples $\mathbf{r}^{(l)} \xleftarrow{\$} \mathbb{F}^q$ and $\mathbf{r}^{(r)} \xleftarrow{\$} \mathbb{F}^q$
P and V run Claymore with $\mathbb{i}^{(1)} = (m, n+q, M')$, $\mathbb{x}^{(1)} = \mathbf{x}$,
$\mathbb{w}^{(1)} = ((\mathbf{w_l}^\mathsf{T} | \mathbf{r}^{(l)\,\mathsf{T}}), (\mathbf{w_r}^\mathsf{T} | \mathbf{r}^{(r)\,\mathsf{T}}), (\mathbf{w_o}^\mathsf{T} | \mathbf{r}^{(l)\,\mathsf{T}} \circ \mathbf{r}^{(r)\,\mathsf{T}}))$

Protocol 7: ZKClaymore

It is tricky to define zero knowledge the context of Polynomial IOPs. The distinguisher D can always query the received oracles in enough points to interpolate and then extract the witness. The notion is only meaningful when the number of queries bounded by some parameter. We furthermore restrict the distinguisher's queries to be distributed identically to that of an honest verifier; this restriction therefore corresponds to *honest-verifier* zero knowledge. As a result, we are not concerned with finding a complete description of the polynomials that make up the transcript. Instead, we are only concerned with the verifier's view of the transcript. This view corresponds to the list of queries and responses to the various oracles.

Theorem 7. *When $q \geq 6$, the Polynomial IOP* ZKClaymore *of protocol 7 has statistical honest-verifier zero-knowledge if all the* InnerProduct *subprotocols are replaced by a single invocation of* BatchedInnerProduct*. Concretely, the statistical distance between the verifier's view of authentic transcript versus the verifier's view of simulated transcript is bounded by $\frac{75+12n+12q}{|\mathbb{F}|-1}$.*

Proof. We show how S produces the verifier view for $(\mathbb{i}, \mathbb{x})$ without knowledge of $\mathbb{w}$. In the process, we establish that this view is indistinguishable from that of an authentic protocol execution.

The protocol ZKClaymore consists of an invocation to Hadamard protocol and an invocation to either the dense or sparse variant of MVP. Note that both protocols DenseMVP and SparseMVP consists of:

1. a query to $f_x(X)$ at uniformly random $\alpha \xleftarrow{\$} \mathbb{F}\backslash\{0\}$;
2. a protocol invocation (ModReduce in DenseMVP, or SparseBiEval in SparseMVP) with inputs that are independent of $\mathbf{w_l}, \mathbf{w_r}, \mathbf{w_o}$;
3. an invocation of InnerProduct on input $f_{1w}(X)$ and another polynomial ($r(X)$ in DenseMVP or $f_{\boldsymbol{\alpha}^\intercal M}(X)$ in SparseMVP), denoted by $f_t(X)$ hereafter, that is also independent of $\mathbf{w_l}, \mathbf{w_r}, \mathbf{w_o}$.

Since S knows M and $\mathbf{x}$, S can compute all polynomials that do not depend on witnesses honestly, *i.e.*, as the honest P would. We therefore restrict attention to polynomials that depend on the witness.

What remains is to demonstrate how to sample the verifier view for InnerProduct on input $f_{1w}(X)$ and $f_t(X)$, and for Hadamard on input $f_{wl}(X)$, $f_{wr}(X)$ and $f_{wo}(X)$. These two subprotocols contribute two polynomial pairs to the BatchedInnerProduct protocol. It suffices to sample the verifier view for the BatchedInnerProduct protocol just for these two polynomial pairs, because the remaining pairs are independent of the witness.

This view consists of several elements, namely:

1. Uniformly random z, β
2. $y_h = \bar{h}(z), y_h^* = \bar{h}(z^{-1})$
3. The verifier view contributed by the InnerProduct protocol in MVP:
   (a) $y_l = f_{wl}(z^2), y_l^* = f_{wl}(z^{-2})$
   (b) $y_r = f_{wr}(z^2), y_r^* = f_{wr}(z^{-2})$
   (c) $y_o = f_{wo}(z^2), y_o^* = f_{wo}(z^{-2})$
   (d) $y_t = f_t(z^2), y_t^* = f_t(z^{-2})$ (S samples these honestly)
4. The verifier view contributed by the top-level Hadamard protocol:
   (a) Uniformly random γ and $y_{o_2} = f_{wo}(\gamma)$
   (b) $y_{l_2} = f_{wl}((\gamma z)^2), y_{l_2}^* = f_{wl}((\gamma z)^{-2})$
   (c) Note that $y_r = f_{wr}(z^2)$ and $y_r^* = f_{wr}(z^{-2})$ have already been determined by the MVP item

In the verifier view of an honest run, the above values satisfy:

$$y_h + (z^{6(n+q)} + z^{6(n+q)+1}) \cdot (f_x(\alpha) + \beta \cdot y_{o_2}) + z^{12(n+q)+1} y_h^* = \tag{31}$$
$$((y_l + y_r + y_o) \cdot y_t^* + \beta \cdot y_{l_2} \cdot y_r) \cdot z^{6(n+q)} + ((y_l^* + y_r^* + y_o^*) \cdot y_t + \beta \cdot y_{l_2}^* \cdot y_r) \cdot z^{6(n+q)+1} \quad .$$

S samples uniformly random $\alpha, \beta, \gamma, z \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and computes y_t, y_t^* honestly.

Next, S samples $y_l, y_l^*, y_{l_2}, y_{l_2}^*$ as follows. Note that except for few choices of z and γ, the following matrix contains at least one 4×4 invertible submatrix in the last q columns.

$$Z_1 = \begin{pmatrix} 1 & z^2 & z^4 & \dots & z^{2(n+q-1)} \\ 1 & z^{-2} & z^{-4} & \dots & z^{-2(n+q-1)} \\ 1 & (\gamma z)^2 & (\gamma z)^4 & \dots & (\gamma z)^{2(n+q-1)} \\ 1 & (\gamma z)^{-2} & (\gamma z)^{-4} & \dots & (\gamma z)^{2(n+q-1)} \end{pmatrix}$$

The last four elements of $\mathbf{r}^{(l)}$ are uniformly random over $\mathbb{F}$, so $(y_l, y_l^*, y_{l_2}, y_{l_2}^*)^\intercal = Z_1 \cdot (\mathbf{w_l}^\intercal | \mathbf{r}^{(l)\intercal})^\intercal$ is uniformly random over $\mathbb{F}^4$, and S samples them as such.

Next, S samples $y_r, y_r^*, y_o, y_o^*, y_{o_2}$ as follows. Note that except for few choices of z, γ and $\mathbf{r}^{(l)}$, the following matrix contains at least one 5×5 invertible submatrix in the last q columns.

$$Z_2 = \begin{pmatrix} 1 & z^2 & z^4 & \cdots & z^{2(n+q-1)} \\ 1 & z^{-2} & z^{-4} & \cdots & z^{-2(n+q-1)} \\ \mathbf{w_l}_{[0]} & \mathbf{w_l}_{[1]} \cdot z^2 & \mathbf{w_l}_{[2]} \cdot z^4 & \cdots & \mathbf{r}^{(l)}_{[q-1]} \cdot z^{2(n+q-1)} \\ \mathbf{w_l}_{[0]} & \mathbf{w_l}_{[1]} \cdot z^{-2} & \mathbf{w_l}_{[2]} \cdot z^{-4} & \cdots & \mathbf{r}^{(l)}_{[q-1]} \cdot z^{-2(n+q-1)} \\ \mathbf{w_l}_{[0]} & \mathbf{w_l}_{[1]} \cdot \gamma & \mathbf{w_l}_{[2]} \cdot \gamma^2 & \cdots & \mathbf{r}^{(l)}_{[q-1]} \cdot \gamma^{n+q-1} \end{pmatrix}$$

The last 5 elements of $\mathbf{r}^{(r)}$ are uniformly random over $\mathbb{F}$ and independent from $\mathbf{r}^{(l)}$, so $(y_r, y_r^*, y_o, y_o^*, y_{o_2}) = Z_2 \cdot (\mathbf{w_r}^\mathsf{T} | \mathbf{r}^{(r)\mathsf{T}})^\mathsf{T}$ is uniformly random over $\mathbb{F}^5$, and S samples them as such.

It remains to sample y_h, y_h^* such that the equation (31) holds. Since we can solve for y_h^* given the other, we only need to show that y_h is uniformly random over $\mathbb{F}$.

Let $\bar{h}_{had}(X) = (f_{wl}((\gamma X)^2) f_{wr}(X^{-2}) + X f_{wl}((\gamma X)^{-2}) f_{wr}(X^2)) \cdot X^{2(n+q-1)} \bmod X^{2(n+q-1)}$. It suffices to show that $\bar{h}_{had}(z)$ is uniformly random, because y_h^* is a polynomial in β and this polynomial has $\bar{h}_{had}(z)$ as a coefficient. Observe that $\bar{h}_{had}(z)$ is equal to

$$(\mathbf{w_l}^\mathsf{T} | \mathbf{r}^{(l)\mathsf{T}}) \cdot \mathsf{diagonal}(1, \gamma^2, \cdots, \gamma^{2n+2q-2}) \cdot \begin{pmatrix} 0 & z^{2(n+q)-3} & z^{2(n+q)-5} & \cdots & z^5 & z^3 & z \\ z^{2(n+q-2)} & 0 & z^{2(n+q)-3} & \cdots & z^7 & z^5 & z^3 \\ z^{2(n+q-3)} & z^{2(n+q-2)} & 0 & \cdots & z^9 & z^7 & z^5 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ z^4 & z^6 & z^8 & \cdots & 0 & z^{2(n+q)-3} & z^{2(n+q)-5} \\ z^2 & z^4 & z^6 & \cdots & z^{2(n+q-2)} & 0 & z^{2(n+q)-3} \\ 1 & z^2 & z^4 & \cdots & z^{2(n+q-3)} & z^{2(n+q-2)} & 0 \end{pmatrix} \begin{pmatrix} \mathbf{w_r} \\ \hline \mathbf{r}^{(r)} \end{pmatrix} . \tag{32}$$

Therefore, $\bar{h}_{had}(z)$ is the inner product of $(\mathbf{w_l}^\mathsf{T} | \mathbf{r}^{(l)\mathsf{T}})$ with another vector that depends only on z, γ, and $(\mathbf{w_r}^\mathsf{T} | \mathbf{r}^{(r)\mathsf{T}})$. This vector is linearly independent from the rows of Z_2 with overwhelming probability. Put this vector into Z_2 as the last row and let the resulting matrix be Z_2'. Then $(y_r, y_r^*, y_o, y_o^*, y_{o_2}, y_h) = Z_2' \cdot (\mathbf{w_r}^\mathsf{T} | \mathbf{r}^{(r)\mathsf{T}})^\mathsf{T}$ is uniformly random over $\mathbb{F}^6$, and S samples them as such.

To complete the argument, except with a negligible failure probability corresponding to the matrices Z_1 or Z_2' being singular, S samples a verifier view from a distribution that is identical to the distribution of verifier views of an authentic protocol execution. The distinguishing advantage of any distinguisher D is bounded by the S's failure probability, which is a negligible function of the field size.

To obtain the concrete bound, start by observing that Z_1 is a Vandermonde matrix whose second column consists of four uniformly sampled quadratic

residues. Its rightmost square submatrix is singular only if duplicates are sampled, so

$$\Pr[\mathsf{det}(Z_{1,[:,n+q-4:n+q-1]}) = 0] \leq \frac{1}{(|\mathbb{F}|-1)/2} \cdot \frac{2}{(|\mathbb{F}|-1)/2} \cdot \frac{3}{(|\mathbb{F}|-1)/2} = \frac{48}{|\mathbb{F}|-1} \ . \tag{33}$$

As for the rightmost square submatrix of Z'_2, we reason about the rows, and consider the conditions that make them zero or a multiple of rows considered earlier.

- Rows 0 and 1 are sequences of powers of z^2 and z^{-2}. Both these rows are nonzero and they are not collinear unless $z^2 = 1$, which occurs with probabiliy $2/(|\mathbb{F}|-1)$.
- Rows 2, 3, and 4 are the Hadamard product of $\mathbf{r}^{(l)}_{[q-6:q-1]}$ with a vector of powers of z^2, z^{-2}, and γ. Considering z and γ fixed, the probability over random $\mathbf{r}^{(l)}_{[q-1]}, \mathbf{r}^{(l)}_{[q-2]}, \mathbf{r}^{(l)}_{[q-3]}$ that row 2 is in the span of rows 0 and 1, is at most $1/|\mathbb{F}|$. Likewise, the probability over random $\mathbf{r}^{(l)}_{[q-1]}, \mathbf{r}^{(l)}_{[q-2]}, \mathbf{r}^{(l)}_{[q-3]}, \mathbf{r}^{(l)}_{[q-4]}$ that row 3 is in the span of rows 0, 1, and 2 is at most $1/|\mathbb{F}|$. And likewise, the probability over random $\mathbf{r}^{(l)}_{[q-1]}, \mathbf{r}^{(l)}_{[q-2]}, \mathbf{r}^{(l)}_{[q-3]}, \mathbf{r}^{(l)}_{[q-4]}, \mathbf{r}^{(l)}_{[q-5]}$ that row 4 is in the span of rows 0, 1, 2, and 3, is at most $1/|\mathbb{F}|$.
- Row 5 contains terms that are linear in $\mathbf{r}^{(l)}_{[q-1]}, \ldots, \mathbf{r}^{(l)}_{[q-6]}$. The coefficient matrix operating on the $\mathbf{r}^{(l)}_{[q-1:q-6]}$ is given (via row-vector-matrix multiplication) by ΓZ_3, where Γ is the diagonal matrix with powers of γ on its diagonal, and where Z_3 is the bottom-right 6×6 Toeplitz matrix of Eqn. 32. Since γ is sampled to be invertible, Γ is invertible as well. The determinant of a 6×6 Toeplitz matrix is a degree 6 multivariate expression in the arguments. The determinant of this particular Toeplitz matrix is a nonzero polynomial of degree $21 + 12n + 12q$. Since z is sampled from $\mathbb{F}\backslash\{0\}$, and by the Schwartz-Zippel lemma, Z_3 is singular with probability bounded by $(21 + 12n + 12q)/(|\mathbb{F}| - 1)$. Assuming Z_3 is invertible, sampling row 5 uniformly at random is equivalent to sampling $\mathbf{r}^{(l)}_{[q-1]}$ through $\mathbf{r}^{(l)}_{[q-6]}$ uniformly at random. Consequently, the probability that row 5 lies in the span of rows 0 through 4 is $1/|\mathbb{F}|$.

By the union bound, we have

$$\Pr[\mathsf{det}(Z'_{2,[:,n+q-6:n+q-1]}) = 0] \leq \frac{27 + 12n + 12q}{|\mathbb{F}| - 1} \ . \tag{34}$$

Consequently, the statistical distance in distributions of the view of the verifier of authentic transcripts versus simulated transcripts, is bounded by $\frac{75+12n+12q}{|\mathbb{F}|-1}$. □

7 Comparison

We compare both variants of Claymore to some other Polynomial IOPs from the literature, namely Sonic, PLONK, Marlin, and Aurora. Of these Polynomial

IOPs, the first three give rise to SNARKs after cryptographic compilation. In contrast, Aurora gives rise to a proof system generating short proofs but whose verifier complexity is linear in the size of the witness. Importantly, Claymore is comparable to both types of proof system: with preprocessing, it gives rise to a SNARK; when preprocessing is omitted, the proofs remain short at the expense of linear verifier complexity.

Table 1 contains an overview of the comparison. It considers the following key performance indicators for Polynomial IOPs.

- The number of polynomials sent by I during the offline preprocessing phase. This number determines the size of the universal or structured reference strings. While this number contributes to the complexity of I, this complexity is generally speaking not a make or break factor.
- The number of polynomials sent by P during the online proving phase. This number contributes to the size of the proof and to the complexity of both P and V.
- The number of evaluations. This number contributes to the size of the proof, as well as indirectly to the complexity of P and V.
- The number of distinct points for evaluation. Some cryptographic compilers (*e.g.*, [6]) enable the merger of two polynomial evaluations provided that they are being evaluated in the same point. This number limits the number of times this optimization can be applied.
- The maximum degree of all polynomials. This number contributes to indexer and prover complexity in two ways. First, before cryptographic compilation, I and P operate on polynomials of this degree and their complexity is affected accordingly. The exception is if the polynomials are sparse, or otherwise exhibit a structure that enable fast computation. Second, some cryptographic compilers induce overheads that are superlinear in this degree.

Table 1. Comparison between Claymore and other Polynomial IOPs from the literature, with respect to key performance indicators.

	# polynomials offline / online	# evaluations	# distinct points	max. degree
Sonic [11]	$12M/3M+7$	$11M+3$	$9M+2$	$O(n)$
PLONK [8]	8 / 6	7	2	$12(n+a)$
Marlin [7]	9 / 12	18	3	$6k+6$
Aurora [4]	- / 7	8	2	$\max(m,n)$
DenseClaymore	1 / 4	18	8	$m(3n+1)-1$
SparseClaymore	8 / 10	45	21	$6K-1$

For Sonic, n refers to the number of multiplication gates. However, due to their technique for simulating bivariate polynomials, the addition gates have fan-in bounded by a parameter M. As a result of converting the original circuit

into one with this fan-in bound, a number of multiplication gates may have to be added, thus explaining the Landau notation.

For PLONK, n refers to the number of multiplication gates and a refers to the number of addition gates, all of which have fan-in 2. We note that there is a variant of PLONK with larger proofs and smaller prover time, which is not shown in the table.

Aurora does not have a preprocessing phase and as a result the verifier's complexity is linear in the number of nonzero elements in the matrices A, B, C from the R1CS tuple. Marlin uses the same mechanics but uses preprocessing to shrink the verifier's workload for the matrix multiplication; this technique requires 9 polynomials in the uniform or structured reference string (3 per matrix) and a few more in the online protocol. The parameter k denotes the largest number of nonzero elements of $\{A, B, C\}$.

Marlin, PLONK, and Aurora work in the Reed-Solomon codeword basis and crucially rely on the structure of the field or of its multiplicative group. In contrast, Sonic and Claymore work for any field.

8 Conclusion

The protocols proposed in this paper challenge the notion that the Reed-Solomon codeword basis is the appropriate basis for representing objects from the arithmetic constraint system in a Polynomial IOP. Instead, the monomial coefficient basis provides a natural and intuitive representation for these objects. In this basis, the native operations on polynomials are identifiable with the matrix operations in the arithmetic constraint system. Moreover, this basis does not impose any restrictions on the structure of the field. The resulting Polynomial IOP for arithmetic constraint systems outperforms similar constructions based on the Reed-Solomon codeword basis, at least as far as the number of polynomials in the transcript is concerned.

The modular approach followed in this paper admits a piece by piece presentation and analysis that benefits simplicity and accessibility. Nevertheless, some noteworthy optimizations violate the boundaries implicit in this modular structure. These optimizations are of independent interest as they may also apply elsewhere; perhaps they have straightforward analogues in the Reed-Solomon codeword domain.

In some cases it is possible to eliminate polynomials. In particular, when a polynomial is queried exactly twice and is involved in exactly two polynomial identities. By moving this polynomial to the left hand side, and equating the right hand sides, the polynomial identities are merged and the polynomial in question is eliminated, all without impacting soundness.

After unrolling a Polynomial IOP, InnerProduct subprotocols appear in great numbers and many places. They can all be batched. In addition to saving polynomials, this batching facilitates a simpler and more direct proof of zero-knowledge that would not be possible otherwise.

Batching may apply in more places still. For instance, the sparse MVP procedure benefits from two invocations of a subprotocol that establishes that a given vector is a Lagrange vector, and two more that another vector is a Vandermonde vector. The Lagrange and Vandermonde vector protocols can be merged in order to save polynomials. In fact, this merger extends to multivariate polynomials in more than two variables.

Concatenating the vectors of left and right wires saves one polynomial, but only if the Hadamard subprotocol can be made to work with the concatenated vector. In particular, this adaptation requires a shifting the protocol's second and third arguments. Performing this shift in either basis is possible, but this shift highlights an interesting difference. In the Reed-Solomon codeword basis, the query to the polynomial oracle is multiplied by a constant factor; in the monomial coefficient basis, however, it is the response that is multiplied by a factor that depends on the query.

Acknowledgements. Both authors are supported by the Nervos Foundation.

References

1. Ames, S., Hazay, C., Ishai, Y., Venkitasubramaniam, M.: Ligero: Lightweight Sublinear Arguments Without a Trusted Setup. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017. pp. 2087–2104. ACM (2017), https://doi.org/10.1145/3133956.3134104
2. Bellare, M., Goldreich, O.: On defining proofs of knowledge. In: Brickell, E.F. (ed.) CRYPTO 1992s. Lecture Notes in Computer Science, vol. 740, pp. 390–420. Springer (1992), https://doi.org/10.1007/3-540-48071-4_28
3. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable zero knowledge with no trusted setup. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part III. Lecture Notes in Computer Science, vol. 11694, pp. 701–732. Springer (2019). https://doi.org/10.1007/978-3-030-26954-8_23
4. Ben-Sasson, E., Chiesa, A., Riabzev, M., Spooner, N., Virza, M., Ward, N.P.: Aurora: Transparent Succinct Arguments for R1CS. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019 , Part I. Lecture Notes in Computer Science, vol. 11476, pp. 103–128. Springer (2019), https://doi.org/10.1007/978-3-030-17653-2_4
5. Bootle, J., Cerulli, A., Chaidos, P., Groth, J., Petit, C.: Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. In: Fischlin, M., Coron, J. (eds.) EUROCRYPT 2016, Part II. Lecture Notes in Computer Science, vol. 9666, pp. 327–357. Springer (2016), https://doi.org/10.1007/978-3-662-49896-5_12
6. Bünz, B., Fisch, B., Szepieniec, A.: Transparent SNARKs from DARK Compilers. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020 Part I. Lecture Notes in Computer Science, vol. 12105, pp. 677–706. Springer (2020), https://eprint.iacr.org/2019/1229.pdf
7. Chiesa, A., Hu, Y., Maller, M., Mishra, P., Vesely, N., Ward, N.P.: Marlin: Preprocessing zksnarks with universal and updatable SRS. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020 Part I. Lecture Notes in Computer Science, vol. 12105, pp. 738–768. Springer (2020), https://eprint.iacr.org/2019/1047.pdf

8. Gabizon, A., Williamson, Z.J., Ciobotaru, O.: PLONK: permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. IACR Cryptology ePrint Archive **2019**, 953 (2019), https://eprint.iacr.org/2019/953
9. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems (extended abstract). In: Sedgewick, R. (ed.) ACM STOC. pp. 291–304. ACM (1985). https://doi.org/10.1145/22145.22178
10. Kate, A., Zaverucha, G.M., Goldberg, I.: Constant-size commitments to polynomials and their applications. In: Abe, M. (ed.) ASIACRYPT 2010. Lecture Notes in Computer Science, vol. 6477, pp. 177–194. Springer (2010), https://doi.org/10.1007/978-3-642-17373-8_11
11. Maller, M., Bowe, S., Kohlweiss, M., Meiklejohn, S.: Sonic: Zero-knowledge snarks from linear-size universal and updatable structured reference strings. In: Cavallaro, L., Kinder, J., Wang, X., Katz, J. (eds.) ACM CCS 2019. pp. 2111–2128. ACM (2019), https://eprint.iacr.org/2019/099.pdf

A Definitional Equivalence: Polynomial IOPs with and without Individual Degree Bounds

Definition 4 presents one possible definition for the notion that is Polynomial IOP, namely where there is one degree bound d that applies to all polynomials. However, all the protocols presented in this paper provide individual degree bounds for each polynomial, corresponding to another possible definition. The discussion following Definition 4 argues that no generality is lost by switching between the two options. We now formalize this intuition.

Definition 6 (Polynomial IOP with Individual Degree Bounds). *Let $\mathcal{R}$ be an indexed relation with corresponding indexed language $\mathcal{L}(\mathcal{R})$, $\mathbb{F}$ some finite field, and $\delta : \mathbb{N} \to \mathbb{N}$ a function that maps polynomial indices to their respective degree bounds. A* Polynomial IOP for $\mathcal{R}$ with individual degree bounds δ *is a pair of interactive machines* (P, V)*, satisfying the following description.*

- (P, V) *is an interactive proof for $\mathcal{L}(\mathcal{R})$ with r rounds, and with soundness error σ.*
- P *sends polynomials $f_i(X) \in \mathbb{F}[X]$ of degree at most $\delta(i)$ to V.*
- V *is an oracle machine with access to a list of oracles, which contains one oracle for each polynomial it has received from the prover.*
- *When an oracle associated with a polynomial $f_i(X)$ is queried on a point $z_j \in \mathbb{F}$, the oracle responds with the value $f_i(z_j)$.*
- V *sends challenges $\alpha_k \in \mathbb{F}$ to P.*
- V *is public coin.*

Showing the equivalence in one direction turns out to be trivial. The next lemma establishes that a Polynomial IOP with individual degree bounds (6) can simulate a Polynomial IOP with a single degree bound (4).

Lemma 1 ((4) $\Rightarrow$ (6)). *Let (P, V) be a Polynomial IOP with degree bound d for a relation $\mathcal{R}$ with soundness error σ according to Definition 4. Then (P, V) is*

a Polynomial IOP with individual degree bounds $\delta(i) = \mathsf{d}$ for $\mathcal{R}$ with soundness error σ according to Definition 6.

Proof. The difference between the two definitions is that the ith polynomial $f_i(X)$ is guaranteed to be of degree at most $\delta(i)$ rather than d. In this particular case, $\delta(i) = \mathsf{d}$, so there is no difference at all. □

The other direction of the equivalence is more involved as it requires a compiler and comes with a (negligible) soundness degradation. Let $\mathsf{C}(\mathsf{P})$ and $\mathsf{C}(\mathsf{V})$ denote the compiled prover and verifier, respectively. The compiler starts by computing $\mathsf{d} = \mathsf{max}_i \delta(i)$. The compiled prover and verifier then mimick the original prover and verifier, except for the following changes:

- Whenever P sends polynomial $f_i(X)$ whose degree is bounded by $\delta(i)$, $\mathsf{C}(\mathsf{P})$ sends polynomial $f_i^\star(X) = X^{\mathsf{d}-\delta(i)} \cdot f_i(X)$.
- Whenever V queries a polynomial oracle $[f_i(X)]$ in a point $z_j \neq 0$ to obtain value $y_j = f_i(z_j)$, $\mathsf{C}(\mathsf{V})$ queries $[f_i^\star(X)]$ in z_j, obtains response $y_j^\star = f_i^\star(z_j)$, and proceeds as V would with value $y_j = y_j^\star / z_j^{\mathsf{d}-\delta(i)}$.

Lemma 2 ((6) ⇒ (4)). *Let (P, V) be a Polynomial IOP with individual degree bounds $\delta(i)$ for a relation $\mathcal{R}$ with soundness error σ and q queries to polynomials in points from $\mathbb{F}\backslash\{0\}$ according to Definition 6. Then $(\mathsf{C}(\mathsf{P}), \mathsf{C}(\mathsf{V}))$ is a Polynomial IOP with degree bounds $\mathsf{d} = \mathsf{max}_i \delta(i)$ for $\mathcal{R}$ with soundness error at most $\sigma + q \cdot \frac{\mathsf{max}_i \delta(i) - \mathsf{min}_i \delta(i)}{|\mathbb{F}|-1}$ and q queries according to Definition 4.*

Proof. Completeness follows from construction. All polynomials are bounded in degree by d, and $\mathsf{C}(V)$ obtains values $y_j = f_i^\star(z_j)/z_j^{\mathsf{d}-\delta(i)} = f_i(z_j)$, *i.e.*, indentical to what V obtains.

In terms of soundness, $\mathsf{C}(\mathsf{V})$ implies that V accepts a false instance or that for some polynomial $[f_i(X)]$ and query z_j, $X^{\mathsf{d}-\delta(i)} \cdot f_i(X) \neq f_i^\star(X)$ but $f_i(z_j) = f_i^\star(z_j)/z_j^{\mathsf{d}-\delta(i)}$. Any one of these latter events occurse with probability at most $\frac{\mathsf{d}-\mathsf{min}_i \delta(i)}{|\mathbb{F}|-1}$ due to Schwartz-Zippel. Since there are q queries where this might occur, the soundness error of $(\mathsf{C}(\mathsf{P}), \mathsf{C}(\mathsf{V}))$ is bounded by $\sigma + q \cdot \frac{\mathsf{max}_i \delta(i) - \mathsf{min}_i \delta(i)}{|\mathbb{F}|-1}$. □

B Sparse Matrix-Vector Product

B.1 Formal Presentation

The formal presentation of the sparse matrix-vector multiplication protocol, which follows, builds the protocol hierarchically. We therefore follow the high-level overview but in reverse order.

Vandermonde Vector. The VandermondeVector protocol realizes the following relation

$$\mathcal{R}_{\text{vv}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (H, K, \varphi(h), \{a_k\}_{k=0}^{K-1}) \\ \mathbb{x} = (z, [f_{\hat{\mathbf{z}}}(X)]) \\ \mathbb{w} = f_{\hat{\mathbf{z}}}(X) \\ R = \begin{pmatrix} \varphi(a_0)^0 & \varphi(a_1)^0 & \cdots \\ \varphi(a_0)^1 & \varphi(a_1)^1 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \\ f_{\hat{\mathbf{z}}}(X) = \sum_{i=0}^{H-1} \hat{z}_i X^i \\ \mathbf{z} = (1\,,\, z\,,\, z^2\,,\, \cdots\,,\, z^{K-1})^{\mathsf{T}} \\ \hat{\mathbf{z}} = R\mathbf{z} \end{array} \right\} . \tag{35}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{vv}})$
inputs: $\mathbb{i}$: $H, K, \varphi(h), \{a_k\}_{k=0}^{K-1}$
$\mathbb{x}$: $z, [f_{\hat{\mathbf{z}}}(X)]$
$\mathbb{w}$: $f_{\hat{\mathbf{z}}}(X)$
// pre-processing
begin
  I computes $f_{\varphi(a_k)}(X) \leftarrow \sum_{k=0}^{K-1} \varphi(a_k) X^k$ and $f_{\varphi(a_k)^H}(X) \leftarrow \sum_{k=0}^{K-1} \varphi(a_k)^H X^k$
  I sends $f_{\varphi(a_k)}(X)$ and $f_{\varphi(a_k)^H}(X)$, both of degree at most $K-1$, to P and V
// online
begin
  V samples $\delta \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and sends δ to P
  P computes $\boldsymbol{\delta} \leftarrow (\delta^0, \delta^1, \ldots, \delta^{H-1})^{\mathsf{T}}$, $\hat{\boldsymbol{\delta}} \leftarrow R^{\mathsf{T}}\boldsymbol{\delta}$, and $f_{\hat{\boldsymbol{\delta}}}(X) \leftarrow \sum_{i=0}^{K-1} \hat{\delta}_i X^i$
  P sends $f_{\hat{\boldsymbol{\delta}}}(X)$ of degree at most $K-1$ to V
  V queries $[f_{\hat{\boldsymbol{\delta}}}(X)]$ in z and receives $y_0 = f_{\hat{\boldsymbol{\delta}}}(z)$
  V queries $[f_{\hat{\mathbf{z}}}(X)]$ in δ and receives $y_1 = f_{\hat{\mathbf{z}}}(\delta)$
  V checks $y_1 \stackrel{?}{=} y_0$
  P and V run Hadamard with $\mathbb{i}^{(1)} = H - 1$,
   $\mathbb{x}^{(1)} = ([f_{\hat{\boldsymbol{\delta}}}(X)], [\delta \cdot f_{\varphi(a_k)}(X) - f_I(X)], [\delta \cdot f_{\varphi(a_k)^H}(X) - f_I(X)])$,
   $\mathbb{w}^{(1)} = (f_{\hat{\boldsymbol{\delta}}}(X), \delta^H \cdot f_{\varphi(a_k)}(X) - f_I(X), \delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X))$, where
   V simulates $[\delta \cdot f_{\varphi(a_k)}(X) - f_I(X)], [\delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X)]$ using the oracles $[f_{\varphi(a_k)}(X)], [f_{\varphi(a_k)^H}(X)]$ and the known scalar δ, in combination with computing $f_I(X) = \sum_{k=0}^{K-1} X^k$ locally

Protocol 8: VandermondeVector

Theorem 8 (Security of VandermondeVector**).** *Protocol* VandermondeVector *is a Polynomial IOP for* $\mathcal{R}_{\text{vv}}$ *with completeness and soundness with soundness error* $\sigma \leq \frac{H+5K-5}{|\mathbb{F}|-1}$.

Proof. Consider the following sequences of equations.

$$\hat{\mathbf{z}} = R\mathbf{z} \tag{36}$$

$$\boldsymbol{\delta}^{\mathsf{T}}\hat{\mathbf{z}} = \boldsymbol{\delta}^{\mathsf{T}} R\mathbf{z} \tag{37}$$

$$f_{\hat{\mathbf{z}}}(\delta) = f_{\hat{\boldsymbol{\delta}}}(z) \tag{38}$$

$$y_1 = y_0 \ , \tag{39}$$

and

$$\forall k \in \{0, \ldots, K-1\} \, . \left(\sum_{h=0}^{H-1} (\delta \cdot \varphi(k))^h \right) \cdot (1 - \delta \cdot \varphi(a_k)) = 1 - (\delta \cdot \varphi(a_k))^H \tag{40}$$

$$\left(\boldsymbol{\delta}^{\mathsf{T}} R\right) \circ (1 - \delta \cdot \varphi(a_k))_{k=0}^{K-1} = \left(1 - (\delta \cdot \varphi(a_k))^H\right)_{k=0}^{K-1} \tag{41}$$

$$f_{\hat{\boldsymbol{\delta}}}(X) \circ \left(\delta \cdot f_{\varphi(a_k)}(X) - f_I(X)\right) = \delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X) \tag{42}$$

$$(\mathbb{i}^{(1)}, \mathbb{x}^{(1)}) = \tag{43}$$

$$(K-1, [f_{\hat{\boldsymbol{\delta}}}(X)], [\delta \cdot f_{\varphi(a_k)}(X) - f_I(X)], [\delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X)]) \in \mathcal{L}(\mathcal{R}_{\text{hadamard}}) \ .$$

Completeness follows from the sequences of implications a) (36) $\Rightarrow$ (37) $\Leftrightarrow$ (38) $\Leftrightarrow$ (39), and b) (40) $\Leftrightarrow$ (41) $\Leftrightarrow$ (42) $\Rightarrow$ (43). Sequence (a) holds for any matrix R. Sequence (b) starts with the equation for a geometric sum derived from the matrix R as defined as in Eqn. 27.

For soundness, consider when the reverse implications fail. There are two such cases:

- (36) $\not\Leftarrow$ (37). By the Schwartz-Zippel lemma, the probability of this event is bounded by $\frac{H-1}{|\mathbb{F}|-1}$.
- (42) $\not\Leftarrow$ (43). The probability of this event is captured by the soundness error of $\mathsf{Hadamard}$, $\sigma_{\mathsf{Hadamard}} \leq \frac{5K-4}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of $\mathsf{VandermondeVector}$ is bounded by $\sigma \leq \frac{H+5K-5}{|\mathbb{F}|-1}$. □

Lagrange Vector. The $\mathsf{LagrangeVector}$ protocol realizes the following relation

$$\mathcal{R}_{\text{lv}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (H, \varphi(h)) \\ \mathbb{x} = (x, [f_{\hat{\mathbf{x}}}(X)]) \\ \mathbb{w} = f_{\hat{\mathbf{x}}}(X) \\ L = \begin{pmatrix} \mathcal{L}_{\varphi(0),0} & \mathcal{L}_{\varphi(0),1} & \cdots \\ \mathcal{L}_{\varphi(1),0} & \mathcal{L}_{\varphi(1),1} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \\ f_{\hat{\mathbf{x}}}(X) = \sum_{i=0}^{H-1} \hat{x}_i X^i \\ \mathbf{x} = (1 \, , \, x \, , \, x^2 \, , \, \cdots \, , \, x^{H-1})^{\mathsf{T}} \\ \hat{\mathbf{x}} = \mathbf{x}^{\mathsf{T}} L \end{array} \right\} \ . \tag{44}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{lv}})$
inputs: $\mathbb{i}$: $H, \varphi(h)$
$\mathbb{x}$: $x, [f_{\hat{\mathbf{x}}}(X)]$
$\mathbb{w}$: $f_{\hat{\mathbf{x}}}(X)$
// pre-processing
begin
I computes $f_{\varphi(h)}(X) \leftarrow \sum_{h=0}^{H-1} \varphi(h) X^h$, $Z_{\mathcal{H}}(X) \leftarrow \prod_{h=0}^{H-1}(X - \varphi(h))$ and $f_{\mathcal{H}}(X) \leftarrow \sum_{h=0}^{H-1} \left(\prod_{i \in \{0 \ldots H-1\} \setminus \{h\}} (\varphi(h) - \varphi(i))\right)^{-1} \cdot X^h$
I sends $f_{\varphi(h)}(X)$, $f_{\mathcal{H}}(X)$, both of degree at most $H-1$, and $Z_{\mathcal{H}}(X)$ of degree at most H, to P and V
// online
begin
V samples $\gamma \xleftarrow{\$} \mathbb{F} \setminus \{0\}$ and sends γ to P
P computes $\boldsymbol{\gamma} \leftarrow (\gamma^0, \gamma^1, \ldots, \gamma^{H-1})^{\mathsf{T}}$, $\hat{\boldsymbol{\gamma}} \leftarrow L\boldsymbol{\gamma}$, and $f_{\hat{\boldsymbol{\gamma}}}(X) \leftarrow \sum_{i=0}^{H-1} \hat{\gamma}_i X^i$
P sends $f_{\hat{\boldsymbol{\gamma}}}(X)$ of degree at most $H-1$ to V
V queries $[f_{\hat{\boldsymbol{\gamma}}}(X)]$ in x and receives $y_0 = f_{\hat{\boldsymbol{\gamma}}}(x)$
V queries $[f_{\hat{\mathbf{x}}}(X)]$ in γ and receives $y_1 = f_{\hat{\mathbf{x}}}(\gamma)$
V checks $y_1 \stackrel{?}{=} y_0$
V queries $[Z_{\mathcal{H}}(X)]$ in γ and receives $u = Z_{\mathcal{H}}(\gamma)$
P and V run Hadamard with $\mathbb{i}^{(1)} = H - 1$,
$\mathbb{x}^{(1)} = ([f_{\hat{\boldsymbol{\gamma}}}(X)], [\gamma f_I(X) - f_{\varphi(h)}(X)], [u f_{\mathcal{H}}(X)])$,
$\mathbb{w}^{(1)} = (f_{\hat{\boldsymbol{\gamma}}}(X), \gamma f_I(X) - f_{\varphi(h)}(X), u f_{\mathcal{H}}(X))$, where V simulates $[\gamma f_I(X) - f_{\varphi(h)}(X)], [u f_{\mathcal{H}}(X)]$ using the oracles $[f_{\varphi(h)}(X)], [f_{\mathcal{H}}(X)]$ and the known scalar γ, in combination with computing $f_I(X) = \sum_{h=0}^{H-1} X^h$ locally

Protocol 9: LagrangeVector

Theorem 9 (Security of LagrangeVector). *Protocol* LagrangeVector *is a Polynomial IOP for* $\mathcal{R}_{\text{lv}}$ *with completeness and soundness with soundness error* $\sigma \leq \frac{6H-5}{|\mathbb{F}|-1}$.

Proof. Consider the following sequences of equations.

$$\hat{\mathbf{x}}^{\mathsf{T}} = \mathbf{x}^{\mathsf{T}} L \tag{45}$$

$$\hat{\mathbf{x}}^{\mathsf{T}} \boldsymbol{\gamma} = \mathbf{x}^{\mathsf{T}} L \boldsymbol{\gamma} \tag{46}$$

$$f_{\hat{\mathbf{x}}}(\gamma) = f_{\hat{\boldsymbol{\gamma}}}(x) \tag{47}$$

$$y_1 = y_0 \ , \tag{48}$$

and

$$\forall h \in \{0, \ldots, H-1\} \,.\, \mathcal{L}_h(\gamma) = \prod_{\substack{i=0 \\ i \neq h}}^{H-1} \frac{\gamma - \varphi(i)}{\varphi(h) - \varphi(i)} \tag{49}$$

$$\forall h \in \{0, \ldots, H-1\} \,.\, \mathcal{L}_h(\gamma) \cdot (\gamma - \varphi(h)) = \frac{Z_{\mathcal{H}}(\gamma)}{\prod_{\substack{i=0 \\ i \neq h}}^{H-1} (\varphi(h) - \varphi(i))} \tag{50}$$

$$(L\boldsymbol{\gamma}) \circ (\gamma - \varphi(h))_{h=0}^{H-1} = Z_{\mathcal{H}}(\gamma) \left(\left(\prod_{i \in \{0 \ldots H-1\} \setminus \{h\}} (\varphi(h) - \varphi(i)) \right)^{-1} \right)_{h=0}^{H-1} \tag{51}$$

$$f_{\hat{\boldsymbol{\gamma}}}(X) \circ (\gamma f_I(X) - f_{\varphi}(X)) = u f_{\mathcal{H}}(X) \tag{52}$$

$$(\mathbb{i}^{(1)}, \mathbb{X}^{(1)}) = \tag{53}$$
$$(H-1, [f_{\hat{\boldsymbol{\gamma}}}(X)], [\gamma f_I(X) - f_{\varphi(h)}(X)], [u f_{\mathcal{H}}(X)]) \in \mathcal{L}(\mathcal{R}_{\text{hadamard}}) \ .$$

Completeness follows from the sequences of implications a) (45) $\Rightarrow$ (46) $\Leftrightarrow$ (47) $\Leftrightarrow$ (48), and b) (49) $\Leftrightarrow$ (50) $\Leftrightarrow$ (51) $\Leftrightarrow$ (52) $\Rightarrow$ (53). Sequence (a) holds for any matrix L. Sequence (b) starts with the definition of Lagrange basis polynomials, and holds when the rows of L are exactly the coefficient vectors of the Lagrange basis polynomials. Recall that Lagrange basis polynomial indexed by h takes the value 1 in $\varphi(h)$ and 0 in all other points of $\mathcal{H}$.

For soundness, consider when the reverse implications fail. There are two such cases:

- (45) $\not\Leftarrow$ (46). By the Schwartz-Zippel lemma, the probability of this event is bounded by $\frac{H-1}{|\mathbb{F}|-1}$.
- (52) $\not\Leftarrow$ (53). The probability of this event is captured by the soundness error of Hadamard, $\sigma_{\text{Hadamard}} \leq \frac{5H-4}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of LagrangeVector is bounded by $\sigma \leq \frac{6H-5}{|\mathbb{F}|-1}$. □

Sparse Univariate Polynomial Evaluation. In terms of sparse univariate polynomial evaluation, we actually achieve something more generic. Let $f(X) = \sum_{k=0}^{K-1} X^{a_k}$. The next protocol establishes that $f_z(X) = \sum_{k=0}^{K-1} z^{a_k} X^k$ is indeed the polynomial whose vector of coefficients corresponds to the monomials of $f(X)$ when evaluated in z. By evaluating $f_z(X)$ in $X = 1$, one obtains the evaluation $f(z)$.

The protocol SparseMonomialVector realizes the following relation.

$$\mathcal{R}_{\text{smv}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (H, K, \{a_k\}_{k=0}^{K-1}) \\ \mathbb{x} = (z, [f_z(X)]) \\ \mathbb{w} = (f_z(X)) \\ f_z(X) = \sum_{k=0}^{K-1} z^{a_k} X^k \\ H = \max_k a_k \end{array} \right\} \tag{54}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{smv}})$
inputs: $\mathbb{i}$: $H, K, \{a_k\}_{k=0}^{K-1}$
$\mathbb{x}$: $z, [f_z(X)]$
$\mathbb{w}$: $f_z(X)$
// pre-processing
begin
- I selects any mapping $\varphi : \mathbb{N} \to \mathbb{F}$ such that $\{0, \ldots, H-1\}$ are mapped to distinct elements
- I runs VandermondeVector.I with $\mathbb{i}^{(1)} = (H, K, \varphi(h), \{a_k\}_{k=0}^{K-1})$
- I runs LagrangeVector.I with $\mathbb{i}^{(2)} = (H, \varphi(h))$

// online
begin
- P computes $f_{\hat{\mathbf{z}}}(X) = \sum_{h=0}^{H-1} z^h \mathcal{L}_h(X)$ where $\mathcal{L}_h(X)$ is the unique monic polynomial that evaluates to 1 in $\varphi(h)$ and to 0 in all other points of $\mathcal{H}$
- P sends $f_{\hat{\mathbf{z}}}(X)$ of degree at most $H-1$ to V
- P and V run LagrangeVector with $\mathbb{i}^{(2)} = (H, \varphi(h))$, $\mathbb{x}^{(2)} = (z, [f_{\hat{\mathbf{z}}}(X)])$, and $\mathbb{w}^{(2)} = f_{\hat{\mathbf{z}}}(X)$
- V samples $y \xleftarrow{\$} \mathbb{F} \backslash \{0\}$ and sends y to P
- V queries $[f_z(X)]$ in y and receives $x = f_z(y)$
- P computes $f_{\hat{\mathbf{y}}}(X) \leftarrow \sum_{h=0}^{H-1} \left(\sum_{k=0}^{K-1} \varphi(a_k)^h y^h \right) X^h$, whose coefficient vector corresponds to $R\mathbf{y}$ with $\mathbf{y} = (1, y, \ldots, y^{K-1})^\intercal \in \mathbb{F}^K$
- P sends $f_{\hat{\mathbf{y}}}(X)$ of degree at most $H-1$ to V
- P and V run VandermondeVector with $\mathbb{i}^{(1)} = (H, K, \varphi(h), \{a_k\}_{k=0}^{K-1})$, $\mathbb{x}^{(1)} = (y, [f_{\hat{\mathbf{y}}}(X)])$, and $\mathbb{w}^{(1)} = f_{\hat{\mathbf{y}}}(X)$
- P and V run InnerProduct with $\mathbb{i}^{(3)} = H - 1$, $\mathbb{x}^{(3)} = ([f_{\hat{\mathbf{z}}}(X)], [f_{\hat{\mathbf{y}}}(X)], x)$, and $\mathbb{w}^{(3)} = (f_{\hat{\mathbf{z}}}(X), f_{\hat{\mathbf{y}}}(X))$

Protocol 10: SparseMonomialVector

Theorem 10. *(Security of* SparseMonomialVector*) Protocol* SparseMonomialVector *is a Polynomial IOP for* $\mathcal{R}_{\text{smv}}$ *with completeness and soundness with soundness error* $\sigma \leq \frac{11H+6K-14}{|\mathbb{F}|-1}$.

Proof. Consider the following sequence of equations.

$$f_z(X) = \sum_{k=0}^{K-1} z^{a_k} X^k \tag{55}$$

$$f_z(y) = \sum_{k=0}^{K-1} z^{a_k} y^k \tag{56}$$

$$f_z(y) = \mathbf{z}^\mathsf{T} B \mathbf{y} \tag{57}$$

$$f_z(y) = \mathbf{z}^\mathsf{T} L R \mathbf{y} \tag{58}$$

$$f_z(y) = \hat{\mathbf{z}}^\mathsf{T} R \mathbf{y} \tag{59}$$

$$f_z(y) = \hat{\mathbf{z}}^\mathsf{T} \hat{\mathbf{y}} \tag{60}$$

$$(\mathbb{i}, \mathbb{x}) = (H-1, ([f_{\hat{\mathbf{z}}}(X)], [f_{\hat{\mathbf{y}}}(X)], x)) \in \mathcal{R}_{\text{ip}} \tag{61}$$

In these formulae, we define $\hat{\mathbf{z}}$ and $\hat{\mathbf{y}}$ as the vectors of coefficients of $f_{\hat{\mathbf{z}}}(X)$ and $f_{\hat{\mathbf{y}}}(X)$, respectively.

Completeness follows from the sequence of implications (55) $\Rightarrow$ (56) $\Leftrightarrow$ (57) $\Leftrightarrow$ (58) $\Rightarrow$ (59) $\Rightarrow$ (60) $\Rightarrow$ (61). For soundness, consider when the reverse implications fail.

- (55) $\not\Leftarrow$ (56). This event happens with probability at most $\frac{K-1}{|\mathbb{F}|-1}$ due to the Schwartz-Zippel lemma.
- (58) $\not\Leftarrow$ (59). This event implies that LagrangeVector succeeded despite being run on a false instance. This happens with probability at most equal to the soundness error of that protocol, $\sigma_{\mathsf{LagrangeVector}} \leq \frac{6H-5}{|\mathbb{F}|-1}$.
- (59) $\not\Leftarrow$ (60). This event implies that VandermondeVector succeeded despite being run on a false instance. This happens with probability at most equal to the soundness error of that protocol, $\sigma_{\mathsf{VandermondeVector}} \leq \frac{H+5K-5}{|\mathbb{F}|-1}$.
- (60) $\not\Leftarrow$ (61). This event implies that InnerProduct succeeded despite being run on a false instance. This happens with probability at most equal to the soundness error of that protocol, $\sigma_{\mathsf{InnerProduct}} \leq \frac{4H-3}{|\mathbb{F}|-1}$.

By the Union Bound, the probability that any one of these events occurs is bounded by $\sigma \leq \frac{11H+6K-14}{|\mathbb{F}|-1}$. □

An important class of sparse univariate polynomials are those that represent permutation matrices. As a consequence, protocol SparseMonomialVector can be used to establish that two polynomials have the same coefficients, except permuted according to a committed permutation. We omit the details of this digression.

Sparse Bivariate Polynomial Evaluation. The relation realized by the protocol SparseBiEval is given as follows.

$$\mathcal{R}_{\text{sbe}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k=0}^{K-1}) \\ \mathbb{x} = (u, v, w) \\ \mathbb{w} = \varnothing \\ H = \max(\max_k\{a_k\}, \max_k\{b_k\}) \\ f(X,Y) = \sum_{k=0}^{K-1} c_k X^{a_k} Y^{b_k} \\ f(u,v) = w \end{array} \right\} \tag{62}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{sbe}})$
inputs: $\mathbb{i}$: $H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k=0}^{K-1}$
$\mathbb{x}$: u, v, w
$\mathbb{w}$: $\varnothing$

// pre-processing
begin
- I selects any mapping $\varphi : \mathbb{N} \to \mathbb{F}$ such that $\{0, \ldots, H-1\}$ are mapped to distinct elements
- I runs SparseMonomialVector.I with $\mathbb{i}^{(1)} = (H, K, \{a_k\}_{k=0}^{K-1})$
- I runs SparseMonomialVector.I with $\mathbb{i}^{(2)} = (H, K, \{b_k\}_{k=0}^{K-1})$
- I computes $f_c(X) \leftarrow \sum_{k=0}^{K-1} c_k X^k$
- I sends $f_c(X)$ of degree at most $K-1$ to P and V

// online
begin
- P computes $f_u(X) \leftarrow \sum_{k=0}^{K-1} u^{a_k} X^k$, $f_v(X) \leftarrow \sum_{k=0}^{K-1} v^{b_k} X^k$, and $f_{uv}(X) \leftarrow \sum_{k=0}^{K-1} u^{a_k} v^{b_k} X^k$
- P sends $f_u(X)$, $f_v(X)$, and $f_{uv}(X)$, all of degree at most $K-1$, to V
- P and V run SparseMonomialVector with $\mathbb{i}^{(1)} = (H, K, \{a_k\}_{k=0}^{K-1})$, $\mathbb{x}^{(1)} = (u, [f_u(X)])$, and $\mathbb{w}^{(1)} = f_u(X)$
- P and V run SparseMonomialVector with $\mathbb{i}^{(2)} = (H, K, \{b_k\}_{k=0}^{K-1})$, $\mathbb{x}^{(2)} = (v, [f_v(X)])$, and $\mathbb{w}^{(2)} = f_v(X)$
- P and V run Hadamard with $\mathbb{i}^{(3)} = K-1$, $\mathbb{x}^{(3)} = ([f_u(X)], [f_v(X)], [f_{uv}(X)])$, and $\mathbb{w}^{(3)} = (f_u(X), f_v(X), f_{uv}(X))$
- P and V run InnerProduct with $\mathbb{i}^{(4)} = K-1$, $\mathbb{x}^{(4)} = ([f_{uv}(X)], [f_c(X)], w)$, and $\mathbb{w}^{(4)} = (f_{uv}(X), f_c(X))$

Protocol 11: SparseBiEval

Theorem 11 (Security of SparseBiEval). *Protocol* SparseBiEval *is a Polynomial IOP for* $\mathcal{R}_{\text{sbi}}$ *with completeness and soundness with soundness error* $\sigma = \frac{22H+21K-35}{|\mathbb{F}|-1}$.

Proof. Consider the following sequence of equations.

$$f(u,v) = w \tag{63}$$

$$\sum_{k=0}^{K-1} c_k u^{a_k} v^{b_k} = w \tag{64}$$

$$\mathsf{coeffs}(f_{uv}(X)) \cdot \mathsf{coeffs}(f_c(X)) = w \tag{65}$$

$$(\mathsf{coeffs}(f_u(X)) \circ \mathsf{coeffs}(f_v(X))) \cdot \mathsf{coeffs}(f_c(X)) = w \tag{66}$$

$$(\mathsf{coeffs}(f_u(X)) \circ \mathsf{coeffs}(f_v(X))) \cdot (c_k)_{k=0}^{K-1} = w \tag{67}$$

$$\left(\mathsf{coeffs}(f_u(X)) \circ \left(v^{b_k}\right)_{k=0}^{K-1}\right) \cdot (c_k)_{k=0}^{K-1} = w \tag{68}$$

$$\left((u^{a_k})_{k=0}^{K-1} \circ \left(v^{b_k}\right)_{k=0}^{K-1}\right) \cdot (c_k)_{k=0}^{K-1} = w \tag{69}$$

Completeness follows from the sequence of implications (63) $\Leftrightarrow$ (64) $\Rightarrow$ (65) $\Rightarrow$ (66) $\Leftrightarrow$ (67) $\Rightarrow$ (68) $\Rightarrow$ (69). For soundness, consider when the reverse implications fail.

- (64) $\not\Leftarrow$ (65). This event happens with probability at most equal to the soundness error of $\mathsf{InnerProduct}$, $\sigma_{\mathsf{InnerProduct}} \leq \frac{4K-3}{|\mathbb{F}|-1}$.
- (65) $\not\Leftarrow$ (66). This event happens with probability at most equal to the soundness error of $\mathsf{Hadamard}$, $\sigma_{\mathsf{Hadamard}} \leq \frac{5K-4}{|\mathbb{F}|-1}$.
- (67) $\not\Leftarrow$ (68). This event happens with probability at most equal to the soundness error of $\mathsf{SparseMonomialVector}$, $\sigma_{\mathsf{SparseMonomialVector}} \leq \frac{11H+6K-14}{|\mathbb{F}|-1}$.
- (68) $\not\Leftarrow$ (69). This event happens with probability at most equal to the soundness error of $\mathsf{SparseMonomialVector}$, $\sigma_{\mathsf{SparseMonomialVector}} \leq \frac{11H+6K-14}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of $\mathsf{SparseBiEval}$ is bounded by $\sigma \leq \frac{22H+21K-35}{|\mathbb{F}|-1}$. □

Sparse Matrix-Vector Product. The relation that is realized by the sparse matrix-vector product protocol is essentially the same as the one realized by the regular (dense) matrix-vector product protocol. However, we restate this relation in such a way so as to stress that the matrix is represented sparsely, *i.e.*, as a list of position-coefficient tuples rather than an array of coefficients.

$$\mathcal{R}_{\text{smvp}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (m, n, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k=0}^{K-1}) \\ \mathbb{x} = ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)]) \\ \mathbb{w} = (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X)) \\ f_{\boldsymbol{a}}(X) = \sum_{i=0}^{n-1} \boldsymbol{a}_{[i]} X^i \text{ for some } \boldsymbol{a} \in \mathbb{F}^n \\ f_{\boldsymbol{b}}(X) = \sum_{i=0}^{m-1} \boldsymbol{b}_{[i]} X^i \text{ for some } \boldsymbol{b} \in \mathbb{F}^m \\ M = \sum_{k=0}^{K-1} c_k \mathbf{e}_{a_k}^{\mathsf{T}} \mathbf{e}_{b_k} \\ \boldsymbol{b} = M\boldsymbol{a} \end{array} \right\} . \tag{70}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{smvp}})$
inputs: $\mathbb{i}$: $m, n, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k=0}^{K-1}$
$\mathbb{x}$: $[f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)]$
$\mathbb{w}$: $f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X)$
// pre-processing
begin
I computes $H \leftarrow \max(m, n)$
I runs SparseBiEval.I with $\mathbb{i}^{(1)} = (H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k-1}^{K-1})$
// online
begin
V samples $\alpha \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and sends α to P
P computes $f_{\boldsymbol{\alpha}^\intercal M}(X) \leftarrow \sum_{k=0}^{K-1} c_k \alpha^{a_k} X^{b_k}$
P sends $f_{\boldsymbol{\alpha}^\intercal M}(X)$ of degree at most $n-1$ to V
P computes $s \leftarrow f_{\boldsymbol{b}}(\alpha)$
V queries $[f_{\boldsymbol{b}}(X)]$ in α and receives $s = f_{\boldsymbol{b}}(\alpha)$
P and V run InnerProduct with $\mathbb{i}^{(2)} = n-1$, $\mathbb{x}^{(2)} = ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{\alpha}^\intercal M}(X)], s)$, and $\mathbb{w}^{(2)} = (f_{\boldsymbol{a}}(X), f_{\boldsymbol{\alpha}^\intercal M}(X))$
V samples $\beta \xleftarrow{\$} \mathbb{F}\backslash\{0\}$
P computes $w \leftarrow f_{\boldsymbol{\alpha}^\intercal M}(\beta)$
V queries $[f_{\boldsymbol{\alpha}^\intercal M}(X)]$ in β and receives $w = f_{\boldsymbol{\alpha}^\intercal M}(\beta)$
P and V run SparseBiEval with $\mathbb{i}^{(1)} = (H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k=0}^{K-1})$, $\mathbb{x}^{(1)} = (\alpha, \beta, w)$, and $\mathbb{w}^{(1)} = \varnothing$

Protocol 12: SparseMVP

Theorem 12 (Security of SparseMVP). *Protocol* SparseMVP *is a Polynomial IOP for* $\mathcal{R}_{\text{smvp}}$ *with completeness and soundness with soundness error* $\sigma \leq \frac{5m+22H+21K-39}{|\mathbb{F}|-1}$.

Proof. Consider the following sequence of equations.

$$\boldsymbol{b} = M\boldsymbol{a} \tag{71}$$

$$\boldsymbol{\alpha}^\intercal \boldsymbol{b} = \boldsymbol{\alpha}^\intercal M\boldsymbol{a} \tag{72}$$

$$f_{\boldsymbol{b}}(\alpha) = \boldsymbol{\alpha}^\intercal M\boldsymbol{a} \tag{73}$$

$$s = \mathsf{coeffs}(f_{\boldsymbol{\alpha}^\intercal M}(X)) \cdot \mathsf{coeffs}(f_{\boldsymbol{a}}(X)) \tag{74}$$

$$s = \mathsf{coeffs}(f_M(\alpha, X)) \cdot \mathsf{coeffs}(f_{\boldsymbol{a}}(X)) \tag{75}$$

Completeness follows from the sequence of implications (71) $\Rightarrow$ (72) $\Leftrightarrow$ (73) $\Rightarrow$ (74) $\Rightarrow$ (75). For soundness, consider when the reverse implications fail.

- (71) $\not\Leftarrow$ (72). Due to the Schwartz-Zippel lemma, this event occurs with probability $\frac{m-1}{|\mathbb{F}|-1}$.
- (73) $\not\Leftarrow$ (74). This event occurs with probability bounded by the soundness error of InnerProduct, $\sigma_{\mathsf{InnerProduct}} \leq \frac{4m-3}{|\mathbb{F}|-1}$.

– (74) $\not\Leftarrow$ (75). This event implies that $f_{\boldsymbol{\alpha}^\intercal M}(X)$ and $f_M(\alpha, X)$ are distinct polynomials. The probability that this distinction is not caught by the SparseBiEval protocol is bounded by that protocol's soundness error, $\sigma_{\mathsf{SparseBiEval}} \leq \frac{22H+21K-35}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of SparseMVP is bounded by $\sigma \leq \frac{5m+22H+21K-39}{|\mathbb{F}|-1}$. □

C Alternative and Optimized Protocols

C.1 DenseMVP

The protocol DenseMVP admits one merger of polynomial identities after unrolling. We present the optimized protocol in several steps to simplify their verification by the reader.

description: decides $\mathcal{L}(\mathcal{R}_{\text{mvp}})$
inputs: $\mathbb{i} : (m, n, M)$
$\mathbb{x} : ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)])$
$\mathbb{w} : (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X))$
// pre-processing
begin
  I computes $f_M(X) \leftarrow \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$
  I sends $f_M(X)$ of degree at most $mn-1$ to P and V
begin
  V samples $\alpha \xleftarrow{\$} \mathbb{F}$ and sends α to P
  P computes $r(X) \leftarrow f_M(X) \bmod X^n - \alpha$
  P sends $r(X)$ of degree at most $n-1$ to V
  P and V run ModReduce with $\mathbb{i}^{(1)} = (mn-1, n-1)$,
   $\mathbb{x}^{(1)} = ([f_M(X)], [r(X)], X^n - \alpha)$, and $\mathbb{w}^{(1)} = (f_M(X), r(X))$
  V queries $[f_{\boldsymbol{b}}(X)]$ in α and receives $y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}} = f_{\boldsymbol{b}}(\alpha)$
  P and V run InnerProduct with $\mathbb{i}^{(2)} = n-1$, $\mathbb{x}^{(2)} = ([r(X)], [f_{\boldsymbol{a}}(X)], y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}})$,
   and $\mathbb{w}^{(2)} = (r(X), f_{\boldsymbol{a}}(X))$

Protocol 13: DenseMVP, original

description: decides $\mathcal{L}(\mathcal{R}_{\text{mvp}})$
inputs: $\mathtt{i} : (m, n, M)$
$\mathtt{x} : ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)])$
$\mathtt{w} : (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X))$
// pre-processing
begin
  I computes $f_M(X) \leftarrow \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$
  I sends $f_M(X)$ of degree at most $mn-1$ to P and V
begin
  V samples $\alpha \xleftarrow{\$} \mathbb{F}$ and sends α to P
  P computes $r(X) \leftarrow f_M(X) \bmod X^n - \alpha$
  P sends $r(X)$ of degree at most $n-1$ to V
  P and V run $\mathsf{ModReduce}$ with $\mathtt{i}^{(1)} = (mn-1, n-1)$,
   $\mathtt{x}^{(1)} = ([f_M(X)], [r(X)], X^n - \alpha)$, and $\mathtt{w}^{(1)} = (f_M(X), r(X))$
  V queries $[f_{\boldsymbol{b}}(X)]$ in α and receives $y_{\boldsymbol{a}^\intercal \boldsymbol{b}} = f_{\boldsymbol{b}}(\alpha)$
  // $\mathsf{InnerProduct}$
  begin
    P computes $h(X) \leftarrow r(X^2) \cdot f_{\boldsymbol{a}}(X^{-2}) \cdot X^{2n-2} + r(X^{-2}) \cdot f_{\boldsymbol{a}}(X^2) \cdot X^{2n-1}$
    P computes $\bar{h}(X) \leftarrow h(X) \mod X^{2n-2}$
    P sends $\bar{h}(X)$ of degree at most $2n-3$ to V
    V samples $z \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and queries $([r(X)], [f_{\boldsymbol{a}}(X)], [\bar{h}(X)])$ in (z^2, z^2, z)
     and in (z^{-2}, z^{-2}, z^{-1})
    V receives $y_a = f_{\boldsymbol{a}}(z^2)$, $y_a^* = f_{\boldsymbol{a}}(z^{-2})$, $y_h = \bar{h}(z)$, and $y_h^* = \bar{h}(z^{-1})$
    V tests
     $y_h + z^{2n-2} \cdot y_{\boldsymbol{a}^\intercal \boldsymbol{b}} + z^{2n-1} \cdot y_{\boldsymbol{a}^\intercal \boldsymbol{b}} + z^{2n} \cdot y_h^* \stackrel{?}{=} y_r \cdot y_a^* \cdot z^{2\mathsf{d}} + y_r^* \cdot y_a \cdot z^{2\mathsf{d}+1}$

Protocol 14: DenseMVP, unrolled InnerProduct

description: decides $\mathcal{L}(\mathcal{R}_{\text{mvp}})$
inputs: $\mathtt{i} : (m, n, M)$
$\mathtt{x} : ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)])$
$\mathtt{w} : (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X))$
// pre-processing
begin
  I computes $f_M(X) \leftarrow \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$
  I sends $f_M(X)$ of degree at most $mn-1$ to P and V
begin
  V samples $\alpha \xleftarrow{\$} \mathbb{F}$ and sends α to P
  P computes $r(X) \leftarrow f_M(X) \bmod X^n - \alpha$
  P sends $r(X)$ of degree at most $n-1$ to V
  // ModReduce
  begin
    P computes $q(X)$ such that $f_M(X) = q(X) \cdot (X^n - \alpha) + r(X)$
    P sends $q(X)$ of degree at most $(m-1)n$ to V
    V samples $z \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and queries $[f_M(X)]$, $[q(X)]$, and $[r(X)]$ in z
    V receives $y_f = f_M(z)$, $y_q = q(z)$, and $y_r = r(z)$
    V tests $y_f \stackrel{?}{=} y_q \cdot (z^n - \alpha) + y_r$
  V queries $[f_{\boldsymbol{b}}(X)]$ in α and receives $y_{\boldsymbol{a}^\intercal \boldsymbol{b}} = f_{\boldsymbol{b}}(\alpha)$
  // InnerProduct
  begin
    P computes $h(X) \leftarrow r(X^2) \cdot f_{\boldsymbol{a}}(X^{-2}) \cdot X^{2n-2} + r(X^{-2}) \cdot f_{\boldsymbol{a}}(X^2) \cdot X^{2n-1}$
    P computes $\bar{h}(X) \leftarrow h(X) \mod X^{2n-2}$
    P sends $\bar{h}(X)$ of degree at most $2n-3$ to V
    V samples $z \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and queries $([r(X)], [f_{\boldsymbol{a}}(X)], [\bar{h}(X)])$ in (z^2, z^2, z) and in (z^{-2}, z^{-2}, z^{-1})
    V receives $y_a = f_{\boldsymbol{a}}(z^2)$, $y_a^* = f_{\boldsymbol{a}}(z^{-2})$, $y_h = \bar{h}(z)$, and $y_h^* = \bar{h}(z^{-1})$
    V tests
    $y_h + z^{2n-2} \cdot y_{\boldsymbol{a}^\intercal \boldsymbol{b}} + z^{2n-1} \cdot y_{\boldsymbol{a}^\intercal \boldsymbol{b}} + z^{2n} \cdot y_h^* \stackrel{?}{=} y_r \cdot y_a^* \cdot z^{2\mathsf{d}} + y_r^* \cdot y_a \cdot z^{2\mathsf{d}+1}$

Protocol 15: DenseMVP, unrolled ModReduce

description: decides $\mathcal{L}(\mathcal{R}_{\text{mvp}})$
inputs: $\mathtt{i} : (m, n, M)$
$\mathtt{x} : ([f_{\boldsymbol{a}}(X)], [f_{\boldsymbol{b}}(X)])$
$\mathtt{w} : (f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X))$
// pre-processing
begin
  I computes $f_M(X) \leftarrow \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} M_{[i,j]} X^{in+j}$
  I sends $f_M(X)$ of degree at most $mn-1$ to P and V
begin
  V samples $\alpha \xleftarrow{\$} \mathbb{F}$ and sends α to P
  P computes $r(X) \leftarrow f_M(X) \bmod X^n - \alpha$
  // ModReduce
  begin
    P computes $q(X)$ such that $f_M(X) = q(X) \cdot (X^n - \alpha) + r(X)$
    P sends $q(X)$ of degree at most $(m-1)n$ to V
    V samples $z \xleftarrow{\$} \mathbb{F} \backslash \{0\}$ and queries $[f_M(X)]$ and $[q(X)]$ in z^2 and in z^{-2}
    V receives $y_f = f_M(z^2)$, $y_f^* = f_M(z^{-2})$, $y_q = q(z^2)$, and $y_q^* = q(z^{-2})$
    V sets $y_r \leftarrow y_f - y_q \cdot (z^{2n} - \alpha)$ and $y_r^* \leftarrow y_f^* - y_q^* \cdot (z^{-2n} - \alpha)$
  V queries $[f_{\boldsymbol{b}}(X)]$ in α and receives $y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}} = f_{\boldsymbol{b}}(\alpha)$
  // InnerProduct
  begin
    P computes $h(X) \leftarrow r(X^2) \cdot f_{\boldsymbol{a}}(X^{-2}) \cdot X^{2\mathsf{n}-2} + r(X^{-2}) \cdot f_{\boldsymbol{a}}(X^2) \cdot X^{2\mathsf{n}-1}$
    P computes $\bar{h}(X) \leftarrow h(X) \mod X^{2n-2}$
    P sends $\bar{h}(X)$ of degree at most $2n-3$ to V
    V queries $([f_{\boldsymbol{a}}(X)], [\bar{h}(X)])$ in (z^2, z) and in (z^{-2}, z^{-1})
    V receives $y_a = f_{\boldsymbol{a}}(z^2)$, $y_a^* = f_{\boldsymbol{a}}(z^{-2})$, $y_h = \bar{h}(z)$, and $y_h^* = \bar{h}(z^{-1})$
  // Merged test
  V tests
  $y_h + z^{2n-2} \cdot y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}} + z^{2n-1} \cdot y_{\boldsymbol{\alpha}^\intercal \boldsymbol{b}} + z^{2n} \cdot y_h^* \stackrel{?}{=} y_r \cdot y_a^* \cdot z^{2\mathsf{d}} + y_r^* \cdot y_a \cdot z^{2\mathsf{d}+1}$

Protocol 16: DenseMVP, eliminated $r(X)$; optimized

C.2 Batched SparseBiEval

BiVandermonde Vector. We batch two VandermondeVector protocols into a single protocol for efficiency. The BiVandermondeVector protocol realizes the following relation

$$\mathcal{R}_{\text{bvv}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (H, K, \varphi(h), \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}) \\ \mathbb{x} = (z, [f_{\hat{\mathbf{z}}}(X)]) \\ \mathbb{w} = f_{\hat{\mathbf{z}}}(X) \\ R_a = \begin{pmatrix} \varphi(a_0)^0 & \varphi(a_1)^0 & \cdots \\ \varphi(a_0)^1 & \varphi(a_1)^1 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \\ R_b = \begin{pmatrix} \varphi(b_0)^0 & \varphi(b_1)^0 & \cdots \\ \varphi(b_0)^1 & \varphi(b_1)^1 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \\ R = \begin{pmatrix} R_a & 0 \\ 0 & R_b \end{pmatrix} \\ f_{\hat{\mathbf{z}}}(X) = \sum_{i=0}^{2H-1} \hat{z}_i X^i \\ \mathbf{z} = (1\,,\, z\,,\, z^2\,,\, \cdots\,,\, z^{2K-1})^{\mathsf{T}} \\ \hat{\mathbf{z}} = R\mathbf{z} \end{array} \right\} . \tag{76}$$

Theorem 13 (Security of BiVandermondeVector). *Protocol* BiVandermondeVector *is a Polynomial IOP for* $\mathcal{R}_{\text{bvv}}$ *with completeness and soundness with soundness error* $\sigma \leq \frac{2H+10K-5}{|\mathbb{F}|-1}$.

Proof. Consider the following sequences of equations.

$$\hat{\mathbf{z}} = R\mathbf{z} \tag{77}$$

$$\boldsymbol{\delta}^{\mathsf{T}}\hat{\mathbf{z}} = \boldsymbol{\delta}^{\mathsf{T}}R\mathbf{z} \tag{78}$$

$$f_{\hat{\mathbf{z}}}(\delta) = f_{\hat{\boldsymbol{\delta}}}(z) \tag{79}$$

$$y_1 = y_0 \;\;, \tag{80}$$

and

$$\forall k \in \{0, \ldots, K-1\} \;.\; \left(\sum_{h=0}^{H-1} (\delta \cdot \varphi(a_k))^h\right) \cdot (1 - \delta \cdot \varphi(a_k)) = 1 - (\delta \cdot \varphi(a_k))^H \tag{81}$$

$$\left(\sum_{h=0}^{H-1} \delta^{H+h} \cdot \varphi(a_k)^h\right) \cdot (1 - \delta \cdot \varphi(b_k)) = \delta^H \cdot \left(1 - (\delta \cdot \varphi(b_k))^H\right)$$

$$\left(\boldsymbol{\delta}^{\mathsf{T}}R\right) \circ \left((1 - \delta \cdot \varphi(a_k))_{k=0}^{K-1} \,\|\, (1 - \delta \cdot \varphi(b_k))_{k=0}^{K-1}\right) =$$

$$\left(1 - (\delta \cdot \varphi(a_k))^H\right)_{k=0}^{K-1} \Big\| \left(1 - (\delta \cdot \varphi(b_k))^H\right)_{k=0}^{K-1} \cdot \delta^H \tag{82}$$

description: decides $\mathcal{L}(\mathcal{R}_{\text{bvv}})$
inputs: $\mathbb{i}$: $H, K, \varphi(h), \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}$
$\mathbb{x}$: $z, [f_{\hat{\boldsymbol{z}}}(X)]$
$\mathbb{w}$: $f_{\hat{\boldsymbol{z}}}(X)$
// pre-processing
begin
I computes $f_{\varphi(a_k)}(X) \leftarrow \sum_{k=0}^{K-1} \varphi(a_k) X^k$, $f_{\varphi(a_k)^H}(X) \leftarrow \sum_{k=0}^{K-1} \varphi(a_k)^H X^k$, $f_{\varphi(b_k)}(X) \leftarrow \sum_{k=0}^{K-1} \varphi(b_k) X^k$ and $f_{\varphi(b_k)^H}(X) \leftarrow \sum_{k=0}^{K-1} \varphi(b_k)^H X^k$
I sends $f_{\varphi(a_k)}(X)$, $f_{\varphi(a_k)^H}(X)$, $f_{\varphi(b_k)}(X)$ and $f_{\varphi(b_k)^H}(X)$, all of degree at most $K-1$, to P and V
// online
begin
V samples $\delta \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and sends δ to P
P computes $\boldsymbol{\delta} \leftarrow (\delta^0, \delta^1, \ldots, \delta^{2H-1})^\mathsf{T}$, $\hat{\boldsymbol{\delta}} \leftarrow R^\mathsf{T}\boldsymbol{\delta}$, and $f_{\hat{\boldsymbol{\delta}}}(X) \leftarrow \sum_{i=0}^{2K-1} \hat{\delta}_i X^i$
P sends $f_{\hat{\boldsymbol{\delta}}}(X)$ of degree at most $2K-1$ to V
V queries $[f_{\hat{\boldsymbol{\delta}}}(X)]$ in z and receives $y_0 = f_{\hat{\boldsymbol{\delta}}}(z)$
V queries $[f_{\hat{\boldsymbol{z}}}(X)]$ in δ and receives $y_1 = f_{\hat{\boldsymbol{z}}}(\delta)$
V checks $y_1 \stackrel{?}{=} y_0$
P and V run Hadamard with $\mathbb{i}^{(1)} = 2K-1$,
$\mathbb{x}^{(1)} = ([f_{\hat{\boldsymbol{\delta}}}(X)], [\delta \cdot f_{\varphi(a_k)}(X) - f_I(X) + (\delta \cdot f_{\varphi(b_k)}(X) - f_I(X)) \cdot \delta^H \cdot X^K]$, $[\delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X) + (\delta^H \cdot f_{\varphi(b_k)^H}(X) - f_I(X)) \cdot \delta^H \cdot X^K])$,
$\mathbb{w}^{(1)} = (f_{\hat{\boldsymbol{\delta}}}(X), \delta^H \cdot f_{\varphi(a_k)}(X) - f_I(X) + (\delta^H \cdot f_{\varphi(b_k)}(X) - f_I(X)) \cdot \delta^H \cdot X^K$, $\delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X) + (\delta^H \cdot f_{\varphi(b_k)^H}(X) - f_I(X)) \cdot \delta^H \cdot X^K)$, where V simulates $[f_{\varphi(a_k)}(\delta X) - f_I(X) + (f_{\varphi(b_k)}(\delta X) - f_I(X)) \cdot \delta^H \cdot X^K]$ and $[f_{\varphi(a_k)^H}(\delta X) - f_I(X) + (f_{\varphi(b_k)^H}(\delta X) - f_I(X)) \cdot \delta^H \cdot X^K]$ using the oracles $[f_{\varphi(a_k)}(X)], [f_{\varphi(a_k)^H}(X)], [f_{\varphi(b_k)}(X)], [f_{\varphi(b_k)^H}(X)]$ and the known scalar δ, in combination with computing $f_I(X) = \sum_{k=0}^{2K-1} X^k$ locally

Protocol 17: BiVandermondeVector

$$f_{\hat{\boldsymbol{\delta}}}(X) \circ \left(\delta \cdot f_{\varphi(a_k)}(X) - f_I(X) + (\delta \cdot f_{\varphi(b_k)}(X) - f_I(X)) \cdot \delta^H \cdot X^K\right) = \delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X) + \left(\delta^H \cdot f_{\varphi(b_k)^H}(X) - f_I(X)\right) \cdot \delta^H \cdot X^K \quad (83)$$

$$\begin{aligned}(\mathbb{i}^{(1)}, \mathbb{x}^{(1)}) = (2K-1, [f_{\hat{\boldsymbol{\delta}}}(X)], \\ [\delta \cdot f_{\varphi(a_k)}(X) - f_I(X) + (\delta \cdot f_{\varphi(b_k)}(X) - f_I(X)) \cdot \delta^H \cdot X^K], \\ [\delta^H \cdot f_{\varphi(a_k)^H}(X) - f_I(X) + (\delta^H \cdot f_{\varphi(b_k)^H}(X) - f_I(X)) \cdot \delta^H \cdot X^K)] \\ \in \mathcal{L}(\mathcal{R}_{\text{hadamard}}) \ . \end{aligned} \quad (84)$$

Completeness follows from the sequences of implications a) (77) $\Rightarrow$ (78) $\Leftrightarrow$ (79) $\Leftrightarrow$ (80), and b) (81) $\Leftrightarrow$ (82) $\Leftrightarrow$ (83) $\Rightarrow$ (84). Sequence (a) holds for any matrix R. Sequence (b) starts with the equation for two geometric sums derived from the matrix R_a and R_b as defined as in Eqn. 27.

For soundness, consider when the reverse implications fail. There are two such cases:

- (77) $\not\Leftarrow$ (78). By the Schwartz-Zippel lemma, the probability of this event is bounded by $\frac{2H-1}{|\mathbb{F}|-1}$.
- (83) $\not\Leftarrow$ (84). The probability of this event is captured by the soundness error of Hadamard, $\sigma_{\mathsf{Hadamard}} \leq \frac{10K-4}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of BiVandermondeVector is bounded by $\sigma \leq \frac{2H+10K-5}{|\mathbb{F}|-1}$. □

BiLagrange Vector. We batch two instances of LagrangeVector protocol into a single protocol for efficiency. The BiLagrangeVector protocol realizes the following relation

$$\mathcal{R}_{\text{lv}} = \left\{ (\mathbb{i}, \mathbb{x}, \mathbb{w}) \;\middle|\; \begin{array}{l} \mathbb{i} = (H, \varphi(h)) \\ \mathbb{x} = (u, v, [f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X)]) \\ \mathbb{w} = f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X) \\ L = \begin{pmatrix} \mathcal{L}_{\varphi(0),0} & \mathcal{L}_{\varphi(0),1} & \cdots \\ \mathcal{L}_{\varphi(1),0} & \mathcal{L}_{\varphi(1),1} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \\ f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X) = \sum_{i=0}^{H-1} \hat{u}_i X^i + \sum_{i=0}^{H-1} \hat{v}_i X^{H+i} \\ \mathbf{u} = (1, u, u^2, \cdots, u^{H-1})^\mathsf{T} \\ \mathbf{v} = (1, v, v^2, \cdots, v^{H-1})^\mathsf{T} \\ \hat{\mathbf{u}} = \mathbf{u}^\mathsf{T} L \quad \hat{\mathbf{v}} = \mathbf{v}^\mathsf{T} L \end{array} \right\} . \quad (85)$$

Theorem 14 (Security of BiLagrangeVector). *Protocol* BiLagrangeVector *is a Polynomial IOP for* $\mathcal{R}_{\text{blv}}$ *with completeness and soundness with soundness error* $\sigma \leq \frac{7H-5}{|\mathbb{F}|-1}$.

description: decides $\mathcal{L}(\mathcal{R}_{\text{blv}})$
inputs: $\mathbb{i}$: $H, \varphi(h)$
$\mathbb{x}$: $u, v, [f_{\mathbf{u\hat{v}}}(X)]$
$\mathbb{w}$: $f_{\mathbf{u\hat{v}}}(X)$
// pre-processing
begin
I computes $f_{\varphi(h)}(X) \leftarrow \sum_{h=0}^{H-1} \varphi(h) X^h$, $Z_{\mathcal{H}}(X) \leftarrow \prod_{h=0}^{H-1}(X - \varphi(h))$ and $f_{\mathcal{H}}(X) \leftarrow \sum_{h=0}^{H-1} \left(\prod_{i \in \{0 \dots H-1\} \setminus \{h\}} (\varphi(h) - \varphi(i))\right)^{-1} \cdot X^h$
I sends $f_{\varphi(h)}(X)$, $f_{\mathcal{H}}(X)$, both of degree at most $H-1$, and $Z_{\mathcal{H}}(X)$ of degree at most H, to P and V
// online
begin
V samples $\gamma \xleftarrow{\$} \mathbb{F} \setminus \{0\}$ and sends γ to P
P computes $\boldsymbol{\gamma} \leftarrow (\gamma^0, \gamma^1, \dots, \gamma^{H-1})^{\mathsf{T}}$, $\hat{\boldsymbol{\gamma}} \leftarrow L\boldsymbol{\gamma}$, and $f_{\hat{\boldsymbol{\gamma}}}(X) \leftarrow \sum_{i=0}^{H-1} \hat{\gamma}_i X^i$
P sends $f_{\hat{\boldsymbol{\gamma}}}(X)$ of degree at most $H-1$ to V
V queries $[f_{\hat{\boldsymbol{\gamma}}}(X)]$ in u, v and receives $y_0 = f_{\hat{\boldsymbol{\gamma}}}(u), y_1 = f_{\hat{\boldsymbol{\gamma}}}(v)$
V queries $[f_{\mathbf{u\hat{v}}}(X)]$ in γ and receives $y_2 = f_{\mathbf{u\hat{v}}}(\gamma)$
V checks $y_2 \stackrel{?}{=} y_0 + \gamma^H \cdot y_1$
V queries $[Z_{\mathcal{H}}(X)]$ in γ and receives $w = Z_{\mathcal{H}}(\gamma)$
P and V run Hadamard with $\mathbb{i}^{(1)} = H - 1$,
$\mathbb{x}^{(1)} = ([f_{\hat{\boldsymbol{\gamma}}}(X)], [\gamma f_I(X) - f_{\varphi(h)}(X)], [w f_{\mathcal{H}}(X)])$,
$\mathbb{w}^{(1)} = (f_{\hat{\boldsymbol{\gamma}}}(X), \gamma f_I(X) - f_{\varphi(h)}(X), w f_{\mathcal{H}}(X))$, where V simulates $[\gamma f_I(X) - f_{\varphi(h)}(X)], [w f_{\mathcal{H}}(X)]$ using the oracles $[f_{\varphi(h)}(X)], [f_{\mathcal{H}}(X)]$ and the known scalar γ, in combination with computing $f_I(X) = \sum_{h=0}^{H-1} X^h$ locally

Protocol 18: BiLagrangeVector

Proof. Consider the following sequences of equations.

$$\hat{\mathbf{u}}^\mathsf{T} = \mathbf{u}^\mathsf{T} L \qquad \hat{\mathbf{v}}^\mathsf{T} = \mathbf{v}^\mathsf{T} L \tag{86}$$

$$\hat{\mathbf{u}}^\mathsf{T}\boldsymbol{\gamma} + \hat{\mathbf{v}}^\mathsf{T}\boldsymbol{\gamma} \cdot \gamma^H = \mathbf{u}^\mathsf{T} L\boldsymbol{\gamma} + \mathbf{v}^\mathsf{T} L\boldsymbol{\gamma} \cdot \gamma^H \tag{87}$$

$$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(\gamma) = f_{\hat{\boldsymbol{\gamma}}}(u) + f_{\hat{\boldsymbol{\gamma}}}(v) \cdot \gamma^H \tag{88}$$

$$y_2 = y_0 + \gamma^H \cdot y_1 \ , \tag{89}$$

and

$$\forall h \in \{0, \ldots, H-1\} \,.\, \mathcal{L}_h(\gamma) = \prod_{\substack{i=0 \\ i \neq h}}^{H-1} \frac{\gamma - \varphi(i)}{\varphi(h) - \varphi(i)} \tag{90}$$

$$\forall h \in \{0, \ldots, H-1\} \,.\, \mathcal{L}_h(\gamma) \cdot (\gamma - \varphi(h)) = \frac{Z_{\mathcal{H}}(\gamma)}{\prod_{\substack{i=0 \\ i \neq h}}^{H-1} (\varphi(h) - \varphi(i))} \tag{91}$$

$$(L\boldsymbol{\gamma}) \circ (\gamma - \varphi(h))_{h=0}^{H-1} = Z_{\mathcal{H}}(\gamma) \left(\left(\prod_{i \in \{0 \ldots H-1\} \setminus \{h\}} (\varphi(h) - \varphi(i)) \right)^{-1} \right)_{h=0}^{H-1} \tag{92}$$

$$f_{\hat{\boldsymbol{\gamma}}}(X) \circ (\gamma f_I(X) - f_\varphi(X)) = w f_{\mathcal{H}}(X) \tag{93}$$

$$(\mathbb{i}^{(1)}, \mathbb{x}^{(1)}) = \tag{94}$$

$$(H-1, [f_{\hat{\boldsymbol{\gamma}}}(X)], [\gamma f_I(X) - f_{\varphi(h)}(X)], [w f_{\mathcal{H}}(X)]) \in \mathcal{L}(\mathcal{R}_{\text{hadamard}}) \ .$$

Completeness follows from the sequences of implications a) (86) $\Rightarrow$ (87) $\Leftrightarrow$ (88) $\Leftrightarrow$ (89), and b) (90) $\Leftrightarrow$ (91) $\Leftrightarrow$ (92) $\Leftrightarrow$ (93) $\Rightarrow$ (94). Sequence (a) holds for any matrix L. Sequence (b) starts with the definition of Lagrange basis polynomials, and holds when the rows of L are exactly the coefficient vectors of the Lagrange basis polynomials. Recall that Lagrange basis polynomial indexed by h takes the value 1 in $\varphi(h)$ and 0 in all other points of $\mathcal{H}$.

For soundness, consider when the reverse implications fail. There are two such cases:

- (86) $\not\Leftarrow$ (87). By the Schwartz-Zippel lemma, the probability of this event is bounded by $\frac{2H-1}{|\mathbb{F}|-1}$.
- (93) $\not\Leftarrow$ (94). The probability of this event is captured by the soundness error of Hadamard, $\sigma_{\mathsf{Hadamard}} \leq \frac{5H-4}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of BiLagrangeVector is bounded by $\sigma \leq \frac{7H-5}{|\mathbb{F}|-1}$. □

Batched SparseBiEval Using the above two protocols, we obtain an improved version of the SparseBiEval protocol that saves four polynomial oracles at the relatively minor expense of doubling their degree. Protocol 19 verifies the relation $\mathcal{R}_{\text{sbi}}$ defined by Eqn. 62.

description: decides $\mathcal{L}(\mathcal{R}_{\text{sbe}})$
inputs: $\mathbb{i}$: $H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1}, \{c_k\}_{k=0}^{K-1}$
$\mathbb{x}$: u, v, w
$\mathbb{w}$: $\varnothing$

// pre-processing
begin
- I selects any mapping $\varphi : \mathbb{N} \to \mathbb{F}$ such that $\{0, \ldots, H-1\}$ are mapped to distinct elements
- I runs BiVandermondeVector.I with $\mathbb{i}^{(1)} = (H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1})$
- I runs BiLagrangeVector.I with $\mathbb{i}^{(2)} = (H, \varphi(h))$
- I computes $f_c(X) \leftarrow \sum_{k=0}^{K-1} c_k X^k$
- I sends $f_c(X)$ of degree at most $K-1$ to P and V

// online
begin
- P computes $f_{u\|v}(X) \leftarrow \sum_{k=0}^{K-1} u^{a_k} X^k + \sum_{k=0}^{K-1} v^{b_k} X^{k+K}$ and $f_{uv}(X) \leftarrow \sum_{k=0}^{K-1} u^{a_k} v^{b_k} X^k$
- P sends $f_{u\|v}(X)$ of degree at most $2K-1$ and $f_{uv}(X)$ of degree at most $K-1$, to V
- **Batched Lagrange vector:**
  - P computes $\mathbf{u} \leftarrow (1, u, u^2, \cdots, u^{H-1})^\mathsf{T}$, $\hat{\mathbf{u}} \leftarrow \mathbf{u}^\mathsf{T} L$, $\mathbf{v} \leftarrow (1, v, v^2, \cdots, v^{H-1})^\mathsf{T}$, $\hat{\mathbf{v}} \leftarrow \mathbf{v}^\mathsf{T} L$
  - P computes $f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X) \leftarrow \sum_{i=0}^{H-1} \hat{u}_i X^i + \sum_{i=0}^{H-1} \hat{v}_i X^{i+H}$
  - P sends $f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X)$ of degree at most $2H-1$ to V
  - P and V run BiLagrangeVector with $\mathbb{i}^{(2)} = (H, \varphi(h))$, $\mathbb{x}^{(2)} = (u, v, [f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X)])$, and $\mathbb{w}^{(2)} = f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X)$
- **Batched Vandermonde vector:**
  - V samples $y \xleftarrow{\$} \mathbb{F}\backslash\{0\}$ and sends y to P
  - P computes $\mathbf{y} \leftarrow (1, y, y^2, \cdots, y^{2K-1})$, $\hat{\mathbf{y}} \leftarrow R\mathbf{y}$ where R is as defined in Eqn. 76
  - P computes $f_{\hat{\mathbf{y}}}(X) \leftarrow \sum_{i=0}^{2K-1} \hat{z}_i X^i$
  - P sends $f_{\hat{\mathbf{y}}}(X)$ of degree at most $2K-1$ to V
  - P and V run BiVandermondeVector with $\mathbb{i}^{(1)} = (H, K, \{a_k\}_{k=0}^{K-1}, \{b_k\}_{k=0}^{K-1})$, $\mathbb{x}^{(1)} = (y, [f_{\hat{\mathbf{y}}}(X)])$, and $\mathbb{w}^{(1)} = f_{\hat{\mathbf{y}}}(X)$
- V queries $[f_{u\|v}(X)]$ in y and receives $s = f_{u\|v}(y)$
- P and V run InnerProduct with $\mathbb{i}^{(3)} = 2H-1$, $\mathbb{x}^{(3)} = ([f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X)], [f_{\hat{\mathbf{y}}}(X)], s)$, and $\mathbb{w}^{(3)} = (f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X), f_{\hat{\mathbf{y}}}(X))$
- P and V run Hadamard with $\mathbb{i}^{(4)} = 3K-1$, $\mathbb{x}^{(4)} = ([f_{u\|v}(X)], [f_{u\|v}(X) \cdot X^K], [f_{uv}(X) \cdot X^K])$, and $\mathbb{w}^{(4)} = (f_{u\|v}(X), f_{u\|v}(X) \cdot X^K, f_{uv}(X) \cdot X^K)$ where V simulates $[f_{u\|v}(X) \cdot X^K]$ and $[f_{uv}(X) \cdot X^K]$ using $[f_{u\|v}(X)]$ and $[f_{uv}(X)]$ respectively
- P and V run InnerProduct with $\mathbb{i}^{(5)} = K-1$, $\mathbb{x}^{(5)} = ([f_{uv}(X)], [f_c(X)], w)$, and $\mathbb{w}^{(5)} = (f_{uv}(X), f_c(X))$

Protocol 19: BatchedSparseBiEval

Theorem 15 (Security of BatchedSparseBiEval). *Protocol* BatchedSparseBiEval *is a Polynomial IOP for* $\mathcal{R}_{\text{sbi}}$ *with completeness and soundness with soundness error* $\sigma = \frac{17H+31K-21}{|\mathbb{F}|-1}$.

Proof. Consider the following sequences of equations.

$$f_{u\|v}(X) = \sum_{k=0}^{K-1} u^{a_k} X^k + \sum_{k=0}^{K-1} v^{b_k} X^{k+K} \tag{95}$$

$$f_{u\|v}(y) = \sum_{k=0}^{K-1} u^{a_k} y^k + \sum_{k=0}^{K-1} v^{b_k} y^{k+K} \tag{96}$$

$$f_{u\|v}(y) = \mathbf{u}^{\mathsf{T}}(\mathbf{e}_{a_0}, \cdots, \mathbf{e}_{a_{K-1}})\mathbf{y}_{[0:K]} + \mathbf{v}^{\mathsf{T}}(\mathbf{e}_{b_0}, \cdots, \mathbf{e}_{b_{K-1}})\mathbf{y}_{[K:2K]} \tag{97}$$

$$f_{u\|v}(y) = \mathbf{u}^{\mathsf{T}} L R_a \mathbf{y}_{[0:K]} + \mathbf{v}^{\mathsf{T}} L R_b \mathbf{y}_{[K:2K]} \tag{98}$$

$$f_{u\|v}(y) = \hat{\mathbf{u}}^{\mathsf{T}} R_a \mathbf{y}_{[0:K]} + \hat{\mathbf{v}}^{\mathsf{T}} R_b \mathbf{y}_{[K:2K]} \tag{99}$$

$$f_{u\|v}(y) = (\hat{\mathbf{u}}^{\mathsf{T}} \| \hat{\mathbf{v}}^{\mathsf{T}}) R \mathbf{y} \tag{100}$$

$$f_{u\|v}(y) = (\hat{\mathbf{u}}^{\mathsf{T}} \| \hat{\mathbf{v}}^{\mathsf{T}}) \cdot \hat{\mathbf{y}} \tag{101}$$

$$(\mathbb{i}, \mathbb{x}) = (2H-1, ([f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}(X)], [f_{\hat{\mathbf{y}}}(X)], s)) \in \mathcal{R}_{\text{ip}} \tag{102}$$

and

$$f(u, v) = w \tag{103}$$

$$\sum_{k=0}^{K-1} c_k u^{a_k} v^{b_k} = w \tag{104}$$

$$\mathsf{coeffs}(f_{uv}(X)) \cdot \mathsf{coeffs}(f_c(X)) = w \tag{105}$$

$$\big(\mathsf{coeffs}(f_{u\|v}(X)) \circ \mathsf{coeffs}(f_{u\|v}(X) \cdot X^K)\big)_{[K:2K]} \cdot \mathsf{coeffs}(f_c(X)) = w \tag{106}$$

$$\big(\mathsf{coeffs}(f_{u\|v}(X)) \circ \mathsf{coeffs}(f_{u\|v}(X) \cdot X^K)\big)_{[K:2K]} \cdot (c_k)_{k=0}^{K-1} = w \tag{107}$$

$$\Big((u^{a_k})_{k=0}^{K-1} \circ \big(v^{b_k}\big)_{k=0}^{K-1}\Big) \cdot (c_k)_{k=0}^{K-1} = w \tag{108}$$

Completeness follows from the sequences of implications: a) (95) $\Rightarrow$ (96) $\Leftrightarrow$ (97) $\Leftrightarrow$ (98) $\Rightarrow$ (99) $\Leftrightarrow$ (100) $\Rightarrow$ (101) $\Rightarrow$ (102) and b) (103) $\Leftrightarrow$ (104) $\Rightarrow$ (105) $\Rightarrow$ (106) $\Leftrightarrow$ (107) $\Leftrightarrow$ (108). For soundness, consider when the reverse implications fail.

- (95) $\not\Leftarrow$ (96). This event happens with probability at most $\frac{2K-1}{|\mathbb{F}|-1}$ due to the Schwartz-Zippel lemma.
- (98) $\not\Leftarrow$ (99). This event implies that BiLagrangeVector succeeded despite being run on a false instance. This happens with probability at most equal to the soundness error of that protocol, $\sigma_{\mathsf{BiLagrangeVector}} \leq \frac{7H-5}{|\mathbb{F}|-1}$.
- (100) $\not\Leftarrow$ (101). This event implies that BiVandermondeVector succeeded despite being run on a false instance. This happens with probability at most equal to the soundness error of that protocol, $\sigma_{\mathsf{BiVandermondeVector}} \leq \frac{2H+10K-5}{|\mathbb{F}|-1}$.

– (101) $\not\Leftarrow$ (102). This event implies that InnerProduct succeeded despite being run on a false instance. This happens with probability at most equal to the soundness error of that protocol, $\sigma_{\mathsf{InnerProduct}} \leq \frac{8H-3}{|\mathbb{F}|-1}$.
– (104) $\not\Leftarrow$ (105). This event happens with probability at most equal to the soundness error of InnerProduct, $\sigma_{\mathsf{InnerProduct}} \leq \frac{4K-3}{|\mathbb{F}|-1}$.
– (105) $\not\Leftarrow$ (106). This event happens with probability at most equal to the soundness error of Hadamard, $\sigma_{\mathsf{Hadamard}} \leq \frac{15K-4}{|\mathbb{F}|-1}$.

By the Union Bound, the soundness error of BatchedSparseBiEval is bounded by $\sigma \leq \frac{17H+31K-21}{|\mathbb{F}|-1}$. □

D Call Graphs and Statistics

Table 2. Callgraph Statistics for Hadamard

protocol	preprocessed	input	new	oracles queried	queried in
Hadamard	-	$f_{\boldsymbol{a}}(X), f_{\boldsymbol{b}}(X), f_{\boldsymbol{c}}(X)$	$\bar{h}(X)$		
				$f_{\boldsymbol{a}}(X)$	$\alpha^2 z^2, \alpha^{-2} z^{-2}$
				$f_{\boldsymbol{b}}(X)$	z^2, z^{-2}
				$f_{\boldsymbol{c}}(X)$	α
				$\bar{h}(X)$	z, z^{-1}
total:	0	3	1	7	5

Table 3. Callgraph Statistics for DenseMVP

protocol	preprocessed	input	new	oracles queried	queried in
DenseMVP	f_M	$f_{\boldsymbol{a}}, f_{\boldsymbol{b}}$	q		
				$f_{\boldsymbol{b}}$	α_6
- InnerProduct		$q, f_M, f_{\boldsymbol{a}}$	$\bar{h}_7$		
-				$\bar{h}_7$	$z_8, (z_8)^{-1}$
-				q	$(z_8)^2, (z_8)^{-2}$
-				l	$(z_8)^2, (z_8)^{-2}$
-				f_M	$(z_8)^2, (z_8)^{-2}$
-				$f_{\boldsymbol{a}}$	$(z_8)^2, (z_8)^{-2}$
total:	1	2	2	9	5

Table 4. Callgraph Statistics for DenseClaymore

protocol	preprocessed	input	new	oracles queried	queried in
DenseClaymore	f_M	$f_{\mathbf{x}}$	f_{wl}, f_{wr}, f_{wo}		
- DenseMVP	f_M	$f_{wl}, f_{wr}, f_{wo}, f_{\mathbf{x}}$	q		
-				$f_{\mathbf{x}}$	α_0
- - InnerProduct		$q, f_M, f_{wl}, f_{wr}, f_{wo}$	$\bar{h}_1$		
- -				$\bar{h}_1$	$z_2, (z_2)^{-1}$
- -				q	$(z_2)^2, (z_2)^{-2}$
- -				l	$(z_2)^2, (z_2)^{-2}$
- -				f_M	$(z_2)^2, (z_2)^{-2}$
- -				f_{wl}	$(z_2)^2, (z_2)^{-2}$
- -				f_{wr}	$(z_2)^2, (z_2)^{-2}$
- -				f_{wo}	$(z_2)^2, (z_2)^{-2}$
- Hadamard		f_{wl}, f_{wr}, f_{wo}			
-				f_{wo}	α_3
- - InnerProduct		f_{wl}, f_{wr}	$\bar{h}_4$		
- -				$\bar{h}_4$	$z_5, (z_5)^{-1}$
- -				f_{wl}	$(\alpha_3 z_5)^2, (\alpha_3 z_5)^{-2}$
- -				f_{wr}	$(z_5)^2, (z_5)^{-2}$
total:	1	1	6	20	12
with BatchedInnerProduct:	1	1	5	18	8
and witness concatenation:	1	1	4	16	8

Table 5. Callgraph Statistics for VandermondeVector

protocol	preprocessed	input	new	oracles queried	queried in
VandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$	$f_{\hat{\mathbf{x}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
				$f_{\hat{\mathbf{x}}}$	δ_0
				$f_{\hat{\boldsymbol{\delta}}}$	z_1
- Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$			
-				$f_{\varphi(a_k)^H}$	$\delta_0^H \alpha_2$
-				f_I	α_2
- - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}$	$\bar{h}_3$		
- -				$\bar{h}_3$	$z_4, (z_4)^{-1}$
- -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_2 z_4)^2, (\alpha_2 z_4)^{-2}$
- -				$f_{\varphi(a_k)}$	$(\delta_0 z_4)^2, (\delta_0 z_4)^{-2}$
- -				f_I	$(z_4)^2, (z_4)^{-2}$
total:	2	1	2	9	9

Table 6. Callgraph Statistics for LagrangeVector

protocol	preprocessed	input	new	oracles queried	queried in
LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\mathbf{x}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
				$f_{\hat{\mathbf{x}}}$	γ_5
				$f_{\hat{\boldsymbol{\gamma}}}$	z_6
				$Z_{\mathcal{H}}$	γ_5
- Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
-				$f_{\mathcal{H}}$	α_7
- - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	$\bar{h}_8$		
- -				$\bar{h}_8$	$z_9, (z_9)^{-1}$
- -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_7 z_9)^2, (\alpha_7 z_9)^{-2}$
- -				f_I	$(z_9)^2, (z_9)^{-2}$
- -				$f_{\varphi(h)}$	$(z_9)^2, (z_9)^{-2}$
total:	3	1	2	10	9

Table 7. Callgraph Statistics for SparseMonomialVector

protocol	preprocessed	input	new	oracles queried	queried in
SparseMonomialVector		$f_{\hat{\boldsymbol{x}}}$	$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$		
				$f_{\hat{\boldsymbol{x}}}$	x_{31}
- VandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
-				$f_{\hat{\boldsymbol{y}}}$	δ_{32}
-				$f_{\hat{\boldsymbol{\delta}}}$	z_{33}
- - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$			
- -				$f_{\varphi(a_k)^H}$	$\delta_{32}^H \alpha_{34}$
- -				f_I	α_{34}
- - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}$	$\bar{h}_{35}$		
- - -				$\bar{h}_{35}$	$z_{36}, (z_{36})^{-1}$
- - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{34} z_{36})^2, (\alpha_{34} z_{36})^{-2}$
- - -				$f_{\varphi(a_k)}$	$(\delta_{32} z_{36})^2, (\delta_{32} z_{36})^{-2}$
- - -				f_I	$(z_{36})^2, (z_{36})^{-2}$
- LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
-				$f_{\hat{\boldsymbol{z}}}$	γ_{37}
-				$f_{\hat{\boldsymbol{\gamma}}}$	z_{38}
-				$Z_{\mathcal{H}}$	γ_{37}
- - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- -				$f_{\mathcal{H}}$	α_{39}
- - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	$\bar{h}_{40}$		
- - -				$\bar{h}_{40}$	$z_{41}, (z_{41})^{-1}$
- - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{39} z_{41})^2, (\alpha_{39} z_{41})^{-2}$
- - -				f_I	$(z_{41})^2, (z_{41})^{-2}$
- - -				$f_{\varphi(h)}$	$(z_{41})^2, (z_{41})^{-2}$
- InnerProduct		$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$	$\bar{h}_{42}$		
-				$\bar{h}_{42}$	$z_{43}, (z_{43})^{-1}$
-				$f_{\hat{\boldsymbol{z}}}$	$(z_{43})^2, (z_{43})^{-2}$
-				$f_{\hat{\boldsymbol{y}}}$	$(z_{43})^2, (z_{43})^{-2}$
total:	5	1	7	26	23

Table 8. Callgraph Statistics for SparseBiEval

protocol	preprocessed	input	new	oracles queried	queried in
SparseBiEval	f_c		f_u, f_v, f_{uv}		
- SparseMonomialVector		f_u	$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$		
-				f_u	x_{23}
- - VandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- -				$f_{\hat{\boldsymbol{y}}}$	δ_{24}
- -				$f_{\hat{\boldsymbol{\delta}}}$	z_{25}
- - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$			
- - -				$f_{\varphi(a_k)^H}$	$\delta_{24}^H \alpha_{26}$
- - -				f_I	α_{26}
- - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}$	h_{27}		
- - - -				$\bar{h}_{27}$	$z_{28}, (z_{28})^{-1}$
- - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{26} z_{28})^2, (\alpha_{26} z_{28})^{-2}$
- - - -				$f_{\varphi(a_k)}$	$(\delta_{24} z_{28})^2, (\delta_{24} z_{28})^{-2}$
- - - -				f_I	$(z_{28})^2, (z_{28})^{-2}$
- - LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- -				$f_{\hat{\boldsymbol{z}}}$	γ_{29}
- -				$f_{\hat{\boldsymbol{\gamma}}}$	z_{30}
- -				$Z_{\mathcal{H}}$	γ_{29}
- - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - -				$f_{\mathcal{H}}$	α_{31}
- - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_{32}		
- - - -				$\bar{h}_{32}$	$z_{33}, (z_{33})^{-1}$
- - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{31} z_{33})^2, (\alpha_{31} z_{33})^{-2}$
- - - -				f_I	$(z_{33})^2, (z_{33})^{-2}$
- - - -				$f_{\varphi(h)}$	$(z_{33})^2, (z_{33})^{-2}$
- - InnerProduct		$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$	h_{34}		
- -				$\bar{h}_{34}$	$z_{35}, (z_{35})^{-1}$
- -				$f_{\hat{\boldsymbol{x}}}$	$(z_{35})^2, (z_{35})^{-2}$
- -				$f_{\hat{\boldsymbol{y}}}$	$(z_{35})^2, (z_{35})^{-2}$
- SparseMonomialVector		f_v	$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$		
-				f_v	x_{36}
- - VandermondeVector	$f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- -				$f_{\hat{\boldsymbol{y}}}$	δ_{37}
- -				$f_{\hat{\boldsymbol{\delta}}}$	z_{38}
- - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$			
- - -				$f_{\varphi(b_k)^H}$	$\delta_{37}^H \alpha_{39}$
- - -				f_I	α_{39}
- - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(b_k)}$	h_{40}		
- - - -				$\bar{h}_{40}$	$z_{41}, (z_{41})^{-1}$
- - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{39} z_{41})^2, (\alpha_{39} z_{41})^{-2}$
- - - -				$f_{\varphi(b_k)}$	$(\delta_{37} z_{41})^2, (\delta_{37} z_{41})^{-2}$
- - - -				f_I	$(z_{41})^2, (z_{41})^{-2}$
- - LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- -				$f_{\hat{\boldsymbol{z}}}$	γ_{42}
- -				$f_{\hat{\boldsymbol{\gamma}}}$	z_{43}
- -				$Z_{\mathcal{H}}$	γ_{42}
- - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - -				$f_{\mathcal{H}}$	α_{44}
- - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_{45}		
- - - -				$\bar{h}_{45}$	$z_{46}, (z_{46})^{-1}$
- - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{44} z_{46})^2, (\alpha_{44} z_{46})^{-2}$
- - - -				f_I	$(z_{46})^2, (z_{46})^{-2}$
- - - -				$f_{\varphi(h)}$	$(z_{46})^2, (z_{46})^{-2}$
- - InnerProduct		$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$	h_{47}		
- -				$\bar{h}_{47}$	$z_{48}, (z_{48})^{-1}$
- -				$f_{\hat{\boldsymbol{x}}}$	$(z_{48})^2, (z_{48})^{-2}$
- -				$f_{\hat{\boldsymbol{y}}}$	$(z_{48})^2, (z_{48})^{-2}$
- Hadamard		f_u, f_v, f_{uv}			
-				f_{uv}	α_{49}
- - InnerProduct		f_u, f_v	h_{50}		
- -				$\bar{h}_{50}$	$z_{51}, (z_{51})^{-1}$
- -				f_u	$(\alpha_{49} z_{51})^2, (\alpha_{49} z_{51})^{-2}$
- -				f_v	$(z_{51})^2, (z_{51})^{-2}$
- InnerProduct		f_{uv}, f_c	h_{52}		
-				$\bar{h}_{52}$	$z_{53}, (z_{53})^{-1}$
-				f_{uv}	$(z_{53})^2, (z_{53})^{-2}$
-				f_c	$(z_{53})^2, (z_{53})^{-2}$
total:	8	0	19	65	57

Table 9. Callgraph Statistics for SparseMVP

protocol	preprocessed	input	new	oracles queried	queried in
SparseMVP		$f_{\boldsymbol{a}}, f_{\boldsymbol{b}}$	$f_{\boldsymbol{\alpha}^\intercal M}$		
				$f_{\boldsymbol{b}}$	α_{smvp}
				$f_{\boldsymbol{\alpha}^\intercal M}$	β_{smvp}
- InnerProduct		$f_{\boldsymbol{a}}, f_{\boldsymbol{\alpha}^\intercal M}$	h_{33}		
-				$\bar{h}_{33}$	$z_{34}, (z_{34})^{-1}$
-				$f_{\boldsymbol{a}}$	$(z_{34})^2, (z_{34})^{-2}$
-				$f_{\boldsymbol{\alpha}^\intercal M}$	$(z_{34})^2, (z_{34})^{-2}$
- SparseBiEval	f_c		f_u, f_v, f_{uv}		
- - SparseMonomialVector		f_u	$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$		
- -				f_u	x_{35}
- - - VandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- - -				$f_{\hat{\boldsymbol{y}}}$	δ_{36}
- - -				$f_{\hat{\boldsymbol{\delta}}}$	z_{37}
- - - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$			
- - - -				$f_{\varphi(a_k)^H}$	$\delta_{36}^H \alpha_{38}$
- - - -				f_I	α_{38}
- - - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}$	h_{39}		
- - - - -				$\bar{h}_{39}$	$z_{40}, (z_{40})^{-1}$
- - - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{38} z_{40})^2, (\alpha_{38} z_{40})^{-2}$
- - - - -				$f_{\varphi(a_k)}$	$(\delta_{36} z_{40})^2, (\delta_{36} z_{40})^{-2}$
- - - - -				f_I	$(z_{40})^2, (z_{40})^{-2}$
- - - LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- - -				$f_{\hat{\boldsymbol{z}}}$	γ_{41}
- - -				$f_{\hat{\boldsymbol{\gamma}}}$	z_{42}
- - -				$Z_{\mathcal{H}}$	γ_{41}
- - - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - - -				$f_{\mathcal{H}}$	α_{43}
- - - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_{44}		
- - - - -				$\bar{h}_{44}$	$z_{45}, (z_{45})^{-1}$
- - - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{43} z_{45})^2, (\alpha_{43} z_{45})^{-2}$
- - - - -				f_I	$(z_{45})^2, (z_{45})^{-2}$
- - - - -				$f_{\varphi(h)}$	$(z_{45})^2, (z_{45})^{-2}$
- - - InnerProduct		$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$	h_{46}		
- - -				$\bar{h}_{46}$	$z_{47}, (z_{47})^{-1}$
- - -				$f_{\hat{\boldsymbol{z}}}$	$(z_{47})^2, (z_{47})^{-2}$
- - -				$f_{\hat{\boldsymbol{y}}}$	$(z_{47})^2, (z_{47})^{-2}$
- - SparseMonomialVector		f_v	$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$		
- -				f_v	x_{48}
- - - VandermondeVector	$f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- - -				$f_{\hat{\boldsymbol{y}}}$	δ_{49}
- - -				$f_{\hat{\boldsymbol{\delta}}}$	z_{50}
- - - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$			
- - - -				$f_{\varphi(b_k)^H}$	$\delta_{49}^H \alpha_{51}$
- - - -				f_I	α_{51}
- - - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(b_k)}$	h_{52}		
- - - - -				$\bar{h}_{52}$	$z_{53}, (z_{53})^{-1}$
- - - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{51} z_{53})^2, (\alpha_{51} z_{53})^{-2}$
- - - - -				$f_{\varphi(b_k)}$	$(\delta_{49} z_{53})^2, (\delta_{49} z_{53})^{-2}$
- - - - -				f_I	$(z_{53})^2, (z_{53})^{-2}$
- - - LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- - -				$f_{\hat{\boldsymbol{z}}}$	γ_{54}
- - -				$f_{\hat{\boldsymbol{\gamma}}}$	z_{55}
- - -				$Z_{\mathcal{H}}$	γ_{54}
- - - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - - -				$f_{\mathcal{H}}$	α_{56}
- - - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_{57}		
- - - - -				$\bar{h}_{57}$	$z_{58}, (z_{58})^{-1}$
- - - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{56} z_{58})^2, (\alpha_{56} z_{58})^{-2}$
- - - - -				f_I	$(z_{58})^2, (z_{58})^{-2}$
- - - - -				$f_{\varphi(h)}$	$(z_{58})^2, (z_{58})^{-2}$
- - - InnerProduct		$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$	h_{59}		
- - -				$\bar{h}_{59}$	$z_{60}, (z_{60})^{-1}$
- - -				$f_{\hat{\boldsymbol{z}}}$	$(z_{60})^2, (z_{60})^{-2}$
- - -				$f_{\hat{\boldsymbol{y}}}$	$(z_{60})^2, (z_{60})^{-2}$
- - Hadamard		f_u, f_v, f_{uv}			
- -				f_{uv}	α_{61}
- - - InnerProduct		f_u, f_v	h_{62}		
- - -				$\bar{h}_{62}$	$z_{63}, (z_{63})^{-1}$
- - -				f_u	$(\alpha_{61} z_{63})^2, (\alpha_{61} z_{63})^{-2}$
- - -				f_v	$(z_{63})^2, (z_{63})^{-2}$
- - InnerProduct		f_{uv}, f_c	h_{64}		
- -				$\bar{h}_{64}$	$z_{65}, (z_{65})^{-1}$
- -				f_{uv}	$(z_{65})^2, (z_{65})^{-2}$
- -				f_c	$(z_{65})^2, (z_{65})^{-2}$
total:	8	2	21	73	63

Table 10. Callgraph Statistics for SparseClaymore

protocol	preprocessed	input	new	oracles queried	queried in
SparseClaymore		$f_{\mathbf{x}}$	f_{wl}, f_{wr}, f_{wo}		
- SparseMVP		$f_{wl}, f_{wr}, f_{wo}, f_{\mathbf{x}}$	$f_{\boldsymbol{\alpha}^\intercal M}$		
-				$f_{\mathbf{x}}$	α_{smvp}
-				$f_{\boldsymbol{\alpha}^\intercal M}$	β_{smvp}
- - InnerProduct		$f_{wl}, f_{wr}, f_{wo}, f_{\boldsymbol{\alpha}^\intercal M}$	h_{146}		
- -				$\bar{h}_{146}$	$z_{147}, (z_{147})^{-1}$
- -				f_{wl}	$(z_{147})^2, (z_{147})^{-2}$
- -				f_{wr}	$(z_{147})^2, (z_{147})^{-2}$
- -				f_{wo}	$(z_{147})^2, (z_{147})^{-2}$
- -				$f_{\boldsymbol{\alpha}^\intercal M}$	$(z_{147})^2, (z_{147})^{-2}$
- - SparseBiEval	f_c		f_u, f_v, f_{uv}		
- - - SparseMonomialVector		f_u	$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$		
- - -				f_u	x_{148}
- - - - VandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- - - -				$f_{\hat{\boldsymbol{y}}}$	δ_{149}
- - - -				$f_{\hat{\boldsymbol{\delta}}}$	z_{150}
- - - - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(a_k)^H}$			
- - - - -				$f_{\varphi(a_k)^H}$	$\delta_{149}^H \alpha_{151}$
- - - - -				f_I	α_{151}
- - - - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}$	h_{152}		
- - - - - -				$\bar{h}_{152}$	$z_{153}, (z_{153})^{-1}$
- - - - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{151} z_{153})^2, (\alpha_{151} z_{153})^{-2}$
- - - - - -				$f_{\varphi(a_k)}$	$(\delta_{149} z_{153})^2, (\delta_{149} z_{153})^{-2}$
- - - - - -				f_I	$(z_{153})^2, (z_{153})^{-2}$
- - - - LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- - - -				$f_{\hat{\boldsymbol{z}}}$	γ_{154}
- - - -				$f_{\hat{\boldsymbol{\gamma}}}$	z_{155}
- - - -				$Z_{\mathcal{H}}$	γ_{154}
- - - - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - - - -				$f_{\mathcal{H}}$	α_{156}
- - - - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_{157}		
- - - - - -				$\bar{h}_{157}$	$z_{158}, (z_{158})^{-1}$
- - - - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{156} z_{158})^2, (\alpha_{156} z_{158})^{-2}$
- - - - - -				f_I	$(z_{158})^2, (z_{158})^{-2}$
- - - - - -				$f_{\varphi(h)}$	$(z_{158})^2, (z_{158})^{-2}$
- - - - InnerProduct		$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$	h_{159}		
- - - -				$\bar{h}_{159}$	$z_{160}, (z_{160})^{-1}$
- - - -				$f_{\hat{\boldsymbol{z}}}$	$(z_{160})^2, (z_{160})^{-2}$
- - - -				$f_{\hat{\boldsymbol{y}}}$	$(z_{160})^2, (z_{160})^{-2}$
- - - SparseMonomialVector		f_v	$f_{\hat{\boldsymbol{x}}}, f_{\hat{\boldsymbol{y}}}$		
- - -				f_v	x_{161}
- - - - VandermondeVector	$f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- - - -				$f_{\hat{\boldsymbol{y}}}$	δ_{162}
- - - -				$f_{\hat{\boldsymbol{\delta}}}$	z_{163}
- - - - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$			
- - - - -				$f_{\varphi(b_k)^H}$	$\delta_{162}^H \alpha_{164}$
- - - - -				f_I	α_{164}
- - - - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(b_k)}$	h_{165}		
- - - - - -				$\bar{h}_{165}$	$z_{166}, (z_{166})^{-1}$
- - - - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_{164} z_{166})^2, (\alpha_{164} z_{166})^{-2}$
- - - - - -				$f_{\varphi(b_k)}$	$(\delta_{162} z_{166})^2, (\delta_{162} z_{166})^{-2}$
- - - - - -				f_I	$(z_{166})^2, (z_{166})^{-2}$
- - - - LagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\boldsymbol{z}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- - - -				$f_{\hat{\boldsymbol{z}}}$	γ_{167}
- - - -				$f_{\hat{\boldsymbol{\gamma}}}$	z_{168}
- - - -				$Z_{\mathcal{H}}$	γ_{167}
- - - - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - - - -				$f_{\mathcal{H}}$	α_{169}
- - - - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_{170}		
- - - - - -				$\bar{h}_{170}$	$z_{171}, (z_{171})^{-1}$
- - - - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_{169} z_{171})^2, (\alpha_{169} z_{171})^{-2}$
- - - - - -				f_I	$(z_{171})^2, (z_{171})^{-2}$
- - - - - -				$f_{\varphi(h)}$	$(z_{171})^2, (z_{171})^{-2}$
- - - - InnerProduct		$f_{\hat{\boldsymbol{z}}}, f_{\hat{\boldsymbol{y}}}$	h_{172}		
- - - -				$\bar{h}_{172}$	$z_{173}, (z_{173})^{-1}$
- - - -				$f_{\hat{\boldsymbol{z}}}$	$(z_{173})^2, (z_{173})^{-2}$
- - - -				$f_{\hat{\boldsymbol{y}}}$	$(z_{173})^2, (z_{173})^{-2}$
- - - Hadamard		f_u, f_v, f_{uv}			
- - -				f_{uv}	α_{174}
- - - - InnerProduct		f_u, f_v	h_{175}		
- - - -				$\bar{h}_{175}$	$z_{176}, (z_{176})^{-1}$
- - - -				f_u	$(\alpha_{174} z_{176})^2, (\alpha_{174} z_{176})^{-2}$
- - - -				f_v	$(z_{176})^2, (z_{176})^{-2}$
- - - InnerProduct		f_{uv}, f_c	h_{177}		
- - -				$\bar{h}_{177}$	$z_{178}, (z_{178})^{-1}$
- - -				f_{uv}	$(z_{178})^2, (z_{178})^{-2}$
- - -				f_c	$(z_{178})^2, (z_{178})^{-2}$
- Hadamard		f_{wl}, f_{wr}, f_{wo}			
-				f_{wo}	α_{179}
- - InnerProduct		f_{wl}, f_{wr}	h_{180}		
- -				$\bar{h}_{180}$	$z_{181}, (z_{181})^{-1}$
- -				f_{wl}	$(\alpha_{179} z_{181})^2, (\alpha_{179} z_{181})^{-2}$
- -				f_{wr}	$(z_{181})^2, (z_{181})^{-2}$
total:	8	1	25	84	70
with BatchedInnerProduct:	8	1	16	66	40
and witness concatenation:	8	1	15	64	40

Table 11. Callgraph Statistics for BiVandermondeVector

protocol	preprocessed	input	new	oracles queried	queried in
BiVandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\mathbf{z}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
				$f_{\hat{\mathbf{z}}}$	δ_0
				$f_{\hat{\boldsymbol{\delta}}}$	z_1
- Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)^H}$			
-				$f_{\varphi(a_k)^H}$	α_2
-				f_I	α_2
-				$f_{\varphi(b_k)^H}$	α_2
- - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}$	h_3		
- -				$\bar{h}_3$	$z_4, (z_4)^{-1}$
- -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_2 z_4)^2, (\alpha_2 z_4)^{-2}$
- -				$f_{\varphi(a_k)}$	$(z_4)^2, (z_4)^{-2}$
- -				f_I	$(z_4)^2, (z_4)^{-2}$
- -				$f_{\varphi(b_k)}$	$(z_4)^2, (z_4)^{-2}$
total:	4	1	2	12	9

Table 12. Callgraph Statistics for BiLagrangeVector

protocol	preprocessed	input	new	oracles queried	queried in
BiLagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
				$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}$	γ_0
				$f_{\hat{\boldsymbol{\gamma}}}$	z_1
				$Z_{\mathcal{H}}$	γ_0
- Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
-				$f_{\mathcal{H}}$	α_2
- - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_3		
- -				$\bar{h}_3$	$z_4, (z_4)^{-1}$
- -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_2 z_4)^2, (\alpha_2 z_4)^{-2}$
- -				f_I	$(z_4)^2, (z_4)^{-2}$
- -				$f_{\varphi(h)}$	$(z_4)^2, (z_4)^{-2}$
total:	3	1	2	10	9

Table 13. Call graph statistics for BatchedSparseBiEval

protocol	preprocessed	input	new	oracles queried	queried in
BatchedSparseBiEval	f_c		$f_{u\|v}, f_{uv}, f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}, f_{\hat{\mathbf{y}}}$	$f_{u\|v}$	y_{10}
- BiLagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
-				$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}$	γ_0
-				$f_{\hat{\boldsymbol{\gamma}}}$	z_1
-				$Z_{\mathcal{H}}$	γ_0
- - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- -				$f_{\mathcal{H}}$	α_2
- - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_3		
- - -				$\bar{h}_3$	$z_4, (z_4)^{-1}$
- - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_2 z_4)^2, (\alpha_2 z_4)^{-2}$
- - -				f_I	$(z_4)^2, (z_4)^{-2}$
- - -				$f_{\varphi(h)}$	$(z_4)^2, (z_4)^{-2}$
- BiVandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\mathbf{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
-				$f_{\hat{\mathbf{y}}}$	δ_5
-				$f_{\hat{\boldsymbol{\delta}}}$	z_6
- - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)^H}$			
- -				$f_{\varphi(a_k)^H}$	α_7
- -				f_I	α_7
- -				$f_{\varphi(b_k)^H}$	α_7
- - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}$	h_8		
- - -				$\bar{h}_8$	$z_9, (z_9)^{-1}$
- - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_7 z_9)^2, (\alpha_7 z_9)^{-2}$
- - -				$f_{\varphi(a_k)}$	$(z_9)^2, (z_9)^{-2}$
- - -				f_I	$(z_9)^2, (z_9)^{-2}$
- - -				$f_{\varphi(b_k)}$	$(z_9)^2, (z_9)^{-2}$
- InnerProduct		$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}, f_{\hat{\mathbf{y}}}$	h_{11}		
-				$\bar{h}_{11}$	$z_{12}, (z_{12})^{-1}$
-				$f_{\hat{\mathbf{u}}\hat{\mathbf{v}}}$	$(z_{12})^2, (z_{12})^{-2}$
-				$f_{\hat{\mathbf{y}}}$	$(z_{12})^2, (z_{12})^{-2}$
- Hadamard		$f_{u\|v}, f_{u\|v}, f_{uv}$			
-				f_{uv}	α_{13}
- - InnerProduct		$f_{u\|v}, f_{u\|v}$	h_{14}		
- -				$\bar{h}_{14}$	$z_{15}, (z_{15})^{-1}$
- -				$f_{u\|v}$	$(z_{15})^2, (z_{15})^{-2}$
- InnerProduct		f_{uv}, f_c	h_{16}		
-				$\bar{h}_{16}$	$z_{17}, (z_{17})^{-1}$
-				f_{uv}	$(z_{17})^2, (z_{17})^{-2}$
-				f_c	$(z_{17})^2, (z_{17})^{-2}$
total:	8	0	11	40	32

Table 14. Call graph statistics for SparseMVP but with BatchedSparseBiEval

protocol	preprocessed	input	new	oracles queried	queried in
BiSparseMVP		$f_{\boldsymbol{a}}, f_{\boldsymbol{b}}$	$f_{\boldsymbol{\alpha}^\intercal M}$		
				$f_{\boldsymbol{b}}$	α_{smvp}
				$f_{\boldsymbol{\alpha}^\intercal M}$	β_{smvp}
- InnerProduct		$f_{\boldsymbol{a}}, f_{\boldsymbol{\alpha}^\intercal M}$	h_0		
-				$\bar{h}_0$	$z_1, (z_1)^{-1}$
-				$f_{\boldsymbol{a}}$	$(z_1)^2, (z_1)^{-2}$
-				$f_{\boldsymbol{\alpha}^\intercal M}$	$(z_1)^2, (z_1)^{-2}$
- BatchedSparseBiEval	f_c		$f_{u\|v}, f_{uv}, f_{\mathbf{uv}}, f_{\hat{\boldsymbol{y}}}$		
-				$f_{u\|v}$	y_{12}
- - BiLagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\mathbf{uv}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- -				$f_{\mathbf{uv}}$	γ_2
- -				$f_{\hat{\boldsymbol{\gamma}}}$	z_3
- -				$Z_{\mathcal{H}}$	γ_2
- - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - -				$f_{\mathcal{H}}$	α_4
- - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_5		
- - - -				$\bar{h}_5$	$z_6, (z_6)^{-1}$
- - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_4 z_6)^2, (\alpha_4 z_6)^{-2}$
- - - -				f_I	$(z_6)^2, (z_6)^{-2}$
- - - -				$f_{\varphi(h)}$	$(z_6)^2, (z_6)^{-2}$
- - BiVandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\boldsymbol{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- -				$f_{\hat{\boldsymbol{y}}}$	δ_7
- -				$f_{\hat{\boldsymbol{\delta}}}$	z_8
- - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)^H}$			
- - -				$f_{\varphi(a_k)^H}$	α_9
- - -				f_I	α_9
- - -				$f_{\varphi(b_k)^H}$	α_9
- - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}$	h_{10}		
- - - -				$\bar{h}_{10}$	$z_{11}, (z_{11})^{-1}$
- - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_9 z_{11})^2, (\alpha_9 z_{11})^{-2}$
- - - -				$f_{\varphi(a_k)}$	$(z_{11})^2, (z_{11})^{-2}$
- - - -				f_I	$(z_{11})^2, (z_{11})^{-2}$
- - - -				$f_{\varphi(b_k)}$	$(z_{11})^2, (z_{11})^{-2}$
- - InnerProduct		$f_{\mathbf{uv}}, f_{\hat{\boldsymbol{y}}}$	h_{13}		
- -				$\bar{h}_{13}$	$z_{14}, (z_{14})^{-1}$
- -				$f_{\mathbf{uv}}$	$(z_{14})^2, (z_{14})^{-2}$
- -				$f_{\hat{\boldsymbol{y}}}$	$(z_{14})^2, (z_{14})^{-2}$
- - Hadamard		$f_{u\|v}, f_{u\|v}, f_{uv}$			
- -				f_{uv}	α_{15}
- - - InnerProduct		$f_{u\|v}, f_{u\|v}$	h_{16}		
- - -				$\bar{h}_{16}$	$z_{17}, (z_{17})^{-1}$
- - -				$f_{u\|v}$	$(z_{17})^2, (z_{17})^{-2}$
- - InnerProduct		f_{uv}, f_c	h_{18}		
- -				$\bar{h}_{18}$	$z_{19}, (z_{19})^{-1}$
- -				f_{uv}	$(z_{19})^2, (z_{19})^{-2}$
- -				f_c	$(z_{19})^2, (z_{19})^{-2}$
total:	8	2	13	48	38

Table 15. Call graph statistics for SparseClaymore but with batched BatchedSparseBiEval

protocol	preprocessed	input	new	oracles queried	queried in
SparseClaymore		$f_{\mathbf{x}}$	f_{wl}, f_{wr}, f_{wo}		
- BiSparseMVP		$f_{wl}, f_{wr}, f_{wo}, f_{\mathbf{x}}$	$f_{\boldsymbol{\alpha}^\intercal M}$		
-				$f_{\mathbf{x}}$	α_{smvp}
-				$f_{\boldsymbol{\alpha}^\intercal M}$	β_{smvp}
- - InnerProduct		$f_{wl}, f_{wr}, f_{wo}, f_{\boldsymbol{\alpha}^\intercal M}$	h_0		
- -				$\bar{h}_0$	$z_1, (z_1)^{-1}$
- -				f_{wl}	$(z_1)^2, (z_1)^{-2}$
- -				f_{wr}	$(z_1)^2, (z_1)^{-2}$
- -				f_{wo}	$(z_1)^2, (z_1)^{-2}$
- -				$f_{\boldsymbol{\alpha}^\intercal M}$	$(z_1)^2, (z_1)^{-2}$
- - BatchedSparseBiEval	f_c		$f_{u\|v}, f_{uv}, f_{\mathbf{uv}}, f_{\hat{\mathbf{y}}}$		
- -				$f_{u\|v}$	y_{12}
- - - BiLagrangeVector	$f_{\varphi(h)}, f_{\mathcal{H}}, Z_{\mathcal{H}}$	$f_{\mathbf{uv}}$	$f_{\hat{\boldsymbol{\gamma}}}$		
- - -				$f_{\mathbf{uv}}$	γ_2
- - -				$f_{\hat{\boldsymbol{\gamma}}}$	z_3
- - -				$Z_{\mathcal{H}}$	γ_2
- - - - Hadamard		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}, f_{\mathcal{H}}$			
- - - -				$f_{\mathcal{H}}$	α_4
- - - - - InnerProduct		$f_{\hat{\boldsymbol{\gamma}}}, f_{\varphi(h)}$	h_5		
- - - - -				$\bar{h}_5$	$z_6, (z_6)^{-1}$
- - - - -				$f_{\hat{\boldsymbol{\gamma}}}$	$(\alpha_4 z_6)^2, (\alpha_4 z_6)^{-2}$
- - - - -				f_I	$(z_6)^2, (z_6)^{-2}$
- - - - -				$f_{\varphi(h)}$	$(z_6)^2, (z_6)^{-2}$
- - - BiVandermondeVector	$f_{\varphi(a_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)}, f_{\varphi(b_k)^H}$	$f_{\hat{\mathbf{y}}}$	$f_{\hat{\boldsymbol{\delta}}}$		
- - -				$f_{\hat{\mathbf{y}}}$	δ_7
- - -				$f_{\hat{\boldsymbol{\delta}}}$	z_8
- - - - Hadamard		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}, f_{\varphi(a_k)^H}, f_{\varphi(b_k)^H}$			
- - - -				$f_{\varphi(a_k)^H}$	α_9
- - - -				f_I	α_9
- - - -				$f_{\varphi(b_k)^H}$	α_9
- - - - - InnerProduct		$f_{\hat{\boldsymbol{\delta}}}, f_{\varphi(a_k)}, f_{\varphi(b_k)}$	h_{10}		
- - - - -				$\bar{h}_{10}$	$z_{11}, (z_{11})^{-1}$
- - - - -				$f_{\hat{\boldsymbol{\delta}}}$	$(\alpha_9 z_{11})^2, (\alpha_9 z_{11})^{-2}$
- - - - -				$f_{\varphi(a_k)}$	$(z_{11})^2, (z_{11})^{-2}$
- - - - -				f_I	$(z_{11})^2, (z_{11})^{-2}$
- - - - -				$f_{\varphi(b_k)}$	$(z_{11})^2, (z_{11})^{-2}$
- - - InnerProduct		$f_{\mathbf{uv}}, f_{\hat{\mathbf{y}}}$	h_{13}		
- - -				$\bar{h}_{13}$	$z_{14}, (z_{14})^{-1}$
- - -				$f_{\mathbf{uv}}$	$(z_{14})^2, (z_{14})^{-2}$
- - -				$f_{\hat{\mathbf{y}}}$	$(z_{14})^2, (z_{14})^{-2}$
- - - Hadamard		$f_{u\|v}, f_{u\|v}, f_{uv}$			
- - -				f_{uv}	α_{15}
- - - - InnerProduct		$f_{u\|v}, f_{u\|v}$	h_{16}		
- - - -				$\bar{h}_{16}$	$z_{17}, (z_{17})^{-1}$
- - - -				$f_{u\|v}$	$(z_{17})^2, (z_{17})^{-2}$
- - - InnerProduct		f_{uv}, f_c	h_{18}		
- - -				$\bar{h}_{18}$	$z_{19}, (z_{19})^{-1}$
- - -				f_{uv}	$(z_{19})^2, (z_{19})^{-2}$
- - -				f_c	$(z_{19})^2, (z_{19})^{-2}$
- Hadamard		f_{wl}, f_{wr}, f_{wo}			
-				f_{wo}	α_{20}
- - InnerProduct		f_{wl}, f_{wr}	h_{21}		
- -				$\bar{h}_{21}$	$z_{22}, (z_{22})^{-1}$
- -				f_{wl}	$(\alpha_{20} z_{22})^2, (\alpha_{20} z_{22})^{-2}$
- -				f_{wr}	$(z_{22})^2, (z_{22})^{-2}$
total:	8	1	17	59	45
with BatchedInnerProduct:	8	1	11	47	21
and witness concatenation:	8	1	10	45	21