1 Multivariate Commitments for a single degree bound

Notation roughly follows that of Marlin. For an ℓ-variate polynomial, p, denote $deg(p)$ as the total degree. Let $\mathcal{W}_{\ell,D}$ be the set of all multisets of $\{1, \cdots, \ell\}$ with cardinality of any individual element at most D.

This scheme follows the hiding strategy of Marlin where polynomial commitments are masked by a random polynomial evaluated at the same points. This technique requires $B \cdot \ell + 1$ additional elements (where B is the hiding bound) in ck, when compared to PST. We will refer to this commitment scheme as $\mathsf{MC_m}$.

Setup. On input a security parameter λ (in unary), the number of variables $\ell \in \mathbb{N}$, a hiding bound B, and a maximum degree bound $D \in \mathbb{N}$ $\mathsf{MC_m}.\mathsf{Setup}$ samples a key pair $(\mathsf{ck}, \mathsf{rk})$ as follows. Sample a bilinear group $\langle \mathsf{group} \rangle \leftarrow \mathsf{SampleGrp}(1^\lambda)$ and parse $\langle \mathsf{group} \rangle$ as a tuple $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, G, H, e)$. Sample random elements $\beta_1, \cdots, \beta_\ell \in \mathbb{F}_q$ and $\gamma \in \mathbb{F}_q^*$. Then compute the vector:

$$\mathbf{\Sigma} := \begin{pmatrix} \{\ (\prod_{i \in W} \beta_i) G\ \}_{W \in \mathcal{W}_{\ell,D}} \\ \gamma G, \{\gamma \beta_i G, \cdots, \gamma \beta_i^B G\}_{i \in [\ell]} \end{pmatrix} \in \mathbb{G}_1^{D^\ell + B\ell + 1}$$

Set $\mathsf{ck} := (\langle \mathsf{group} \rangle, \mathbf{\Sigma})$ and $\mathsf{rk} := (D, \langle \mathsf{group} \rangle, \gamma G, \beta_1 H, \cdots, \beta_\ell H)$, and then output the public parameters $(\mathsf{ck}, \mathsf{rk})$. These public parameters will support ℓ-variate polynomials over the field $\mathbb{F}_q$ of degree at most D.

Commit. On input ck, ℓ-variate polynomials $\boldsymbol{p} := [p_i]_{i=1}^n$ over $\mathbb{F}_q$, and randomness $\boldsymbol{\omega} := [\omega_i]_{i=1}^n$ over $\mathbb{F}_q$. $\mathsf{MC_m}.\mathsf{Commit}$ outputs commitments $\boldsymbol{c} := [c_i]_{i=1}^n$ that are computed as follows. If for any $p_i \in \boldsymbol{p}$, $deg(p_i) > D$, abort. Else, for each $i \in [n]$, if ω_i is not $\perp$ then obtain random polynomial $\bar{p}_i$ with individual degree B in each variable from ω_i, otherwise set $\bar{p}_i$ to be a zero polynomial. For each $i \in [n]$, output $c_i := p_i(\boldsymbol{\beta})G + \gamma \bar{p}_i(\boldsymbol{\beta})G$.

Open. On input ck, ℓ-variate polynomials $\boldsymbol{p} := [p_i]_{i=1}^n$ over $\mathbb{F}_q$, evaluation point $\boldsymbol{z} \in \mathbb{F}_q^\ell$, opening challenge $\xi \in \mathbb{F}_q$, and randomness $\boldsymbol{\omega} := [\omega_i]_{i=1}^n$ (the same randomness used for $\mathsf{MC_m}.\mathsf{Commit}$), $\mathsf{MC_m}.\mathsf{Open}$ outputs an evaluation proof π that is computed as follows. If for any $p_i \in \boldsymbol{p}$, $deg(p_i) > D$, abort. Else, for each $i \in [n]$, if ω_i is not $\perp$ then obtain random polynomial $\bar{p}_i$ of individual degree B in each variable from ω_i, otherwise set $\bar{p}_i$ to be a zero polynomial. Then compute the linear combination of polynomials $p(\boldsymbol{X}) := \sum_{i=1}^n \xi^i p_i(\boldsymbol{X})$ and $\bar{p}(\boldsymbol{X}) := \sum_{i=1}^n \xi^i \bar{p}_i(\boldsymbol{X})$. Compute $\boldsymbol{w} := [w_j]_{j=1}^\ell$ and $\bar{\boldsymbol{w}} := [\bar{w}_j]_{i=j}^\ell$ satisfying:

$$p(\boldsymbol{X}) - p(\boldsymbol{z}) = \sum_{j=1}^{\ell} (X_j - z_j) w_j(\boldsymbol{X})$$

$$\bar{p}(\boldsymbol{X}) - \bar{p}(\boldsymbol{z}) = \sum_{j=1}^{\ell} (X_j - z_j) \bar{w}_j(\boldsymbol{X})$$

Such $\boldsymbol{w}$ and $\bar{\boldsymbol{w}}$ can always be found efficiently by Lemma 1.4. For $j \in [\ell]$, set $\mathsf{w}_j := w_j(\boldsymbol{\beta})G + \gamma\bar{w}_j(\boldsymbol{\beta})G \in \mathbb{G}_1$ and $\bar{v} := \bar{p}(\boldsymbol{\beta}) \in \mathbb{F}_q$. The evaluation proof is $\pi := ([\mathsf{w_j}]_{j=1}^{\ell}, \bar{v})$

Check. On input rk, commitments $\boldsymbol{c} := [c_i]_{i=1}^n$, evaluation point $\boldsymbol{z} \in \mathbb{F}_q^\ell$, alleged evaluations $\boldsymbol{v} := [v_i]_{i=1}^n$ over $\mathbb{F}_q$, evaluation proof $\pi := ([\mathsf{w_j}]_{j=1}^{\ell}, \bar{v})$, and challenge $\xi \in \mathbb{F}_q$, $\mathsf{MC_m}.\mathsf{Check}$ proceeds as follows. Compute the linear combination $C := \sum_{i=1}^n \xi^i c_i$, then compute the linear combination of evaluations $v := \sum_{i=1}^n \xi^i v_i$, and check the evaluation proof via the equality $e(C - vG - \gamma\bar{v}G, H) = \prod_{j=1}^{\ell} e(\mathsf{w_j}, \beta_j H - z_j H)$

Lemma 1.1. *The commitment scheme* $\mathsf{MC_m}$ *achieves completeness following Definition B.1*

Proof. Fix any number of variables ℓ , hiding bound B, maximum degree bound D and efficient adversary $\mathcal{A}$. Let $(\mathsf{ck}, \mathsf{rk}) \leftarrow \mathsf{MC_m}.\mathsf{Setup}(1^\lambda, \ell, B, D)$ and $\langle \mathsf{group} \rangle, \mathbb{F}_q$ be the corresponding algebraic structures given by $(\mathsf{ck}, \mathsf{rk})$.

Let $\mathcal{A}$ $(\mathsf{ck}, \mathsf{rk})$ select ℓ-variate polynomials $\boldsymbol{p} := [p_i]_{i=1}^n$ over $\mathbb{F}_q$, evaluation point $\boldsymbol{z} \in \mathbb{F}_q^\ell$, and opening challenge $\xi \in \mathbb{F}_q$. By assumption, we only consider $\mathcal{A}$ which choose $\boldsymbol{p}$, s.t. $deg(\boldsymbol{p}) \leq D$.

Given $\boldsymbol{c} \leftarrow \mathsf{MC_m}.\mathsf{Commit}(\mathsf{ck}, \boldsymbol{p})$ and $\pi \leftarrow \mathsf{MC_m}.\mathsf{Open}(\mathsf{ck}, \boldsymbol{p}, \boldsymbol{z}, \xi)$ we show that for $\boldsymbol{v} := \boldsymbol{p}(\boldsymbol{z})$:

$$\mathsf{MC_m}.\mathsf{Check}(\mathsf{rk}, \boldsymbol{c}, \boldsymbol{z}, \boldsymbol{v}, \pi, \xi) = 1$$

We demonstrate this directly:

$$\begin{aligned}
e(C - vG - \gamma\bar{v}G, H) &= e(\sum_{i=1}^n \xi^i c_i - (\sum_{i=1}^n \xi^i v_i)G - \gamma\bar{p}(\boldsymbol{z})G, H) \\
&= e((p(\boldsymbol{\beta}) - p(\boldsymbol{z}) + \gamma(\bar{p}(\boldsymbol{\beta}) - \bar{p}(\boldsymbol{z})))G, H) \\
&= e((\sum_{j=1}^{\ell}(\beta_j - z_j)w_i(\boldsymbol{\beta}) + \sum_{j=1}^{\ell}\gamma(\beta_j - z_j)\bar{w}_j(\boldsymbol{\beta}))G, H) \\
&= e((\sum_{j=1}^{\ell}(\beta_j - z_j)(w_j(\boldsymbol{\beta}) + \gamma\bar{w}_j(\boldsymbol{\beta}))G, H) \\
&= \prod_{j=1}^{\ell} e((\beta_j - z_j)(w_j(\boldsymbol{\beta}) + \gamma\bar{w}_j(\boldsymbol{\beta}))G, H) \\
&= \prod_{j=1}^{\ell} e(\mathsf{w_j}, \beta_j H - z_j H)
\end{aligned}$$

□

Lemma 1.2. *The commitment scheme* $\mathsf{MC_m}$ *achieves succinctness following Definition B.3*

Proof. For a list of n ℓ-variate polynomials, the scheme $\mathsf{MC_m}$ requires n $\mathbb{G}_1$ elements to commit to $\boldsymbol{c}$, ℓ+1 $\mathbb{G}_1$ elements for the evaluation proof, and the time to check this proof of evaluation requires $\ell + 1$ pairings and one variable-base multi-scalar multiplication of size n. □

Theorem 1.3. *The commitment scheme* $\mathsf{MC_m}$ *achieves hiding following Definition B.4*

Proof. We describe a polynomial-time simulator $\mathcal{S}$ such that, for every number of variables ℓ, hiding bound B, maximum degree D, and efficient adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, the adversary $\mathcal{A}$ cannot distinguish between the real and ideal world experiments.

$\mathcal{S}$ is defined as follows:

$\mathcal{S}.\mathsf{Setup}(1^\lambda, \ell, B, D)$:

1. Run $\mathsf{MC_z}.\mathsf{Setup}(1^\lambda, \ell, B, D)$ and define $\mathsf{trap} := (\mathsf{ck}, \mathsf{rk}, \beta, \gamma)$
2. Output $(\mathsf{ck}, \mathsf{rk}, \mathsf{trap})$

$\mathcal{S}.\mathsf{Commit}(\mathsf{trap}, k;\ \boldsymbol{\omega})$:

1. Parse $\boldsymbol{\omega}$ as $[\omega_i]_{i=1}^n$
2. For $i = 1, \cdots, k$:
   (a) Obtain the random polynomial $\bar{p}_i(\boldsymbol{X})$ from ω_i
   (b) Set $c_i := \bar{p}_i(\boldsymbol{\beta})\gamma G$
3. Output $\boldsymbol{c} := [c_i]_{i=1}^k$

$\mathcal{S}.\mathsf{Open}(\mathsf{trap}, \boldsymbol{p}, \boldsymbol{v}, \boldsymbol{Q}, \xi;\ \boldsymbol{r})$:

1. Parse $\boldsymbol{p} := [p_i]_{i=1}^n$, $\boldsymbol{v} := [v_i]_{i=1}^n$, and $\boldsymbol{\omega} := [\omega_i]_{i=1}^n$
2. Parse query set $\boldsymbol{Q}$ as $T \times \boldsymbol{z}$ for some $T \subseteq [n]$ and $\boldsymbol{z} \in \mathbb{F}_q^\ell$
3. For $i \in T$:
   (a) Obtain the random polynomial $\bar{p}_i(\boldsymbol{X})$ from ω_i
   (b) Set $\tilde{v}_i := \bar{p}_i(\boldsymbol{z}) - \frac{v_i}{\gamma}$
4. Compute $\bar{v} := \sum_{i=1}^n \xi^i \tilde{v}_i$, $v := \sum_{i=1}^n \xi^i v_i$, $\bar{p}(\boldsymbol{X}) = \sum_{i=1}^n \xi^i \bar{p}_i(\boldsymbol{X})$
5. Compute $\bar{\boldsymbol{w}} := [\bar{w}_j]_{j=1}^\ell$ which satisfies $\bar{p}(\boldsymbol{X}) - \bar{p}(\boldsymbol{z}) = \sum_{j=1}^\ell (X_j - z_j)\bar{w}_j(\boldsymbol{X})$
6. If $\boldsymbol{z} \neq \boldsymbol{\beta}$: compute $\mathsf{w}_j = \bar{w}_j(\boldsymbol{\beta})\gamma G$
7. Else $\boldsymbol{z} = \boldsymbol{\beta}$: compute $\mathsf{w}_j = 0G$
8. Output $\pi = ([\mathsf{w}_j]_{j=1}^\ell, \bar{v})$

Clearly, $\mathcal{S}$ is polynomial-time. Associated with each p_i output by $\mathcal{A}$ there is an independently and randomly sampled degree H polynomial $\bar{p}_i$ defined by ω_i. We define a polynomial $\bar{p}_i{}'$ such that in the real world, $\bar{p}_i{}' := \bar{p}_i$, whereas in the ideal world $\bar{p}_i{}' := \bar{p}_i(\boldsymbol{X}) - \frac{p_i(\boldsymbol{X})}{\gamma}$. Observe that each $\bar{p}_i{}'$ is, except with negligible probability, at least degree B in each variable (we will see why this is necessary later) and independently and randomly distributed. It follows that the two polynomials are identically distributed in both worlds for $\leq B$ queries. Furthermore, since $\mathcal{S}.\mathsf{Setup}$ uses $\mathsf{MC_m}.\mathsf{Setup}$ to generate $(\mathsf{ck}, \mathsf{rk})$, we see that $(\mathsf{ck}, \mathsf{rk})$ is also identically distributed.

We claim that upon fixing $(\mathsf{ck}, \mathsf{rk})$ and $\bar{p}_i{}', \forall i \in [n]$, the resulting c_i are given by a deterministic function in $p_i(\boldsymbol{\beta})$ and, after fixing a query point $\boldsymbol{z}$, the evaluation proof π is given by a deterministic function in $(p(\boldsymbol{X}), \boldsymbol{z}, \xi)$. Since these functions are parametrized by values already shown to be identically distributed in the two worlds, it follows that their outputs will also be identically distributed.

We define $\mathsf{factor} : \mathbb{F}[X_1, \cdots, X_\ell] \to \mathbb{F}[X_1, \cdots, X_\ell]^\ell$ to be the polynomial factorizing algorithm at the point $\boldsymbol{z}$ described in Lemma 1.4. Note that this is a linear function. We claim that the following relations hold in both worlds:

$$c_i(p_i(\boldsymbol{\beta})) := p_i(\boldsymbol{\beta})G + \bar{p}_i{}'(\boldsymbol{\beta})\gamma G$$
$$\pi = ([\mathsf{w_j}]_{j=1}^{\ell}, \bar{v})$$

where

$$\mathsf{w_j}(\boldsymbol{z}, p_i(\boldsymbol{X})) = \begin{cases} \mathsf{factor}(p(\boldsymbol{X}) + \gamma\bar{p}'(\boldsymbol{X}))_j(\boldsymbol{\beta})G & \text{if } \boldsymbol{z} \neq \boldsymbol{\beta} \\ 0G & \text{if } \boldsymbol{z} = \boldsymbol{\beta} \end{cases}, \qquad \bar{v}(\boldsymbol{z}, \xi) = \sum_{i=1}^{n} \xi^i \bar{p}_i{}'(\boldsymbol{z})$$

Now we show that the above describe the outputs of $\mathsf{MC_m}$ and $\mathcal{S}$.

Indistinguishability of commitments. In the real world we have:

$$c_i = p_i(\boldsymbol{\beta})G + \bar{p}_i(\boldsymbol{\beta})\gamma G$$

since we have defined $\bar{p}_i' := \bar{p}_i$, equivalence follows immediately. In the ideal world, we have that:

$$c_i = \bar{p}_i(\boldsymbol{\beta})\gamma G$$

here we have defined $\bar{p}_i'(\boldsymbol{X}) := \bar{p}_i(\boldsymbol{X}) - \frac{p(\boldsymbol{X})}{\gamma}$. Plugging this in we get that:

$$\begin{aligned} c_i &= p_i(\boldsymbol{\beta})G + \gamma\bar{p}_i'(\boldsymbol{\beta})G \\ &= p_i(\boldsymbol{\beta})G + \gamma(\bar{p}_i(\boldsymbol{\beta}) - \frac{p_i(\boldsymbol{\beta})}{\gamma})G \\ &= \bar{p}_i(\boldsymbol{\beta})\gamma G \end{aligned}$$

Which is exactly what $\mathcal{S}$ outputs. Thus, the commitments are indistinguishable with respect to all adversaries.

Indistinguishability of evaluation proofs. In the real world, $\bar{v} = \sum_{i=1}^{n} \xi^i \bar{p}_i(\boldsymbol{z})$ which coincides directly since $\bar{p}_i' = \bar{p}_i$. In the ideal world we have that $\bar{v} = \sum_{i=1}^{n} \xi^i \tilde{v}_i$ which also follows directly since $\tilde{v}_i = \bar{p}_i'(\boldsymbol{z})$. Thus, the $\bar{v}$ are indistinguishable to all adversaries.

Finally, we consider each $[\mathsf{w}_j]_{j=1}^{\ell}$. In the real world, we have that:

$$\begin{aligned} \mathsf{w}_j &= \mathsf{factor}(p(\boldsymbol{X}))_j(\boldsymbol{\beta})G + \gamma\mathsf{factor}(\bar{p}(\boldsymbol{X}))_j(\boldsymbol{\beta})G \\ &= \mathsf{factor}(p(\boldsymbol{X}) + \gamma\bar{p}(\boldsymbol{X}))_j(\boldsymbol{\beta})G \end{aligned}$$

since we have defined $\bar{p}_i' := \bar{p}_i$, equivalence follows immediately. In the ideal world, we have that:

$$\mathsf{w}_j := \mathsf{factor}(\gamma\bar{p}(\boldsymbol{X}))_j(\boldsymbol{\beta})G$$

here we have defined $\bar{p}_i'(\boldsymbol{X}) := \bar{p}_i(\boldsymbol{X}) - \frac{p(\boldsymbol{X})}{\gamma}$. Plugging in we get that:

$$\begin{aligned}
\mathsf{w}_j &= \mathsf{factor}(p(\boldsymbol{X}) + \gamma\bar{p}'(\boldsymbol{X}))_j(\boldsymbol{\beta})G \\
&= \mathsf{factor}(p(\boldsymbol{X}) + \gamma(\bar{p}(\boldsymbol{X}) - \frac{p(\boldsymbol{X})}{\gamma}))_j(\boldsymbol{\beta})G \\
&= \mathsf{factor}(\gamma\bar{p}(\boldsymbol{X}))_j(\boldsymbol{\beta})G
\end{aligned}$$

Thus, our expression for $[\mathsf{w}_j]_{j=1}^{\ell}$ is correct. Note that for any polynomial $q \in \mathbb{F}_q[X_1, \cdots, X_\ell]$, if q does not contain the indeterminate X_j, it will be in the kernel of $\mathsf{factor}(q)_j$. It follow that each w_j leaks whether $\bar{p}'$ contains the indeterminate X_j. Thus, in order for the $\bar{p}'$ to be indistinguishable, we must require that they have at least degree 1 in each of the ℓ indeterminates. We conclude that no adversary can distinguish between the two worlds. $\square$

Lemma 1.4. *Let $p(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ be an ℓ-variate polynomial. Then $\forall \boldsymbol{z} \in \mathbb{F}_q^{\ell}$, there exists polynomials $w_i(\boldsymbol{X})$ such that $p(\boldsymbol{X}) - p(\boldsymbol{z}) = \sum_{i=1}^{\ell}(X_i - z_i)w_i(\boldsymbol{X})$. Furthermore, all the w_is can be found with a polynomial-time algorithm.*

Proof. We can recover each w_i with a single polynomial division. Start by dividing $p(\boldsymbol{X}) - p(\boldsymbol{z})$ by $(X_1 - z_1)$ and define the quotient as $w_1(\boldsymbol{X})$. We have can now express $p(\boldsymbol{X}) - p(\boldsymbol{z}) = (X_1 - z_1)w_1(\boldsymbol{X}) + r(X_2, \cdots, X_\ell)$. Notably, the remainder of the division is a polynomial in terms of $X_2, \cdots, X_\ell$. We divide this polynomial by $(X_2 - z_2)$, yielding $w_2(\boldsymbol{X})$ and a remainder in terms of $X_3, \cdots, X_\ell$. We continue this until we can express $p(\boldsymbol{X}) - p(\boldsymbol{z}) = \sum_{i=1}^{\ell}(X_i - z_i)w_i(\boldsymbol{X}) + r$. We evaluate the indeterminate $\boldsymbol{X}$ at $\boldsymbol{z}$:

$$\begin{aligned}
p(\boldsymbol{z}) - p(\boldsymbol{z}) &= \sum_{i=1}^{\ell}(z_i - z_i)w_i(\boldsymbol{X}) + r \\
0 &= 0 + r \\
\implies p(\boldsymbol{X}) - p(\boldsymbol{z}) &= \sum_{i=1}^{\ell}(X_i - z_i)w_i(\boldsymbol{X})
\end{aligned}$$

$\square$