Efficient NIZK for NP without Knowledge Assumptions

Alonso González[1]

Mi casita

Abstract. Insert abstract here.

1 Introduction

In this work we construct a NIZK proof system for the language

$$\mathsf{CircuitSat} := \{C : \exists x \in \{0,1\}^* \text{ s.t. } C(x) = 1\},$$

with proof size $2|x| + \Theta(\text{depth}(C))$ elements of a bilinear group. We do so by constructing a QA-NIZK proof system for the language

$$\mathsf{CircuitSat}_{ck} := \left\{ \begin{array}{l} ([\zeta_1]_1, \ldots, [\zeta_n]_1, C) : \exists x_1, \ldots, x_n \in \{0,1\}, w_1, \ldots, w_n \in \mathbb{Z}_q \text{ s.t.} \\ C(x) = 1 \text{ and } \forall i \in [n]\ [\zeta_i]_1 = \mathsf{GS.Com}_{ck}([x_i]_1; w_i) \end{array} \right\},$$

with proof size $\Theta(\text{depth}(C))$.

The first case is the more general form of a set-membership proof where the set is dynamically chosen. In the second case each instance of the proof system is fixed to a specific set (encoded in the CRS) and is the same notion of the proofs for "fixed sets" from Section **??**. We note that the aggregated set-membership proofs for $S \subset \mathbb{G}_s$ from Chapter **??** are proofs of membership in $\mathcal{L}^n_{ck,S}$.

In Section **??**, we start with an intuitive description for the case $S \subset \mathbb{Z}_q$ without aggregation. We note that even in this simpler case, to the best of our knowledge, the shortest non-interactive proof, under falsifiable assumptions and without assuming anything about S,[1] that exists in the literature is the one of Chandran et al. of size $\Theta(\sqrt{|S|})$. Our approach is to commit to the binary representation $(b_1, \ldots, b_{\log t}) \in \{0,1\}^{\log t}$ of the index of the purported $x \in S$, for $S = \{s_1, \ldots, s_t\}$ and where b_1 is the least significant bit, to select the the leaves under the paths $(b_{\log t}), (b_{\log t}, b_{\log t-1}), \ldots, (b_{\log t}, \ldots, b_1)$ in the binary tree whose leaves are (from left to right) $s_1, \ldots, s_t$. In order to keep a logarithmic proof, we commit to the selected leaves using MP commitments from Section **??** and show, for each $\ell \in [\log t]$, that the leaves under the path $(b_m, \cdots, b_\ell)$ are equal the leftmost or rightmost, depending of b_ℓ, leaves under the path $(b_{\log t}, \cdots, b_{\ell-1})$. We use these ideas together with a clever usage of QA-NIZK proofs of membership in linear subspaces, Groth-Sahai proofs, and the proof systems from Chapters **??** and **??**.

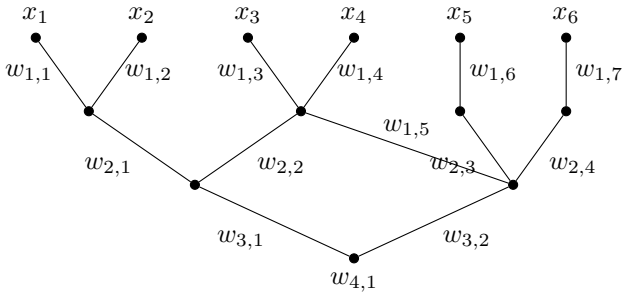
[1] If $S = [a, b] \subset \mathbb{Z}_q$ and $a < b$ we can use range proofs.

In Section **??** we give a full description of the non-aggregated case and then we show how to extend this result to the case $S \subset \mathbb{G}_s$. We use the ideas from Section **??** and aggregate many instances using similar techniques to those from Chapter **??**. We note that, to the best of our knowledge, there is no aggregated proof in the literature (i.e. all proofs are of size $\Omega(n)$) with the sole exception of our proof from Section **??** which is of size $\Theta(|S|)$. Our proof bears some similarities with the work of Groth and Kohlweiss [**?**] – both allow to construct proofs of membership in a set of logarithmic size using the binary encoding of the element index – but they are in general incomparable. Indeed, Groth and Kohlweiss's construction is on a different setting (interactive, without pairings) and does not support aggregation of many proofs.

There is a straightforward application of the improved aZKSMP. In the proof of a shuffle from Section **??**, the size of the proof that $[\mathbf{F}] \in \mathcal{L}^n_{ck,S}$ can be reduced from $2n+\Theta(1)$ to $\Theta(\log n)$ and thus the total proof size is reduced from $4n+o(n)$ to $2n + o(n)$.

1.1 Intuition

We represent a circuit C with a binary tree as described below



without aggregation, that is, there is a single commitment $[\boldsymbol{c}]_1 = \mathsf{GS.Com}_{ck_{\mathsf{GS}}}(x; r)$ and we want to show that $x = s_\alpha$, for some $\alpha \in [t]$. In Section **??** we will show how to aggregate many proofs.

The (non-aggregated) proof from Section **??** essentially codifies the position α as a weight 1 binary vector $\boldsymbol{b}$ of size t such that $x = \sum_{i\in[t]} b_i s_i$ and $b_i = 1$ if $i = \alpha$ and 0 if not.[2] A step further in efficiency was given by Chandran et al. [**?**] (already discussed in Section **??**). There the position α is codified as two weight 1 binary vectors $\boldsymbol{b}$ and $\boldsymbol{b}'$ of size $\sqrt{t}$ such that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{\sqrt{t}} \end{pmatrix} = \sum_{i=1}^{\sqrt{t}} b_i \begin{pmatrix} s_{(i-1)\sqrt{t}+1} \\ \vdots \\ s_{(i-1)\sqrt{t}+\sqrt{t}} \end{pmatrix}, \; x = \sum_{i=1}^{\sqrt{t}} b'_i x_i,$$

and $b_i = 1$ iff $i = i_\alpha$ and $b'_j = 1$ iff $j = j_\alpha$, where $\alpha = (i_\alpha - 1)\sqrt{t} + j_\alpha$. Since $\sqrt{t}$ new variables are added (variables $x_1, \ldots, x_{\sqrt{t}}$), the proof must contain $\sqrt{t}$ new

[2] The case $S \subset \mathbb{Z}_q$ is not really discussed in Section **??**, but it is straightforward that the same techniques from the case $S \subset \mathbb{G}_s$ apply.

commitments to these variables. However, this does not not affect the asymptotic size of the proof, which is $\Theta(\sqrt{t})$ anyway.

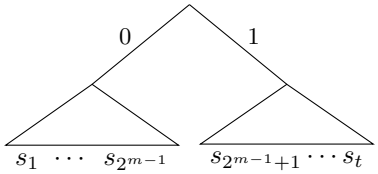
Let $m := \log t$.[3] The natural next step is to codify α as m weight 1 binary vectors of size 2 (note that a weight 1 binary vector of size 2 can be always written as $(1-b, b)$, $b \in \{0,1\}$) such that

$$\begin{pmatrix} x_{\ell,1} \\ \vdots \\ x_{\ell,2^{\ell-1}} \end{pmatrix} = (1-b_\ell) \begin{pmatrix} x_{\ell+1,1} \\ \vdots \\ x_{\ell+1,2^{\ell-1}} \end{pmatrix} + b_\ell \begin{pmatrix} x_{\ell+1,2^{\ell-1}+1} \\ \vdots \\ x_{\ell+1,2^\ell} \end{pmatrix} \text{ if } \ell \in [m], \tag{1}$$

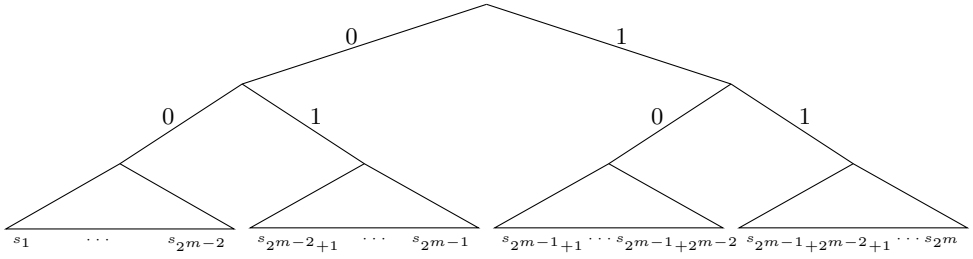
$$x = x_{1,1}, \tag{2}$$

where $x_{m+1,i} := s_i$, $i \in [t]$, and $\alpha = \sum_{i=1}^{m} b_i 2^{i-1} + 1$. Note that we have added the additional variables $x_{\ell,i}$, $\ell \in [m]$ and $i \in [2^\ell]$.

Consider the binary tree whose leaves are $x_{m+1,1} = s_1, \ldots, x_{m+1,t} = s_t$, where the leftmost leaf is s_1 and the rightmost leaf is $s_{2^m} = s_t$. Intuitively, equation (1) for $\ell = m$ says that variables $x_{m,1}, \ldots, x_{m,2^{m-1}}$ are the leaves of the subtree under the path (b_m). For example, if $b_m = 1$, the variables $x_{m,1}, \ldots, x_{m,2^{m-1}}$ are equal to $s_{2^{m-1}+1}, \ldots, s_t$, which are the leaves of the subtree under the path (1) as depicted below.



Similarly, equation (1) for $\ell = m-1$ says that variables $x_{m-1,1}, \ldots, x_{m-1,2^{m-2}}$ are the leaves of the subtree under the path (b_m, b_{m-1}). For example, if $(b_m, b_{m-1}) = (1,0)$, the variables $x_{m-1,1}, \ldots, x_{m-1,2^{m-2}}$ are equal to $x_{m,1} = s_{2^{m-1}+1}, \ldots, x_{m,2^{m-2}} = s_{2^{m-1}+2^{m-2}}$, which are the leaves of the subtree under the path (1,0) as depicted below.



[3] W.l.o.g. we assume that $\log t \in \mathbb{N}$, because we can always prove membership in the (multi-)set $S' = S \uplus_{i=1}^{2^{\lceil \log t \rceil} - t} \{s_t\}$ and it holds that $|S'| = 2^{\lceil \log t \rceil}$ and that $x \in S \iff x \in S'$.

In general, the variables $x_{\ell,1}, \ldots, x_{\ell,2^{\ell-1}}$ are equal to the leaves $s_{\mathsf{left}}, \ldots, s_{\mathsf{right}}$ under the path $(b_m, \ldots, b_\ell)$, where $\mathsf{left} = \sum_{i=\ell}^{m} b_i 2^{i-1} + 1$ and $\mathsf{right} = \mathsf{left} + 2^{\ell-1} - 1$. Therefore, for $\ell = 1$ equation (1) says that the variable $x_{1,1}$ is equal to the leaf $s_{\mathsf{left}} = s_{\mathsf{right}} = s_\alpha$, since $\mathsf{left} = \mathsf{right} = \sum_{i=1}^{m} b_i 2^{i-1} + 1 = \alpha$, which is the unique leaf (and the unique node) in the subtree under the path $(b_m, \ldots, b_1)$.

Similarly as in Chandran et al.'s proof, for each new variable a new commitment must be added to the proof. But, in contrast with Chandran et al.'s proof, in this case the additional commitments do increase the asymptotic size of the proof. Indeed, the total number of new variables is $2^{m-1} + 2^{m-2} + \ldots + 1 = 2^m - 1 = t - 1$, and thus $t - 1$ new commitments must be added.

One can reduce the total size of the commitments using the length reducing multi-Pedersen commitments from Section **??**. However, this must be done carefully in order to be able to express equation (1) with a Groth-Sahai proof of an equation that involves the MP commitments and the variables $b_1, \ldots, b_m$. For example, if one computes a single commitment to all variables $\mathsf{MP.Com}_{ck}((x_{1,1}, \ldots, x_{m,2^{m-1}})^\top; r)$ it is not clear how to use it to express equation (1), because not all the variables appear at once in this equation (but all the variables appear in the previous commitment). Our solution is to compute a single MP commitment to each vector that appears in equation (1) in order to show with Groth-Sahai proofs that

$$\begin{aligned}\mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} x_{\ell,1} \\ \vdots \\ x_{\ell,2^{\ell-1}} \end{pmatrix}; r_\ell\right) = (1-b_\ell)\mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} x_{\ell+1,1} \\ \vdots \\ x_{\ell+1,2^{\ell-1}} \end{pmatrix}; r_{\ell,1}\right) + \\ b_\ell \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} x_{\ell+1,2^{\ell-1}+1} \\ \vdots \\ x_{\ell+1,2^\ell} \end{pmatrix}; r_{\ell,2}\right) + \\ \mathsf{MP.Com}_{ck_\ell}(\mathbf{0}; y_\ell),\end{aligned}$$

$$\begin{aligned}&\iff \\ &\mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} x_{\ell,1} \\ \vdots \\ x_{\ell,2^{\ell-1}} \end{pmatrix} - (1-b_\ell)\begin{pmatrix} x_{\ell+1,1} \\ \vdots \\ x_{\ell+1,2^{\ell-1}} \end{pmatrix} - b_\ell \begin{pmatrix} x_{\ell+1,2^{\ell-1}+1} \\ \vdots \\ x_{\ell+1,2^\ell} \end{pmatrix}; \right. \\ &\qquad\qquad \left. r_\ell - (1-b_\ell) r_{\ell,1} - b_\ell r_{\ell,2} \right) \\ &= \mathsf{MP.Com}_{ck_\ell}(\mathbf{0}; y_\ell)\end{aligned}$$

for each $\ell \in [m]$ and some $y_\ell \in \mathbb{Z}_q$. In this way, we only need $3m = 3 \log t$ additional commitments. The reason for using different commitment keys for each $\ell \in [m]$ will be clear when we explain soundness.

Concretely, the prover computes

$$[\boldsymbol{c}_\ell]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell,1}, \ldots, x_{\ell,2^{\ell-1}})^\top; r_\ell),$$

for random $r_\ell \in \mathbb{Z}_q$ and $\ell \in [m]$, and

$$[\boldsymbol{c}_{\ell,1}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,1}, \ldots, x_{\ell+1,2^{\ell-1}})^\top; r_{\ell,1}),$$
$$[\boldsymbol{c}_{\ell,2}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,2^{m-1}+1}, \ldots, x_{\ell+1,2^\ell})^\top; r_{\ell,2}),$$

for random $r_{\ell,1}, r_{\ell,2} \in \mathbb{Z}_q$ and $\ell \in [m-1]$. Note that the prover does not need to compute commitments to $(x_{m+1,1}, \ldots, x_{m+1,t})^\top$ since $x_{m+1,i} = s_i$, $i \in [t]$, and thus they can be computed by the verifier.

Then, the prover shows that equation (1) holds with a GS proof of the satisfiability of

$$[\boldsymbol{c}_\ell]_1 - (1-b_\ell)[\boldsymbol{c}_{\ell,1}]_1 - b_\ell[\boldsymbol{c}_{\ell,2}]_1 = \mathsf{MP.Com}_{ck_\ell}(\mathbf{0}; y_\ell), \text{ for } \ell \in [m], \tag{3}$$

where $[\boldsymbol{c}_{m,1}] := \mathsf{MP.Com}_{ck_m}((s_1, \ldots, s_{2^{m-1}})^\top; 0)$ and $[\boldsymbol{c}_{m,2}] := \mathsf{MP.Com}_{ck_m}($ $(s_{2^{m-1}+1}, \ldots, s_t)^\top; 0)$ can be directly computed by the verifier, and $y_\ell := r_\ell - (1-b_\ell)r_{\ell,1} - b_\ell r_{\ell,2}$. It also computes Groth-Sahai proofs that

$$b_\ell(b_\ell - 1) = 0 \tag{4}$$

for each $\ell \in [m]$ (or equivalently a proof that $b_\ell \in \{0,1\}$).

The prover also shows that equation (2) is satisfied with a QA-NIZK proof that

$$[\boldsymbol{c}]_1 \text{ and } [\boldsymbol{c}_1]_1 \text{ open to the same value,} \tag{5}$$

using the proof system from Section **??**.

Note that variables $x_{\ell+1,1}, \ldots, x_{\ell+1,2^{\ell-1}}$ appear in both $[\boldsymbol{c}_{\ell,1}]_1$ and $[\boldsymbol{c}_{\ell+1}]_1$, as well as $x_{\ell+1,2^{\ell-1}+1}, \ldots, x_{\ell+1,2^\ell}$ appear in both $[\boldsymbol{c}_{\ell,2}]_1$ and $[\boldsymbol{c}_{\ell+1}]_1$. To get a sound proof, the prover needs to show that this redundancy is consistent. That is, the prover needs to show that $[\boldsymbol{c}_{\ell,1}]_1$ and $[\boldsymbol{c}_{\ell,2}]_1$ are commitments to the first and last halves of the opening of $[\boldsymbol{c}_{\ell+1}]_1$.

For $\ell \in [m]$, let $ck_\ell := ([\mathbf{G}_\ell]_1, [\boldsymbol{g}_{\ell,2^{\ell-1}+1}]_1) \in \mathbb{G}_1^{2\times 2^{\ell-1}+1}$ the commitment key of a MP commitment scheme and let

$$\mathbf{G}_{\ell,1} := \left(\boldsymbol{g}_{\ell,1} \cdots \boldsymbol{g}_{\ell,2^{\ell-2}}\right), \qquad \mathbf{G}_{\ell,2} := \left(\boldsymbol{g}_{\ell,2^{\ell-2}+1} \cdots \boldsymbol{g}_{\ell,2^{\ell-1}}\right)$$
$$\mathbf{G}_\ell := \mathbf{G}_{\ell,1} | \mathbf{G}_{\ell,2}$$

To prove consistency the prover will show that, for each $\ell \in [m-1]$, the following linear system is satisfied

$$\begin{pmatrix} \boldsymbol{c}_{\ell+1} \\ \boldsymbol{c}_{\ell,1} \\ \boldsymbol{c}_{\ell,2} \end{pmatrix} = \left(\begin{array}{cc|ccc} \mathbf{G}_{\ell+1,1} & \mathbf{G}_{\ell+1,2} & \boldsymbol{g}_{\ell+1,2^\ell+1} & \mathbf{0} & \mathbf{0} \\ \mathbf{G}_\ell & \mathbf{0}_{2\times 2^{\ell-1}} & \mathbf{0} & \boldsymbol{g}_{\ell,2^{\ell-1}+1} & \mathbf{0} \\ \mathbf{0}_{2\times 2^{\ell-1}} & \mathbf{G}_\ell & \mathbf{0} & \mathbf{0} & \boldsymbol{g}_{\ell,2^{\ell-1}+1} \end{array}\right) \boldsymbol{w}, \tag{6}$$

for some $\boldsymbol{w} \in \mathbb{Z}_q^{2^\ell+3}$, which can be proven using the proof system from Section **??**.

Intuitively, $\boldsymbol{w}$ should be equal to $(x_{\ell+1,1}, \ldots, x_{\ell+1,2^\ell}, r_{\ell+1}, r_{\ell,1}, r_{\ell,2})$ and thus

$$[\boldsymbol{c}_{\ell,1}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,1}, \ldots, x_{\ell+1,2^{\ell-1}})^\top; r_{\ell,1}) \text{ and}$$
$$[\boldsymbol{c}_{\ell,2}]_1 = \mathsf{MP.Com}_{ck_\ell}((x_{\ell+1,2^{\ell-1}+1}, \ldots, x_{\ell+1,2^\ell})^\top; r_{\ell,2}).$$

However, since multi-Pedersen commitments have multiple openings it might be the case that the satisfying witness of the proof is different from $(x_{\ell+1,1}, \ldots, x_{\ell+1,2^\ell}, r_{\ell+1}, r_{\ell,1}, r_{\ell,2})$ and thus the intuitive reasoning is invalid.

Despite this flawed reasoning, we will show that the proof system is still sound.

Soundness Intuition Suppose that an adversary against soundness outputs GS commitments to $b_1, \ldots, b_m \in \mathbb{Z}_q$, outputs commitments $[\boldsymbol{c}_\ell]_1$, $\ell \in [m]$, and $[\boldsymbol{c}_{\ell,1}]_1, [\boldsymbol{c}_{\ell,2}]$, $\ell \in [m-1]$, a GS proofs of the satisfiability of equation (3), and QA-NIZK proofs of (5) and (6) for each $\ell \in [m-1]$. Note that perfect soundness of Groth-Sahai proofs for equation (4) imply that $b_1, \ldots, b_m \in \{0,1\}$.

For $\ell \in [m]$, define α_ℓ as the position of s_α respective to the leaves under the path $(b_m, \ldots, b_\ell)$, that is $\alpha_\ell := \alpha - \mathsf{left} + 1$. Note that $\alpha_\ell \in [1, 2^{\ell-1}]$ since

$$1 \leq \alpha_\ell = \sum_{i=1}^{m} b_i 2^{i-1} - \sum_{i=\ell}^{m} b_i 2^{i-1} + 1 = \sum_{i=1}^{\ell-1} b_i 2^{i-1} + 1 \leq 2^{\ell-1}.$$

The key observation is that, for a fixed $\alpha \in [m]$, even if in equation (1) $x_{\ell,j}$ is not correctly computed for $j \neq \alpha_\ell$, it holds that $x_{m,1} = s_\alpha$ anyway. We will take advantage of this observation and the fact that the adversary commits to a fixed $\alpha = \sum_{i=1}^{n} b_i 2^{i-1} + 1$ to guarantee perfect soundness of equation (1) at least for coordinate α_ℓ for each $\ell \in [m]$. We do so by picking the commitment key ck_ℓ in such a way that its α_ℓ th column is linearly independent from the other columns. Although we will not be able to guarantee that $x_{\ell,j}$ is correctly computed if $j \neq \alpha_\ell$, at least we will be able to do so for x_{ℓ,α_ℓ}.

In the reduction we will guess the (sub-)path $(b_{m-1}, \ldots, b_1)$ (it will be not necessary to guess first the edge of the path) chosen by the adversary. While in the real scheme $\mathrm{rank}(\mathbf{G}_\ell) = 1$, for each $\ell \in [m]$, we jump to a game where $\boldsymbol{g}_{\ell,\alpha_\ell}$ is linearly independent from the other $2^{\ell-1}$ vectors in ck_ℓ. This can be done choosing random $b'_{m-1}, \ldots, b'_1 \in \{0,1\}$ and aborting if $(b'_{m-1}, \ldots, b'_1) \neq (b_{m-1}, \cdots, b_1)$. Therefore, our security reduction will have a security loss factor of $1/2^{m-1} = 2/t$. We sample $ck_\ell \leftarrow \mathcal{L}_1^{2^{\ell-1},\alpha_\ell}$, as defined on Section **??**, which implies that for every $\ell \in [m]$ there exists unique $\tilde{x}_\ell, \tilde{r}_\ell \in \mathbb{Z}_q$ such that $\boldsymbol{c}_\ell := \tilde{x}_\ell \boldsymbol{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \boldsymbol{g}_{\ell,2^{\ell-1}+1}$.

We prove by induction on ℓ that $\boldsymbol{c}_\ell = s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \boldsymbol{g}_{\ell,2^{\ell-1}+1}$, for some $\tilde{r}_\ell \in \mathbb{Z}_q$. If this is the case $\boldsymbol{c}_1 = s_\alpha \boldsymbol{g}_{1,1} + \tilde{r}_1 \boldsymbol{g}_{1,2}$. Soundness of proof for equation (5) together with the fact that ck_1 is perfectly binding implies that $x = \tilde{x}_1 = s_\alpha \in S$ which proves soundness.

First, it will be useful to prove the next lemma about α_ℓ.

Lemma 1. *Let $b_m, \ldots, b_1 \in \{0,1\}$. For all $\ell \in [m-1]$, $\alpha_{\ell+1} = \alpha_\ell + b_\ell 2^{\ell-1}$.*

Proof. To avoid confusion, define here $\mathsf{left}_\ell := \sum_{i=\ell}^{m} b_i 2^{i-1} + 1$ (previously simply defined as left, the index of the leftmost leaf under the path $(b_m, \cdots, b_\ell)$). It holds that

$$\begin{aligned}
\alpha_{\ell+1} &= \alpha - \mathsf{left}_{\ell+1} + 1 \\
&= \sum_{i=1}^{m} b_i 2^{i-1} - \sum_{i=\ell+1}^{m} b_i 2^{i-1} + 1 \\
&= \sum_{i=1}^{m} b_i 2^{i-1} - \sum_{i=\ell}^{m} b_i 2^{i-1} + 1 + b_\ell 2^{\ell-1} \\
&= \alpha - \mathsf{left}_\ell + 1 + b_\ell 2^{\ell-1} \\
&= \alpha_\ell + b_\ell 2^{\ell-1}
\end{aligned}$$

Now we prove that, for all $\ell \in [m]$, $\boldsymbol{c}_\ell = s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \boldsymbol{g}_{\ell,2^{\ell-1}+1}$. In the base case ($\ell = m$) the fact that $\boldsymbol{g}_{m,i} \in \mathbf{Span}(\boldsymbol{g}_{m,2^{m-1}+1})$ if $i \neq \alpha_m$ together with Lemma 1 implies that

$$\begin{aligned}
\boldsymbol{c}_m &= (1-b_m) \sum_{i=1}^{2^{m-1}} s_i \boldsymbol{g}_{m,i} + b_m \sum_{i=1}^{2^{m-1}} s_{i+2^{m-1}} \boldsymbol{g}_{m,i} \\
&= (1-b_m) s_{\alpha_m} \boldsymbol{g}_{m,\alpha_m} + b_m s_{\alpha_m + 2^{m-1}} \boldsymbol{g}_{m,\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,2^{m-1}+1} \\
&= (1-b_m) s_{\alpha - \mathsf{left}+1} \boldsymbol{g}_{m,\alpha_m} + b_m s_{\alpha - \mathsf{left}+1+2^{m-1}} \boldsymbol{g}_{m,\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,2^{m-1}+1} \\
&= \begin{cases} s_{\alpha-1+1} \boldsymbol{g}_{m,\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,t/2} & \text{if } b_m = 0 \text{ (and thus } \mathsf{left} = 1) \\ s_{\alpha-(2^{m-1}+1)+1+2^{m-1}} \boldsymbol{g}_{m,\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,t/2} & \text{if } b_m = 1 \text{ (and thus } \mathsf{left} = 2^{m-1}+1) \end{cases}
\end{aligned}$$

for some $\tilde{r}_1 \in \mathbb{Z}_q$. In both cases $\boldsymbol{c}_m = s_\alpha \boldsymbol{g}_{1,\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,t/2}$.

In the inductive case we assume that $\boldsymbol{c}_{\ell+1} = s_\alpha \boldsymbol{g}_{\ell+1,\alpha_{\ell+1}} + \tilde{r}_{\ell+1} \boldsymbol{g}_{\ell+1,2^\ell+1}$ and we want to show that $\boldsymbol{c}_\ell = s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + \tilde{r}_\ell \boldsymbol{g}_{\ell,2^{\ell-1}+1}$. Since $\boldsymbol{g}_{\ell+1,\alpha_{\ell+1}}$ is linearly independent from the rest of vectors in $ck_{\ell+1}$, any solution to equation (6) is equal to s_α at position $\alpha_{\ell+1} = \alpha_\ell + b_\ell 2^{\ell-1}$ as depicted below.

$$\begin{pmatrix} \boldsymbol{c}_{\ell+1} \\ \boldsymbol{c}_{\ell,1} \\ \boldsymbol{c}_{\ell,2} \end{pmatrix} = \begin{pmatrix} \cdots & \boldsymbol{g}_{\ell+1,\alpha_\ell} & \cdots & \boldsymbol{g}_{\ell+1,\alpha_\ell+2^{\ell-1}} & \cdots \\ \cdots & \boldsymbol{g}_{\ell,\alpha_\ell} & \cdots & \mathbf{0} & \cdots \\ \cdots & \mathbf{0} & \cdots & \boldsymbol{g}_{\ell,\alpha_\ell} & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ s_\alpha \\ \vdots \end{pmatrix}$$

If $b_\ell = 0$, by Lemma 1, $\alpha_{\ell+1} = \alpha_\ell$. Therefore, any solution to equation (6) is equal to s_α at position α_ℓ and thus $\boldsymbol{c}_{\ell,1} = s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + \tilde{r}_{\ell,1} \boldsymbol{g}_{\ell,2^{\ell-1}+1}$. Equation (3) implies that

$$\begin{aligned}
\boldsymbol{c}_\ell =& (1-b_\ell)(s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + \tilde{r}_{\ell,1} \boldsymbol{g}_{\ell,2^{\ell-1}+1}) + b_\ell \boldsymbol{c}_{\ell,2} + y_\ell \boldsymbol{g}_{\ell,2^{\ell-1}+1} \\
=& s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + (\tilde{r}_{\ell,1} + y_\ell) \boldsymbol{g}_{\ell,2^{\ell-1}+1}.
\end{aligned}$$

If $b_\ell = 1$, then $\alpha_{\ell+1} = \alpha_\ell + 2^{\ell-1}$ and similarly, $\boldsymbol{c}_\ell = s_\alpha \boldsymbol{g}_{\ell,\alpha_\ell} + (\tilde{r}_{\ell,2} + y_\ell) \boldsymbol{g}_{\ell,2^{\ell-1}+1}$.

2 Preliminaries

3 Our Construction

Let $t := |S|$ and $m := \log t$. The statement is now $[\boldsymbol{\zeta}_1] = \mathsf{GS.Com}_{ck_{\mathsf{GS}}}(x_1; r_1), \ldots, [\boldsymbol{\zeta}_n]_1 = \mathsf{GS.Com}_{ck_{\mathsf{GS}}}(x_n; r_n)$, for some $n \in \mathbb{N}$, and the prover wants to show that $x_i = s_{\alpha_i}$, for all $i \in [n]$ and $\alpha_i = \sum_{j=1}^{m} b_{i,j} 2^{j-1} + 1$, for some $b_{i,1}, \ldots, b_{i,m} \in \{0, 1\}$. We need to reformulate equations (1) and (2) to take in count new variables. For $\ell \in [m], i \in [n]$, define

$$\boldsymbol{x}^i_\ell := \begin{pmatrix} \boldsymbol{x}^i_{\ell,1} \\ \boldsymbol{x}^i_{\ell,2} \end{pmatrix} := \begin{pmatrix} x^i_{\ell,1} \\ \vdots \\ x^i_{\ell,2^{\ell-2}} \\ \hline x^i_{\ell,2^{\ell-2}+1} \\ \vdots \\ x^i_{\ell,2^{\ell-1}} \end{pmatrix}, \quad \boldsymbol{x}^i_{m+1,1} := \begin{pmatrix} s_1 \\ \vdots \\ s_{t/2} \end{pmatrix}, \text{ and } \boldsymbol{x}^i_{m+1,2} := \begin{pmatrix} s_{t/2+1} \\ \vdots \\ s_t \end{pmatrix},$$

and define new equations for each $\ell \in [m], i \in [n]$

$$\boldsymbol{x}^i_\ell = (1 - b_{i,\ell})\boldsymbol{x}^i_{\ell+1,1} + b_{i,\ell}\boldsymbol{x}^i_{\ell+1,2}, \tag{7}$$

$$x_i = \boldsymbol{x}^i_1 \tag{8}$$

Next, we construct an aZKSMP for $S \subset \mathbb{Z}_q$ and in Section 3.1 we show how to extend these ideas for the case of fixed $S \subset \mathbb{G}_1$. The construction follows the intuition outlined before but it "aggregates" many instances on a single $\Theta(\log t)$ proof. From a high level this is done as follows.

We will rewrite equation (7), which is a system of mn equations, as m equations of the form

$$\boldsymbol{x}\boldsymbol{y}^\top = \begin{pmatrix} 0 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & 0 & \cdots & x_2y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_my_1 & x_my_2 & \cdots & 0 \end{pmatrix}, \tag{9}$$

where $\boldsymbol{x} \in \mathbb{Z}_q^m, \boldsymbol{y} \in \mathbb{Z}_q^n$ (i.e. the diagonal of the matrix $\boldsymbol{x}\boldsymbol{y}^\top$ is $\mathbf{0}$). We will use similar techniques to those of Chapter **??** to give a constant size proof for the satisfiability of each of these equations. Therefore, to prove m of these equations we will require $\Theta(m) = \Theta(\log t)$ group elements.

We can compute $\boldsymbol{x}\boldsymbol{y}^\top$ in the "commitment space" by means of $[\boldsymbol{c}]_1[\boldsymbol{d}^\top]_2$, where $[\boldsymbol{c}]_1 := \mathsf{MP.Com}_{ck_1}(\boldsymbol{x}; r_1)$ and $[\boldsymbol{d}]_2 := \mathsf{MP.Com}_{ck_2}(\boldsymbol{y}; r_2)$. Indeed, by the definition of MP commitments it holds that

$$\begin{aligned}[\boldsymbol{c}]_1[\boldsymbol{d}^\top]_2 &= \left(\sum_{i=1}^{m} x_i[\boldsymbol{g}_i]_1 + r_1[\boldsymbol{g}_{m+1}]_1\right)\left(\sum_{j=1}^{n} y_j[\boldsymbol{h}_j^\top]_2 + r_2[\boldsymbol{h}_{n+1}^\top]_2\right) \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} x_iy_j[\boldsymbol{g}_i\boldsymbol{h}_j^\top]_T + \sum_{i=1}^{m} x_ir_2[\boldsymbol{g}_i\boldsymbol{h}_{n+1}^\top]_T + \sum_{j=1}^{n+1} r_1y_j[\boldsymbol{g}_{m+1}\boldsymbol{h}_j^\top]_T\end{aligned}$$

Therefore, if the diagonal of $\boldsymbol{x}\boldsymbol{y}^\top$ is $\mathbf{0}$, then $[\boldsymbol{c}]_1[\boldsymbol{d}^\top]_2$ is in the space spanned by $\{[\boldsymbol{g}_i\boldsymbol{h}_j^\top]_T : i \neq j \text{ or } i = m+1 \text{ or } j = n+1\}$. Similarly as done in Section **??**, equation (9) can be proven computing two matrices $[\boldsymbol{\Theta}]_1 \in \mathbb{G}_1^{2\times 2}$ and $[\boldsymbol{\Pi}]_2 \in \mathbb{G}_2^{2\times 2}$ and showing that $[\boldsymbol{c}]_1[\boldsymbol{d}^\top]_2 = [\boldsymbol{\Theta}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[\boldsymbol{\Pi}]_2$ and $\boldsymbol{\Theta}+\boldsymbol{\Pi} \in \mathbf{Span}(\{\boldsymbol{g}_i\boldsymbol{h}_j^\top : i = m+1 \text{ or } j = n+1\})$.

For each $\ell \in [m]$, to rewrite the right side of equation (7) in the $\boldsymbol{x}\boldsymbol{y}^\top$ form, we observe that

$$\begin{pmatrix} \boldsymbol{x}^1_{\ell+1,1} \\ \vdots \\ \boldsymbol{x}^n_{\ell+1,1} \end{pmatrix} \left(\begin{pmatrix} b_{1,\ell} \\ \vdots \\ b_{n,\ell} \end{pmatrix} - \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \right)^\top + \begin{pmatrix} \boldsymbol{x}^1_{\ell+1,1} \\ \vdots \\ \boldsymbol{x}^n_{\ell+1,2} \end{pmatrix} \begin{pmatrix} b_{1,\ell} \\ \vdots \\ b_{n,\ell} \end{pmatrix}^\top =$$
$$\begin{pmatrix} (1-b_{1,\ell})\boldsymbol{x}^1_{\ell+1,1} + b_{1,\ell}\boldsymbol{x}^1_{\ell+1,2} & \cdots & (1-b_{n,\ell})\boldsymbol{x}^1_{\ell+1,1} + b_{n,\ell}\boldsymbol{x}^1_{\ell+1,2} \\ \vdots & \ddots & \vdots \\ (1-b_{1,\ell})\boldsymbol{x}^n_{\ell+1,1} + b_{1,\ell}\boldsymbol{x}^n_{\ell+1,2} & \cdots & (1-b_{n,\ell})\boldsymbol{x}^n_{\ell+1,1} + b_{n,\ell}\boldsymbol{x}^n_{\ell+1,2} \end{pmatrix}.$$

If we view the previous matrix as one of size $n \times n$ where each entry is a vector from $\mathbb{Z}_q^{2^{\ell-1}}$, then the diagonal forms the right side of equation (7). We rewrite the left side of equation (7) as

$$\begin{pmatrix} \boldsymbol{x}^1_\ell \\ \vdots \\ \boldsymbol{x}^n_\ell \end{pmatrix} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}^\top = \begin{pmatrix} \boldsymbol{x}^1_\ell & \cdots & \boldsymbol{x}^1_\ell \\ \vdots & & \vdots \\ \boldsymbol{x}^n_\ell & \cdots & \boldsymbol{x}^n_\ell \end{pmatrix}.$$

and, again, the diagonal forms the left side of equation (7).

Now we prove that equation (7) holds by replacing variables with MP commitments and showing that

$$[\boldsymbol{c}_\ell]_1 \left(\sum_{j=1}^n [\boldsymbol{h}_j]_2 \right)^\top - [\boldsymbol{c}_{\ell,1}]_1 \left([\boldsymbol{d}_\ell]_2 - \sum_{j=1}^n [\boldsymbol{h}_j]_2 \right)^\top - [\boldsymbol{c}_{\ell,2}]_1[\boldsymbol{d}]_2^\top =$$
$$[\boldsymbol{\Theta}]_1[\mathbf{I}]_2 + [\mathbf{I}]_1[\boldsymbol{\Pi}]_2,$$

where

$$[\boldsymbol{c}_\ell]_1 := \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} \boldsymbol{x}^1_\ell \\ \vdots \\ \boldsymbol{x}^n_\ell \end{pmatrix}; r_\ell \right) \qquad [\boldsymbol{d}_\ell]_1 := \mathsf{MP.Com}_{ck}\left(\begin{pmatrix} b_{1,\ell} \\ \vdots \\ b_{n,\ell} \end{pmatrix}; t_\ell \right)$$
$$[\boldsymbol{c}_{\ell,1}]_1 := \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} \boldsymbol{x}^1_{\ell+1,1} \\ \vdots \\ \boldsymbol{x}^n_{\ell+1,1} \end{pmatrix}; r_{\ell,1} \right) \qquad [\boldsymbol{c}_{\ell,2}]_1 := \mathsf{MP.Com}_{ck_\ell}\left(\begin{pmatrix} \boldsymbol{x}^1_{\ell+1,2} \\ \vdots \\ \boldsymbol{x}^n_{\ell+1,2} \end{pmatrix} \right)$$
$$ck_\ell := [\left(\mathbf{G}^1_\ell \cdots \mathbf{G}^n_\ell \; \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\right)]_1 \qquad \mathbf{G}^i_\ell := \left(\boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+1} \cdots \boldsymbol{g}_{\ell,i2^{\ell-1}}\right)$$
$$ck := [\mathbf{H}]_2 \qquad \mathbf{H} := \left(\boldsymbol{h}_1 \cdots \boldsymbol{h}_n \; \boldsymbol{h}_{n+1}\right).$$

We need to show that $\boldsymbol{\Theta}+\boldsymbol{\Pi}$ is in the appropriate space, which is the one without components "in the diagonal" or with components in $\boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_j$ or $\boldsymbol{g}_i\boldsymbol{h}_{n+1}$ for any $i \in [n2^{\ell-1}], j \in [n+1]$. However, since we are working with matrices whose entries are vectors in $\mathbb{Z}_q^{2^{\ell-1}}$, we in fact need to show that

$$\boldsymbol{\Theta}+\boldsymbol{\Pi} \in \mathbf{Span}(\{\boldsymbol{g}_{\ell,i}\boldsymbol{h}_j^\top : j \in [n+1], i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}] \setminus [n2^{\ell-1}+1]\}),$$

since the indices i and j where $i \in [(j-1)2^{\ell-1}+1, j2^{\ell-1}]$ are those which range over the elements in the diagonal of a matrix whose entries are elements from $\mathbb{Z}_q^{2^{\ell-1}}$.

It is only left to prove the "aggregated version" of equation (6) from the non-aggregated case, and to prove equation (8). Equation (6) is proven in the same way as in the non-aggregated case, but enlarging the matrix as consequence of the enlargement of commitment keys. Additionally, we prove equation (8) with a proof that

$$[\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1 \text{ and } [\boldsymbol{c}_1]_1 \text{ open to the same values,}$$

using the proof system from Section **??**.

The Scheme

$\mathsf{K}_1(gk, ck_{\mathsf{GS}})$**:** Parse ck_{GS} as $[\boldsymbol{u}_1|\boldsymbol{u_2}]_1$. For each $\ell \in [m]$ let $\mathbf{G}_\ell := \mathbf{G}_\ell^1|\cdots|\mathbf{G}_\ell^n|\boldsymbol{g}_{\ell,n2^{\ell-1}+1} \leftarrow \mathcal{L}_1^{n2^{\ell-1}+1,0}$, where

$$\mathbf{G}_\ell^i = (\mathbf{G}_{\ell,1}^i|\mathbf{G}_{\ell,2}^i) =$$
$$(\boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+1}\cdots\boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+2^{\ell-2}}|\boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+2^{\ell-2}+1}\cdots\boldsymbol{g}_{\ell,i2^{\ell-1}}) \in \mathbb{Z}_q^{2\times 2^{\ell-1}},$$

$i \in [n]$, and define $ck_\ell := [\mathbf{G}_\ell]_1$. Let $\mathbf{H} = \begin{pmatrix}\boldsymbol{h}_1 \cdots \boldsymbol{h}_n\, \boldsymbol{h}_{n+1}\end{pmatrix} \leftarrow \mathcal{L}_1^{n,0}$ and define $ck := [\mathbf{H}]_2$.
For each $\ell \in [m]$, $i \in [n2^{\ell-1}+1]$, $j \in [n+1]$, such that $i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}]$ define matrices

$$\mathbf{M}_{i,j}^\ell := ([\mathbf{C}_{i,j}^\ell]_1, [\mathbf{D}_{i,j}^\ell]_2) := ([\boldsymbol{g}_{\ell,i}\boldsymbol{h}_j^\top + \mathbf{T}]_1, [-\mathbf{T}]_2),$$

For $\ell \in [m]$, pick $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ and let

$$\mathcal{M}_\ell := \{\mathbf{M}_{i,j}^\ell : j \in [n+1], i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}] \setminus [n2^{\ell-1}+1]\}$$

and let

$$\mathcal{C}_\ell := \{\mathbf{C}_{i,j}^\ell : j \in [n+1], i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}] \setminus [n2^{\ell-1}+1]\}.$$

Let Π_{sum} be the proof system for sum in subspace (Section **??**), Π_{lin} the proof system for membership in linear subspaces from Section **??**, Π_{bits} the proof system for proving that many commitments open to bit-strings from section

??, and Π_{com} be an instance of the proof system for equal commitment opening (Section **??**).
For each $\ell \in [m]$, let $\mathsf{crs}_{\mathsf{sum},\ell} \leftarrow \Pi_{\mathsf{sum}}.\mathsf{K}_1(gk, \mathcal{M}_\ell)$.[4], let $\mathsf{crs}_{\mathsf{lin},\ell} \leftarrow \Pi_{\mathsf{lin}}.\mathsf{K}_1(gk; [\mathbf{G}_{\ell,\mathsf{split}}]_1, n2^{\ell-1}+3)$, let $\mathsf{crs}_{\mathsf{bits}} \leftarrow \Pi_{\mathsf{bits}}.\mathsf{K}_1(gk, [\mathbf{H}]_2, m)$, and let $\mathsf{crs}_{\mathsf{com}} \leftarrow \Pi_{\mathsf{com}}.\mathsf{K}_1(gk, ck_1, CK_{\mathsf{GS}}, m)$, where

$$\mathbf{G}_{\ell,\mathsf{split}} := \begin{pmatrix} \mathbf{G}^1_{\ell+1,1} & \mathbf{G}^1_{\ell+1,2} & \cdots & \mathbf{G}^n_{\ell+1,1} & \mathbf{G}^n_{\ell+1,2} & \boldsymbol{g}_{\ell+1,n2^\ell+1} & \mathbf{0} & \mathbf{0} \\ \mathbf{G}^1_{\ell,1} & \mathbf{0} & \cdots & \mathbf{G}^n_{\ell,n} & \mathbf{0} & \mathbf{0} & \boldsymbol{g}_{\ell,n2^{\ell-1}+1} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}^1_{\ell,1} & \cdots & \mathbf{0} & \mathbf{G}^n_{\ell,n} & \mathbf{0} & \mathbf{0} & \boldsymbol{g}_{\ell,n2^{\ell-1}+1} \end{pmatrix},$$

$$CK_{\mathsf{GS}} := \begin{pmatrix} [\boldsymbol{u}_1]_1 & & [\mathbf{0}]_1 & [\boldsymbol{u}_2]_1 & & [\mathbf{0}]_1 \\ & \ddots & & & \ddots & \\ [\mathbf{0}]_1 & & [\boldsymbol{u}_1]_1 & [\mathbf{0}]_1 & & [\boldsymbol{u}_2]_1 \end{pmatrix} \in \mathbb{G}_1^{2n\times 2n}.$$

The common reference string is given by:

$$\mathsf{crs} := (gk, [\mathbf{G}]_1, [\mathbf{H}]_2, \{\mathcal{M}_\ell, \mathsf{crs}_{\mathsf{sum},\ell}, \mathsf{crs}_{\mathsf{lin},\ell} : \ell \in [m]\}, \mathsf{crs}_{\mathsf{bits}}, \mathsf{crs}_{\mathsf{com}}).$$

$\mathsf{P}(\mathsf{crs}, ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S), \langle (x_1, \ldots, x_n), (w_1, \ldots, w_n)\rangle)$**:** The prover compute commitments

$$\begin{aligned}
&[\boldsymbol{c}_\ell]_1 := \mathsf{MP.Com}_{ck_\ell}({\boldsymbol{x}^1_\ell}^\top, \ldots, {\boldsymbol{x}^n_\ell}^\top; r_\ell), \text{ for } \ell \in [m],\\
&[\boldsymbol{c}_{\ell,1}]_1 := \mathsf{MP.Com}_{ck_\ell}({\boldsymbol{x}^1_{\ell+1,1}}^\top, \ldots, {\boldsymbol{x}^n_{\ell+1,1}}^\top; r_{\ell,1}),\\
&[\boldsymbol{c}_{\ell,2}]_1 := \mathsf{MP.Com}_{ck_\ell}({\boldsymbol{x}^1_{\ell+1,2}}^\top, \ldots, {\boldsymbol{x}^n_{\ell+1,2}}^\top; r_{\ell,2}), \text{ for } \ell \in [m-1]\\
&[\boldsymbol{d}_\ell]_2 := \mathsf{MP.Com}_{ck}(\boldsymbol{b}_\ell; t_\ell), \text{ for } \ell \in [m]
\end{aligned}$$

where $r_\ell, r_{\ell,1}, r_{\ell,2}, t_j \leftarrow \mathbb{Z}_q$ and the variables $\boldsymbol{x}^i_\ell, \boldsymbol{x}^i_{\ell,j}, \boldsymbol{b}_\ell$ are the ones defined in equation (7). The prover computes a proof π_{bits} that $[\boldsymbol{d}_1]_2, \ldots, [\boldsymbol{d}_m]_2$ open to bit-strings. Then, for $\ell \in [m]$, the prover pick matrices $\mathbf{R}_\ell \leftarrow \mathbb{Z}_q^{2\times 2}$, computes

$$\begin{aligned}
&([\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2) :=\\
&\sum_{i=1}^{n}\sum_{j\neq i}\sum_{k=1}^{2^{\ell-1}}(x^i_{\ell,k} - x^i_{\ell+1,k}(1-b_{j,\ell}) - x^i_{\ell+1,2^{\ell-1}+k}b_{j,\ell})\mathbf{M}^\ell_{(i-1)2^{\ell-1}+k,j}\\
&+\sum_{i=1}^{n}\sum_{k=1}^{2^{\ell-1}} t_\ell(x^i_{\ell+1,k} - x^i_{\ell+1,2^{\ell-1}+k})\mathbf{M}^\ell_{(i-1)2^{\ell-1}+k,n+1}\\
&+\sum_{j=1}^{n}(r_\ell - r_{\ell,1}(1-b_{j,\ell}) - r_{\ell,2}b_{j,\ell})\mathbf{M}^\ell_{n2^{\ell-1}+1,j}\\
&+(r_{\ell,1}-r_{\ell,2})t_\ell\mathbf{M}^\ell_{n2^{\ell-1}+1,n+1} + ([\mathbf{R}_\ell]_1, [-\mathbf{R}_\ell]_2),
\end{aligned}$$

[4] We identify matrices in $\mathbb{G}_1^{2\times 2}$ (respectively in $\mathbb{G}_2^{2\times 2}$) with vectors in $\mathbb{G}_1^4$ (resp. in $\mathbb{G}_2^4$).

where $r_{1,1} = r_{1,2} = 0$, and computes proofs $\pi_{\mathsf{lin},\ell}, \pi_{\mathsf{sum},\ell}$ that, respectively,

$$\begin{pmatrix} \boldsymbol{c}_{\ell+1} \\ \boldsymbol{c}_{\ell,1} \\ \boldsymbol{c}_{\ell,2} \end{pmatrix} \in \mathbf{Span}(\mathbf{G}_{\ell,\mathsf{split}}) \text{ (if } \ell < m), \qquad \boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell \in \mathbf{Span}(\mathcal{C}_\ell).$$

Finally, it computes a proof π_{com} that $([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1)$ and $[\boldsymbol{c}_1]_1$ open to the same value.

The proof is $\pi := (\{([\boldsymbol{c}_\ell]_1, [\boldsymbol{c}_{\ell,1}]_1, [\boldsymbol{c}_{\ell,2}]_1, [\boldsymbol{d}_\ell]_2, [\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2, \pi_{\mathsf{lin},\ell}, \pi_{\mathsf{sum},\ell}) : \ell \in [m]\}, \pi_{\mathsf{bits}}, \pi_{\mathsf{com}})$.

$\mathsf{V}(\mathsf{crs}, ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S), \pi)$**:** Let $[\boldsymbol{c}_{m,1}]_1 := \mathsf{MP.Com}_{ck_m}(s_1, \ldots, s_{t/2}; 0), [\boldsymbol{c}_{m,2}] := \mathsf{MP.Com}_{ck_m}(s_{t/2+1}, \ldots, s_t; 0)$. The verifier checks the validity of $\pi_{\mathsf{bits}}, \pi_{\mathsf{com}}$ and, for each $\ell \in [m]$, checks the validity of $\pi_{\mathsf{lin},\ell}, \pi_{\mathsf{sum},\ell}$ and of equations

$$[\boldsymbol{c}_\ell]_1 \left(\sum_{j=1}^{n} [\boldsymbol{h}_j]_2 \right)^\top - [\boldsymbol{c}_{\ell,1}]_1 \left(\sum_{j=1}^{n} [\boldsymbol{h}_j]_2 - [\boldsymbol{d}_\ell]_2 \right)^\top - [\boldsymbol{c}_{\ell,2}]_1 [\boldsymbol{d}_\ell]_2^\top = [\boldsymbol{\Theta}_\ell]_1 [\mathbf{I}]_2 + [\mathbf{I}]_1 [\boldsymbol{\Pi}_\ell]_2. \tag{10}$$

If any of these checks fails, it rejects the proof.

$\mathsf{S}_1(gk, ck_{\mathsf{GS}})$**:** The simulator receives as input a description of an asymmetric bilinear group gk and a GS commitment key ck_{GS}. It generates and outputs the CRS in the same way as K_1, but additionally outputs the simulation trapdoor $\tau := (\mathbf{H}, \tau_{\mathsf{com}}, \tau_{\mathsf{bits}}, \{\tau_{\mathsf{sum},\ell}, \tau_{\mathsf{lin},\ell} : \ell \in [m]\})$, where $\tau_{\mathsf{sum}}, \tau_{\mathsf{bits}}, \tau_{\mathsf{sum},\ell}, \tau_{\mathsf{lin},\ell}$ are, respectively, $\mathit{\Pi}_{\mathsf{sum}}, \mathit{\Pi}_{\mathsf{com}}, \mathit{\Pi}_{\mathsf{sum}}, \mathit{\Pi}_{\mathsf{lin}}$ simulation trapdoors.

$\mathsf{S}_2(\mathsf{crs}, ([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S), \tau)$**:** Define $\boldsymbol{x}_\ell^i := \mathbf{0}$ and $\boldsymbol{b}_\ell := \mathbf{0}$ for all $\ell \in [m], i \in [n]$, and computes $[\boldsymbol{c}_\ell]_1, [\boldsymbol{c}_{\ell,1}]_1, [\boldsymbol{c}_{\ell,2}]_1, [\boldsymbol{d}_\ell]_2$ and $[\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2$, as an honest prover would do (that is, with all variables set to 0). Finally, simulate proofs $\pi_{\mathsf{com}}, \pi_{\mathsf{bits}}, \pi_{\mathsf{sum},\ell}, \pi_{\mathsf{lin},\ell}$ using the respective trapdoors.

We prove the following Theorem.

Theorem 1. *The proof system described above is a QA-NIZK proof system for the language $\mathcal{L}^n_{ck_{\mathsf{GS}},\mathsf{set}}$ with perfect completeness, computational soundness, and perfect zero-knowledge.*

Completeness Completeness follows from completeness of $\Pi_{\mathsf{sum}}, \Pi_{\mathsf{lin}}, \Pi_{\mathsf{bits}}, \Pi_{\mathsf{com}}$, and from the fact that equation (10) is satisfied for each $\ell \in [m]$:

$$
\begin{aligned}
&\boldsymbol{c}_\ell \left(\sum_{j=1}^{n} \boldsymbol{h}_j\right)^\top - \boldsymbol{c}_{\ell,1} \left(\sum_{j=1}^{n} \boldsymbol{h}_j - \boldsymbol{d}_\ell\right)^\top - \boldsymbol{c}_{\ell,2}\boldsymbol{d}_\ell^\top && = \\
&\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{G}_\ell^i \boldsymbol{x}_\ell^i \boldsymbol{h}_j^\top + \sum_{j=1}^{n} r_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_j^\top - \sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{G}_\ell^i \boldsymbol{x}_{\ell+1,1}^i (1-b_{j,\ell})\boldsymbol{h}_j^\top \\
&+ \sum_{i=1}^{n} \mathbf{G}_\ell^i \boldsymbol{x}_{\ell+1,1}^i t_\ell \boldsymbol{h}_{n+1}^\top - \sum_{j=1}^{n} r_{\ell,1}(1-b_{j,\ell})\boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_j^\top + r_{\ell,1}t_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_{n+1}^\top \\
&- \sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{G}_\ell^i \boldsymbol{x}_{\ell+1,2}^i b_{j,\ell}\boldsymbol{h}_j^\top - \sum_{i=1}^{n} \mathbf{G}_\ell^i \boldsymbol{x}_{\ell+1,2}^i t_\ell \boldsymbol{h}_{n+1}^\top - \sum_{j=1}^{n} r_{\ell,2} b_{j,\ell}\boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_j^\top \\
&- r_{\ell,2}t_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_{n+1}^\top && = \\
&\sum_{i=1}^{n}\sum_{j\neq i} \mathbf{G}_\ell^i (\boldsymbol{x}_\ell^i - \boldsymbol{x}_{\ell+1,1}^i(1-b_{j,\ell}) - \boldsymbol{x}_{\ell+1,2}^i b_{j,\ell})\boldsymbol{h}_j^\top + \\
&\sum_{i=1}^{n} \mathbf{G}_\ell^i (\boldsymbol{x}_{\ell+1,1}^i - \boldsymbol{x}_{\ell+1,2}^i) t_\ell \boldsymbol{h}_{n+1}^\top + \sum_{j=1}^{n} (r_\ell - r_{\ell,1}(1-b_{j,\ell}) - r_{\ell,2}b_{j,\ell})\boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_j^\top \\
&+ (r_{\ell,1} - r_{\ell,2}) t_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_{n+1}^\top && = \\
&\sum_{i=1}^{n}\sum_{j\neq i}\sum_{k=1}^{2^{\ell-1}} (x_{\ell,k}^i - x_{\ell+1,k}^i(1-b_{j,\ell}) - x_{\ell+1,2^{\ell-1}+k}^i b_{j,\ell}))\boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+k}\boldsymbol{h}_j^\top \\
&+ \sum_{i=1}^{n}\sum_{k=1}^{2^{\ell-1}} t_\ell (x_{\ell+1,k}^i - x_{\ell+1,2^{\ell-1}+k}^i \boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+k}\boldsymbol{h}_{n+1}^\top \\
&\sum_{j=1}^{n} (r_\ell - r_{\ell,1}(1-b_{j,\ell}) - r_{\ell,2}b_{j,\ell})\boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_j^\top + (r_{\ell,1}-r_{\ell,2})t_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\boldsymbol{h}_{n+1}^\top && = \\
&\boldsymbol{\Theta}\mathbf{I} + \boldsymbol{\Pi}\mathbf{I}.
\end{aligned}
$$

Soundness The following theorem guarantees soundness.

Theorem 2. *Let* $\mathsf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{A})$ *be the advantage of an adversary* A *against the soundness of the proof system described above. There exist PPT adversaries* $\mathsf{D}_1, \mathsf{D}_2, \mathsf{B}_{\mathsf{bits}}, \mathsf{B}_{\mathsf{com}}, \mathsf{B}_{\mathsf{sum}}, \mathsf{B}_{\mathsf{lin}}$ *such that*

$$
\begin{aligned}
\mathsf{Adv}_{\Pi_{\mathsf{set}}}(\mathsf{A}) \leq n\,(&\mathsf{Adv}_{\mathcal{L}_1,\mathbb{G}_1}(\mathsf{D}_1) + t/2\,(4/q + \mathsf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_{\mathsf{bits}}) + \mathsf{Adv}_{\mathcal{L}_1,\mathbb{G}_2}(\mathsf{B}_2) \\
&+\ \mathsf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_{\mathsf{com}}) + m\mathsf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_{\mathsf{sum}}) + m\mathsf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_{\mathsf{lin}}))).
\end{aligned}
$$

Recall that, given $b_1, \ldots, b_m \in \{0,1\}$, we defined $\alpha := \sum_{i=1}^{m} b_i 2^{i-1} + 1$. Recall also that, given a path $(b_m, \ldots, b_\ell)$ in the binary tree whose leaves are labeled from left to right by $s_1, \ldots, s_t$, we defined $\mathsf{left} := \sum_{i=\ell}^{m} b_i 2^{i-1} + 1$, $\mathsf{right} := \mathsf{left} + 2^{\ell-1} - 1$, and we defined $\alpha_\ell := \alpha - \mathsf{left} + 1$ the position of s_α relative to the leaves under $s_{\mathsf{left}}, \ldots, s_{\mathsf{right}}$.

The proof follows from the indistinguishability of the following games:

- Real: This is the real soundness game. The output is 1 if the adversary submits some $([\boldsymbol{\zeta}_1]_1, \ldots, [\boldsymbol{\zeta}_n]_1, S) \notin \mathcal{L}^n_{ck_{\mathsf{GS}},\mathsf{set}}$ and the corresponding proof which is accepted by the verifier.
- Game_0: This identical to Real, except that K_1 does not receive ck_{GS} as a input but it samples ck_{GS} itself together with its discrete logarithms.
- Game_1: This game is identical to Game_0 except that now it chooses random $j^* \in [n]$ and it aborts if $x_{j^*} \notin S$.
- Game_2: This game is identical to Game_1 except that now $\mathbf{H} \leftarrow \mathcal{L}_1^{n,j^*}$.
- Game_3: This game is identical to Game_2 except that now it defines $b_m := b_{j^*,m}$ and chooses a random (sub-)path $(b_{m-1}, \cdots, b_1) \leftarrow \{0,1\}^{m-1}$ (which ignores the first edge) in the tree whose leaves are $s_1, \ldots, s_t$. This game aborts if $(b_{j^*,1}, \ldots, b_{j^*,m}) \notin \{0,1\}^m$ or $(b_1, \ldots, b_{m-1}) \neq (b_{j^*,1}, \ldots, b_{j^*,m-1})$, where $b_{j^*,1}, \ldots, b_{j^*,m}$ are the openings of $[\boldsymbol{d}_2]_2, \ldots, [\boldsymbol{d}_m]_2$ at coordinate j^*, respectively.
- Game_4: This game is identical to Game_3 except that now $\mathbf{G}_\ell \leftarrow \mathcal{L}_1^{n2^{\ell-1},\Delta+\alpha_\ell}$, for $\ell \in [m]$ and $\Delta := (j^*-1)2^{\ell-1}$.

It is obvious that the first two games are indistinguishable. The rest of the argument goes as follows.

Lemma 2. $\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] \geq \frac{1}{n} \Pr[\mathsf{Game}_0(\mathsf{A}) = 1]$.

Proof. The probability that $\mathsf{Game}_1(\mathsf{A}) = 1$ is the probability that a) $\mathsf{Game}_0(\mathsf{A}) = 1$ and b) $x_{j^*} \notin S$. The view of adversary A is independent of j^*, while, if $\mathsf{Game}_0(\mathsf{A}) = 1$, then there is at least one index $j \in [n]$ such that such that $x_j \notin S$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_0(\mathsf{A}) = 1$, is greater than or equal to $1/n$ and the lemma follows.

Lemma 3. *There exists a* $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ *adversary* D_2 *such that* $|\Pr[\mathsf{Game}_1(\mathsf{A}) = 1] - \Pr[\mathsf{Game}_2(\mathsf{A}) = 1]| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathsf{Gen}_a}(\mathsf{D}_2)$.

Proof. We construct an adversary D_2 that receives a challenge $([\boldsymbol{a}]_2, [\boldsymbol{u}]_2)$ of the $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_2}$ assumption. From this challenge, D_2 just defines the matrix $[\mathbf{H}]_2 \in \mathbb{G}_2^{2\times(n+1)}$ as the matrix whose last column is $[\boldsymbol{a}]_2$, the ith column is $[\boldsymbol{u}]_2$, and the rest of the columns are random vectors in the image of $[\boldsymbol{a}]_2$. Obviously, when $[\boldsymbol{u}]_2$ is sampled from the image of $[\boldsymbol{a}]_2$, $\mathbf{H}$ follows the distribution $\mathcal{L}_1^{m,0}$, while if $[\boldsymbol{u}]_2$ is a uniform element of $\mathbb{G}_2^2$, $\mathbf{H}$ follows the distribution $\mathcal{L}_1^{n,j^*}$.

Adversary D_2 samples $\mathbf{G}^\ell \leftarrow \mathcal{L}_1^{n2^{\ell-1},0}$. Given that D_2 does not know the discrete logarithms of $[\mathbf{H}]_2$, it cannot compute the pairs $(\mathbf{C}^\ell_{i,j}, \mathbf{D}^\ell_{i,j})$ exactly as

in Game_0. Nevertheless, for each $\ell \in [m], i \in [n2^{\ell-1}+1], j \in [n+1]$ such that $i \notin [(j-1)2^{\ell-1}+1, j2^{\ell-1}]$, it can compute identically distributed pairs by picking $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ and defining

$$([\mathbf{C}_{i,j}^{\ell}]_1, [\mathbf{D}_{i,j}^{\ell}]_2) := ([\mathbf{T}]_1, \boldsymbol{g}_{\ell,i}[\boldsymbol{h}_j]_2^{\top} - [\mathbf{T}]_2).$$

The rest of the elements of the CRS are honestly computed. When $\mathbf{H} \leftarrow \mathcal{L}_1^{n,0}$, D_2 perfectly simulates Game_0, and when $\mathbf{H} \leftarrow \mathcal{L}_1^{n,j^*}$, D_2 perfectly simulates Game_1, which concludes the proof.

Lemma 4. *There exists an adversary* $\mathsf{B}_{\mathsf{bits}}$ *against* Π_{bits} *such that* $\Pr[\mathsf{Game}_2(\mathsf{A})=1] \geq \frac{2}{t}(\Pr[\mathsf{Game}_3(\mathsf{A})=1] + \mathbf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_{\mathsf{bits}}))$.

Proof. The probability that $\mathsf{Game}_3(\mathsf{A})=1$ is the probability that a) $\mathsf{Game}_2(\mathsf{A})=1$ and b) $(b_{j^*,1},\ldots,b_{j^*,m}) \notin \{0,1\}^m$ or $(b_1,\ldots,b_{m-1}) \neq (b_{j^*,1},\ldots,b_{j^*,m-1})$. If $(b_{j^*,1},\ldots,b_{j^*,m}) \notin \{0,1\}^m$ we can build an adversary $\mathsf{B}_{\mathsf{bits}}$ against Π_{bits} and thus, the probability that $(b_{j^*,1},\ldots,b_{j^*,m}) \in \{0,1\}^m$ is less than $\mathbf{Adv}_{\Pi_{\mathsf{bits}}}(\mathsf{B}_1)$. The view of adversary A is independent of $(b_1,\ldots,b_{m-1})$, while, if $\mathsf{Game}_2(\mathsf{A})=1$ and $(b_{j^*,1},\ldots,b_{j^*,m}) \in \{0,1\}^m$, then $(b_{j^*,1}\cdots b_{j^*,m-1}) \in \{0,1\}^{m-1}$. Thus, the probability that the event described in b) occurs conditioned on $\mathsf{Game}_2(\mathsf{A})=1$ and $(b_{j^*,1},\ldots,b_{j^*,m}) \in \{0,1\}^m$, is greater than or equal to $2/t$ and the lemma follows.

Lemma 5. *There exists a* $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ *adversary* D_1 *such that* $|\Pr[\mathsf{Game}_3(\mathsf{A})=1] - \Pr[\mathsf{Game}_4(\mathsf{A})=1]| \leq \mathsf{Adv}_{\mathcal{L}_1,\mathbb{G}_1}(\mathsf{D}_1)$.

Proof. We construct an adversary D_1 that receives a challenge $([\boldsymbol{a}]_1, [\boldsymbol{u}]_1)$ of the $\mathcal{L}_1$-$\mathsf{MDDH}_{\mathbb{G}_1}$ assumption. From this challenge, D_1 defines for each $\ell \in [m]$ the matrix $[\mathbf{G}_\ell]_1$ as the matrix whose $\Delta+\alpha_\ell$ th column is $[\boldsymbol{u}]_1$, and the rest of the columns are random vectors in the image of $[\boldsymbol{a}]_1$. Obviously, when $[\boldsymbol{u}]_1$ is sampled from the image of $[\boldsymbol{a}]_1$, $[\mathbf{G}_\ell]_1$ follows the distribution $\mathcal{L}_1^{n2^{\ell-1},0}$, while if $[\boldsymbol{u}]_1$ is a uniform element of $\mathbb{G}_1^2$, $[\mathbf{G}_\ell]_1$ follows the distribution $\mathcal{L}_1^{n2^{\ell-1},\Delta+\alpha_\ell}$.

The rest of the elements of the CRS are honestly computed. When $[\boldsymbol{u}]_1$ is sampled from the image of $[\mathbf{a}]_1$, D_1 perfectly simulates Game_3, and when $[\boldsymbol{u}]_1$ is uniform, D_1 perfectly simulates Game_4, which concludes the proof.

Lemma 6. *There exist adversaries* $\mathsf{B}_{\mathsf{com}}$*, against the strong soundness of* Π_{com}*,* $\mathsf{B}_{\mathsf{sum}}$*, against the soundness of* Π_{sum}*, and an adversary* $\mathsf{B}_{\mathsf{lin}}$ *against the soundness of* Π_{lin}*, such that* $\Pr[\mathsf{Game}_4(\mathsf{A})=1] \leq 4/q + \mathbf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_{\mathsf{com}}) + m\mathbf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_{\mathsf{sum}}) + m\mathbf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_{\mathsf{lin}})$.

Proof. With probability $1-4/q$, $\{\boldsymbol{g}_{\ell,\Delta+\alpha_\ell}, \boldsymbol{g}_{\ell,n2^{\ell-1}+1}\}$, $\ell \in [m]$, and $\{\boldsymbol{h}_{j^*}, \boldsymbol{h}_{m+1}\}$ are bases of $\mathbb{Z}_q^2$, and, for each $\ell \in [m], \mu \in \{1,2\}$, we can define $\tilde{s}_\ell, \tilde{s}_{\ell,\mu}, \tilde{r}_\ell, \tilde{r}_{\ell,\mu}, b_{j^*,\ell}, \tilde{t}_\ell$ as the unique coefficients in $\mathbb{Z}_q$ such that $\boldsymbol{c}_\ell = \tilde{s}_\ell \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}$, $\boldsymbol{c}_{\ell,\mu} = \tilde{s}_{\ell,\mu}\boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_{\ell,\mu}\boldsymbol{g}_{\ell,n2^{\ell-1}+1}$, and $\boldsymbol{d}_\ell = b_{j^*,\ell}\boldsymbol{h}_{j^*} + \tilde{t}_\ell \boldsymbol{h}_{n+1}$.

Recall that if $\mathsf{Game}_4(\mathsf{A})=1$ then $x_{j^*} \notin S$. The adversary can win in Game_4 if one of the following events happen:

E_1: the adversary breaks soundness of Π_{com} and $x_{j^*} \neq \tilde{s}_1$,
E_2: the adversary breaks one of the m instances of Π_{sum} and $\boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell \notin \mathbf{Span}(\mathcal{C}_\ell)$,
E_3: the adversary breaks one of the m instances of Π_{lin} and $(\boldsymbol{c}_{\ell+1}, \boldsymbol{c}_{\ell,1}, \boldsymbol{c}_{\ell,2}) \notin \mathbf{Span}(\mathbf{G}_{\ell,\mathsf{split}})$,
E_4: neither of E_1,E_2, or E_3 happens, but $x_{j^*} \notin S$ anyway.

By the law of total probabilities, $\Pr[\mathsf{Game}_4(\mathsf{A}) = 1] \leq 4/q + \Pr[E_1] + \Pr[E_2] + \Pr[E_3] + \Pr[E_4]$, and is not hard to see that there exist adversaries $\mathsf{B}_{\mathsf{com}}, \mathsf{B}_{\mathsf{sum}}, \mathsf{B}_{\mathsf{lin}}$ such that $\Pr[E_1] = \mathbf{Adv}_{\Pi_{\mathsf{com}}}(\mathsf{B}_{\mathsf{com}}), \Pr[E_2] = m\mathbf{Adv}_{\Pi_{\mathsf{sum}}}(\mathsf{B}_{\mathsf{sum}})$, and $\Pr[E_3] = m\mathbf{Adv}_{\Pi_{\mathsf{lin}}}(\mathsf{B}_{\mathsf{lin}})$. Below we will show that $\Pr[E_4] = 0$ (using the same argument used in the non-aggregated case).

We prove by induction on ℓ that $\tilde{s}_\ell = s_\alpha$. If this is the case, the fact that $\neg E_1$ implies that $x_{j^*} = \tilde{s}_1 = s_\alpha \in S$, which finish the proof.

But first note that given a vector $\boldsymbol{k} \in \mathbb{Z}_q^2$, such that $\boldsymbol{h}_j^\top \boldsymbol{k} = 1$ if $j = j^*$ and 0 if not (which exists since $\{\boldsymbol{h}_{j^*}, \boldsymbol{h}_{n+1}\}$ is a basis of $\mathbb{Z}_q^2$), if we multiply equation (10) on the right by $\boldsymbol{k}$ we get

$$[\boldsymbol{c}_\ell]_T - (1 - b_{j^*,\ell})[\boldsymbol{c}_{\ell,1}]_T - b_{j^*,\ell}[\boldsymbol{c}_{\ell,2}]_T = [(\boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell)\boldsymbol{k}]_T.$$

The fact that $\boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell \in \mathbf{Span}(\mathcal{C}_\ell)$, $\boldsymbol{g}_{\ell,i} \in \mathbf{Span}(\boldsymbol{g}_{\ell,n2^{\ell-1}+1})$ if $i \neq \Delta + \alpha_\ell$, and $\Delta + \alpha_\ell \in [\Delta + 1, \Delta + 2^{\ell-1}]$, implies that

$$(\boldsymbol{\Theta}_\ell + \boldsymbol{\Pi}_\ell)\boldsymbol{k} = \sum_{i \in [n2^{\ell-1}+1] \setminus [\Delta+1, \Delta+2^{\ell-1}]} \beta_i \boldsymbol{g}_{\ell,i} = \beta \boldsymbol{g}_{\ell,n2^{\ell-1}+1}$$

for some $\beta_i, \beta \in \mathbb{Z}_q$, $i \in [n2^{\ell-1} + 1] \setminus [\Delta + 1, \Delta + 2^{\ell-1}]$.

Therefore, given that we are in the case $b_\ell = b_{j^*,\ell}$, equation (10) implies that

$$[\boldsymbol{c}_\ell]_T = (1 - b_\ell)[\boldsymbol{c}_{\ell,1}]_T + b_\ell[\boldsymbol{c}_{\ell,2}]_T + \beta \boldsymbol{g}_{\ell,n2^{\ell-1}+1}.$$

In the base case ($\ell = m$), the fact that $\boldsymbol{g}_{m,i} \in \mathbf{Span}(\boldsymbol{g}_{m,n2^{m-1}+1})$, if $i \neq \Delta + \alpha_m$, implies that

$$\begin{aligned}
\boldsymbol{c}_m &= (1 - b_m) \sum_{i=1}^{2^{m-1}} s_i \boldsymbol{g}_{m,\Delta+i} + b_m \sum_{i=1}^{2^{m-1}} s_{i+2^{m-1}} \boldsymbol{g}_{m,\Delta+i} \\
&= (1 - b_m) s_{\alpha_m} \boldsymbol{g}_{m,\Delta+\alpha_m} + b_m s_{\alpha_m+2^{m-1}} \boldsymbol{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,n2^{m-1}+1} \\
&= (1 - b_m) s_{\alpha-\mathsf{left}+1} \boldsymbol{g}_{m,\Delta+\alpha_m} + b_m s_{\alpha-\mathsf{left}+1+2^{m-1}} \boldsymbol{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,n2^{m-1}+1} \\
&= \begin{cases} s_{\alpha-1+1} \boldsymbol{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,n2^{m-1}+1} & \text{if } b_m = 0 \ (\mathsf{left} = 1) \\ s_{\alpha-(2^{m-1}+1)+1+2^{m-1}} \boldsymbol{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,n2^{m-1}+1} & \text{if } b_m = 1 \ (\mathsf{left} = 2^{m-1}+1) \end{cases}
\end{aligned}$$

for some $\tilde{r}_1 \in \mathbb{Z}_q$. In both cases $\boldsymbol{c}_1 = s_\alpha \boldsymbol{g}_{m,\Delta+\alpha_m} + \tilde{r}_1 \boldsymbol{g}_{m,n2^{m-1}}$.

In the inductive case we assume that $\boldsymbol{c}_{\ell+1} = s_\alpha \boldsymbol{g}_{\ell+1,2\Delta+\alpha_{\ell+1}} + \tilde{r}_{\ell+1} \boldsymbol{g}_{\ell+1,n2^\ell+1}$ and we want to show that $\boldsymbol{c}_\ell = s_\alpha \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1}$.[5] Since $\boldsymbol{g}_{\ell+1,\alpha_{\ell+1}}$ is

[5] Note that $\mathbf{G}_{\ell+1} \leftarrow \mathcal{L}_1^{n2^\ell,(j^*-1)2^\ell+\alpha_{\ell+1}}$ and thus, the $(j^* - 1)2^\ell + \alpha_{\ell+1} = 2\Delta + \alpha_{\ell+1}$ th column of $\mathbf{G}_{\ell+1}$ is l.i. from the rest.

linearly independent from the rest of vectors in $ck_{\ell+1}$, any solution to

$$\begin{pmatrix} \boldsymbol{c}_{\ell+1} \\ \boldsymbol{c}_{\ell,1} \\ \boldsymbol{c}_{\ell,2} \end{pmatrix} = \mathbf{G}_{\ell,\mathsf{split}}\boldsymbol{w} \tag{11}$$

is equal to s_α at position $2\Delta + \alpha_{\ell+1} = 2\Delta + \alpha_\ell + b_\ell 2^{\ell-1}$ as depicted below.

$$\begin{pmatrix} \boldsymbol{c}_{\ell+1} \\ \boldsymbol{c}_{\ell,1} \\ \boldsymbol{c}_{\ell,2} \end{pmatrix} = \begin{pmatrix} \cdots & \boldsymbol{g}_{\ell+1,2\Delta+\alpha_\ell} & \cdots & \boldsymbol{g}_{\ell+1,2\Delta+\alpha_\ell+2^{\ell-1}} & \cdots \\ \cdots & \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} & \cdots & \mathbf{0} & \cdots \\ \cdots & \mathbf{0} & \cdots & \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ s_\alpha \\ \vdots \end{pmatrix}$$

If $b_\ell = 0$, by Lemma 1, $\alpha_{\ell+1} = \alpha_\ell$. Therefore, any solution to equation (11) is equal to s_α at position $2\Delta + \alpha_\ell$ and thus $\boldsymbol{c}_{\ell,1} = s_\alpha \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_{\ell,1}\boldsymbol{g}_{\ell,n2^{\ell-1}+1}$. Equation 10 implies that

$$\begin{aligned} \boldsymbol{c}_\ell =& (1-b_\ell)(s_\alpha \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + \tilde{r}_{\ell,1}\boldsymbol{g}_{\ell,n2^{\ell-1}+1}) + b_\ell \boldsymbol{c}_{\ell,2} + y_\ell \boldsymbol{g}_{\ell,n2^{\ell-1}+1} \\ =& s_\alpha \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + (\tilde{r}_{\ell,1} + y_\ell)\boldsymbol{g}_{\ell,n2^{\ell-1}+1}. \end{aligned}$$

If $b_\ell = 1$, then $\alpha_{\ell+1} = \alpha_\ell + 2^{\ell-1}$ and similarly, $\boldsymbol{c}_\ell = s_\alpha \boldsymbol{g}_{\ell,\Delta+\alpha_\ell} + (\tilde{r}_{\ell,2} + y_\ell)\boldsymbol{g}_{\ell,n2^{\ell-1}+1}$.

Perfect Zero-Knowledge Note that the vectors $[\boldsymbol{c}_\ell], [\boldsymbol{c}_{\ell,1}]_1, [\boldsymbol{c}_{\ell,2}]_1, [\boldsymbol{d}_\ell]_2$ and matrices $[\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_2$, $1 \leq \ell \leq m$, output by the prover and the simulator are, respectively, uniform vectors and uniform matrices conditioned on satisfying equation 10. This follows from the fact that $ck, ck_1, \ldots, ck_\ell$ are all perfectly hiding commitment keys and that $[\boldsymbol{\Theta}_\ell]_1, [\boldsymbol{\Pi}_\ell]_1$ are the unique solutions of equation (10) modulo the random choice of $\mathbf{R}_\ell$. Finally, the rest of the proof follows from zero-knowledge of $\Pi_{\mathsf{com}}, \Pi_{\mathsf{bits}}, \Pi_{\mathsf{sum}}$, and Π_{lin}.

3.1 The case $S \subset \mathbb{G}_1$

We briefly justify that the case $S \subset \mathbb{G}_1$ follows directly from the case $S \subset \mathbb{Z}_q$ when S is a fixed witness samplable set. That is, there is a fixed set S for each CRS, and there is an efficient algorithm that samples $s_1, \ldots, s_t \in \mathbb{Z}_q$ such that $S = \{[s_1]_1, \ldots, [s_t]_1\}$.

The reason why is not clear how to compute proofs in this setting is that it requires to compute values of the type $[\boldsymbol{s}_i\gamma]_1$, where $[\gamma]_\mu$, $\mu \in \{1,2\}$, is a group element included in the CRS. The solution is straightforward: use $s_1, \ldots, s_t$ to compute these values and add them to the CRS (with the consequent CRS growth). Therefore, the new CRS contains also, for each $\alpha \in [n], \ell \in [m], i \in [n2^{\ell-1}], j \in [n]$, such that $i \neq (j-1)2^{\ell-1} + \alpha_\ell$:

$$s_\alpha[\boldsymbol{g}_{\ell,(i-1)2^{\ell-1}+\alpha_\ell}]_1 \text{ and } s_\alpha([\mathbf{C}^\ell_{(i-1)2^{\ell-1}+\alpha_\ell,j}]_1, [\mathbf{D}^\ell_{(j-1)2^{\ell-1},j}]_2).$$