A Simple Range Proof From Polynomial Commitments

Dan Boneh, Ben Fisch, Ariel Gabizon, and Zac Williamson

Let's construct a simple zero knowledge range proof from a hiding polynomial commitment scheme (PCS).

The setup

Let p be a prime, where $p > 2^n$ for some n. We want a commitment scheme for elements in $\mathbb{F}_p$ that allows a prover to efficiently convince a verifier that a committed quantity $z \in \mathbb{F}_p$ is in the range $0 \leq z < 2^n$.

We show that for a committed $z \in \mathbb{F}_p$, the prover can provide an HVZK proof to convince the verifier that $0 \leq z < 2^n$ by committing to **two** polynomials of degree $(n+1)$, and running the polynomial evaluation protocol **three** times. Therefore:

- For the pairing-based polynomial commitment scheme of Kate, Zaverucha and Goldberg, this gives a range proof of length $O_\lambda(1)$ that can be verified in time $O_\lambda(1)$, with a trusted setup and an updatable SRS of size $O_\lambda(n)$.
- For the DARK polynomial commitment scheme of Bünz, Fisch, and Szepieniec, this gives a range proof of length $O_\lambda(\log n)$ that can be verified in time $O_\lambda(\log n)$, with no trusted setup.
- For comparison, recall that Bulletproofs give a range proof with no trusted setup of length $O_\lambda(\log n)$ that can be verified in time $O_\lambda(n)$.

In what follows we use $\mathbb{F}_p^{(<n)}[X]$ to denote polynomials in $\mathbb{F}_p[X]$ of degree less than n. We assume that n divides $p-1$ so that there is an element $\omega \in \mathbb{F}_p$ of order n. Let $H = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$.

The commitment scheme

Suppose that we have available a hiding and binding PCS for polynomials in $\mathbb{F}_p^{(<n)}[X]$. Moreover, we assume that the polynomial evaluation protocol is HVZK.

To commit to an element $z \in \mathbb{F}_p$, choose an arbitrary polynomial $f \in \mathbb{F}_p^{(<n)}[X]$ such that $f(1) = z$. Taking f as the constant polynomial $f(X) = z$ is sufficient. The commitment to z is the polynomial commitment $\mathbf{com}_f$ to f.

If the PCS is additive, then the commitment scheme is additively homomorphic: given commitments to z_1 and z_2 in $\mathbb{F}_p$, anyone can construct a commitment to $z_1 + z_2$.

Range proof for the range $[0, 2^n)$

Let $\mathbf{com}_f$ be a commitment to $z \in \mathbb{F}_p$ so that $f(1) = z$, as above. Let $z_0, \ldots, z_{n-1} \in \{0,1\}$ be the binary digits of z, so that $z = \sum_{i=0}^{n-1} 2^i \cdot z_i$.

Now, given $\mathbf{com}_f$, the prover proves that $0 \leq z < 2^n$, by constructing a degree-$(n-1)$ polynomial $g \in \mathbb{F}_p^{(<n)}[X]$ such that

$$g(\omega^{n-1}) = z_{n-1} \quad \text{and} \quad g(\omega^i) = 2g(\omega^{i+1}) + z_i \ \text{ for all } i = n-2, \ldots, 0.$$

Observe that $g(1) = g(\omega^0) = \sum_{i=0}^{n-1} 2^i \cdot z_i = z$. Now the prover needs to prove three things:

1. $g(1) = f(1)$,
2. $g(\omega^{n-1}) \in \{0,1\}$, and
3. $g(X) - 2g(X\omega) \in \{0,1\}$ for all $x \in H \setminus \{\omega^{n-1}\}$.

Condition (1) proves that $g(1) = z$; Conditions (2) and (3) prove that $z_0, \ldots, z_{n-1}$ are all in $\{0,1\}$ and are the binary digital of z. Together, these conditions prove that $0 \leq z < 2^n$, as required.

To prove Conditions (1)-(3), the prover sends to the verifier a polynomial commitment to g. It then proves to the verifier that the following polynomials evaluate to zero for all $x \in H$:

$$\begin{aligned} w_1(X) &= (g - f) \cdot \left(\tfrac{X^n - 1}{X - 1}\right), \\ w_2(X) &= g \cdot (1 - g) \cdot \left(\tfrac{X^n - 1}{X - \omega^{n-1}}\right), \quad \text{and} \\ w_3(X) &= \big[g(X) - 2g(X\omega)\big] \cdot \big[1 - g(X) + 2g(X\omega)\big] \cdot (X - \omega^{n-1}). \end{aligned}$$

This can be done efficiently using a batch opening technique described in this paper. The verifier sends a radom $\tau \in \mathbb{F}_p$ to the prover, and the prover computes the quotient polynomial

$$q(X) = (w_1 + \tau w_2 + \tau^2 w_3)/(X^n - 1).$$

The prover sends a polynomial commitment to q to the verifier, and then proves that the polynomial

$$w(X) = w_1 + \tau w_2 + \tau^2 w_3 - q \cdot (X^n - 1)$$

is the zero polynomial. To do so, the verifier sends a random $\rho \in \mathbb{F}_p$ to the prover, and together they run the evaluation protocol three times: once for $g(\rho)$, once for $g(\rho\omega)$, and once for evaluating $\hat{w}(\rho)$, where $\hat{w}(X) = f(X) \cdot \left(\frac{\rho^n - 1}{\rho - 1}\right) + q(X) \cdot (\rho^n - 1)$. This $\hat{w}$ is a linear combination of f and q, and therefore the verifier can construct a commitment to $\hat{w}$ using the additiving property of the PCS. The three evaluations, $g(\rho)$, $\hat{w}(\rho)$, and $g(\rho\omega)$, along with ρ and τ, are sufficient to evaluate $w(\rho)$ and confirm that the result is zero. This proves, with high probability, that w is the zero polynomial.

There is one remaining issue, which is that revealing $g(\rho)$, $\hat{w}(\rho)$, and $g(\rho\omega)$ is not zero-knowledge. The fix is simple: the prover constructs g as a degree $n+1$ polynomial by interpolating g to a random value at two more points ω', ω'' outside H. That is, g is defined in exactly the same way on all points in H, but $g(\omega') = \alpha$ and $g(\omega'') = \beta$ for random $\alpha, \beta \in \mathbb{F}_p$ and $\omega, \omega' \notin H$. Since g has the same values over all points in H, this has no effect on the relations checked above. This is zero-knowledge because $g(\rho)$ and $g(\rho\omega)$ can now be simulated as independent random values in $\mathbb{F}_p$. Moreover, the value of $\hat{w}(\rho)$ is completely determined by the fact that $w(\rho) = 0$, and can therefore also be simulated. Note that we need to restrict the choice of ρ to $(\mathbb{F}_p \setminus H)$ to ensure that the simulation is valid.

This entire process makes two polynomial commitments, to g and q, and uses the polynomial evaluation protocol three times to evaluate $g(\rho)$, $\hat{w}(\rho)$, and $g(\rho\omega)$. We note that, if needed, it is possible to reduce the degree of g by writing z in a base greater than 2.

Other constructions

The Bulletproofs paper (Section 4.1) shows how to implement a range proof using an inner-product argument. The DARK paper shows how to implemement an inner-product argument using a polynomial commitment scheme. Combining the two gives another way to construct a range proof from a polynomial commitment scheme with similar properties as the range proof described above. Interestingly, the resulting protocol is quite different.

Implementation/related work

This scheme initially appeared as a component of Turbo Plonk by Ariel Gabizon and Zac Williamson