IOP for RICS

Lecture 22

Recall

SNARKs
from IOPs

- Interactive version of PCP: Allow committing to multiple strings over multiple rounds
  - Can be made into a proof system using Merkle hashes
- Polynomial IOP: the strings are polynomial evaluations
  - Can be implemented using any polynomial commitment scheme
  - In particular, there are polynomial commitment schemes which are derived from "standard" IOPs (in turn implemented using Merkle hashes)
- Public coin
  - So that it can be made non-interactive

IOP for R1CS

- R1CS: m constraints on $z \in \mathbb{F}^n$ of the form $\langle a_i, z \rangle \langle b_i, z \rangle = \langle c_i, z \rangle$
- Written as $Az \circ Bz = Cz$, where , $A_{ij} = (a_i)_j$, $B_{ij} = (b_i)_j$, $C_{ij} = (c_i)_j$
- Can express conditions like F(z)=0 where F is an arithmetic circuit using sparse matrices (A,B,C) (each row having only a constant number of non-zero entries)
- Plan: An (information-theoretic) IOP for R1CS
  - Uses a univariate sum-check protocol
  - The prover's complexity can be kept proportional to the number of non-zero entries in A, B, C
- Can be converted into a SNARK using any univariate polynomial commitment scheme

Univariate Sum-Check

- Recall $Z_H(X) = \Pi_{\sigma \in H} (X - \sigma)$
- Fact: Let H be a multiplicative subgroup of a field $\mathbb{F}$. For any univariate polynomial U over $\mathbb{F}$, $\Sigma_{\sigma \in H} U(\sigma) = 0$ iff $\exists$ polynomials Q, R s.t degree(Q) $\leq$ degree(U) - |H|, and degree(R) $\leq$ |H|-2 and $U(X) = Z_H(X)\, Q(X) + X\, R(X)$
- To prove $\Sigma_{\sigma \in H} U(\sigma) = 0$ using a polynomial IOP, prover provides oracles (of the right degrees) for Q, R (in addition to the oracle for U) and the verifier checks $U(\beta) = Z_H(\beta)\, Q(\beta) + \beta\, R(\beta)$ for $\beta \leftarrow \mathbb{F}$
- Fact: If H is a multiplicative subgroup, $Z_H(X) = X^m - 1$, where m=|H|
  - Because $a^m - 1 = 0$ $\forall m \in H$ (m being the order of the group) and so $Z_H(X)$ divides $X^m - 1$. Comparing coefficients of X^m, they are equal.
- $Z_H(\beta) = \beta^m - 1$ can be computed in O(log m) time. U, Q, R will be queried at β.

Polynomial IOP for R1CS

- Recall R1CS: m constraints on $z \in \mathbb{F}^n$ of the form $\langle a_i, z\rangle \langle b_i, z\rangle = \langle c_i, z\rangle$
- Written as $Az \circ Bz = Cz$, where , $A_{ij} = (a_i)_j$, $B_{ij} = (b_i)_j$, $C_{ij} = (c_i)_j$
- Identify row and column indices with elements in H and H', two multiplicative subgroups of $\mathbb{F}$
- Polynomial IOP: Degree m-1 polynomial oracles to be given: $P_z(X)$ s.t. $\forall \sigma \in H$, $P_z(\sigma) = z_\sigma$, and for $M \in \{A,B,C\}$, $P_M(X)$ s.t. $\forall \sigma \in H$, $P_M(\sigma) = (Mz)_\sigma$
- Need to check $\forall \sigma \in H$, $P_M(\sigma) = (Mz)_\sigma$ for $M \in \{A,B,C\}$ and also $P_A(\sigma)P_B(\sigma) = P_C(\sigma)$, without going through elements of H individually

Polynomial IOP for R1CS

- Need to check $\forall \sigma \in H$, $P_M(\sigma) = (Mz)_\sigma$ for $M \in \{A,B,C\}$ and also $P_A(\sigma)P_B(\sigma) = P_C(\sigma)$, without going through elements of H individually
- Note: Degree of $P_A(X)P_B(X) - P_C(X)$ is $2(m-1)$, but it is required to be 0 only in m points. So, it need not be that $P_A(X)P_B(X) = P_C(X)$
- $\forall \sigma \in H \;\; P_A(\sigma)P_B(\sigma) = P_C(\sigma) \Leftrightarrow \exists Q \; P_A(X)P_B(X) - P_C(X) = Z_H(X) \cdot Q(X)$

  (where Q is of degree m-1)

- Prover should provide an oracle for the polynomial Q as well. Verifier checks $P_A(\beta)P_B(\beta) - P_C(\beta) = Z_H(\beta) \cdot Q(\beta)$ for $\beta \leftarrow \mathbb{F}$, by querying the oracles P_A, P_B, P_C, Q and evaluating $Z_H(\beta) = \beta^n - 1$ itself (in $O(\log n)$ time).

Polynomial IOP for R1CS

- Need to check $\forall \sigma \in H$, $P_M(\sigma) = (Mz)_\sigma$ for $M \in \{A,B,C\}$ and also $P_A(\sigma)P_B(\sigma) = P_C(\sigma)$, without going through elements of H individually
  - Encode each $M \in \{A,B,C\}$ as a polynomial $T_M(X,Y)$ of degree m-1 in X and n-1 in Y s.t. $\forall \sigma \in H, \sigma' \in H'$ $T_M(\sigma,\sigma') = M_{\sigma,\sigma'}$ for $M \in \{A,B,C\}$
    - Let $t^{(i)}(Y) = \Sigma_j\ t_{ij}\ Y^j$ be the degree n-1 polynomial such that $t^{(i)}(j) = M_{ij}$. Let $s^{(j)}(X)$ be the degree m-1 polynomial s.t. $s^{(j)}(i) = t_{ij}$. Then let $T_M(X,Y) = \Sigma_j\ s^{(j)}(X)\ Y^j$
  - Need to check $\forall \sigma \in H$, $P_M(\sigma) = \Sigma_{\sigma'}\ T_M(\sigma,\sigma')\ z_{\sigma'}$. Since $P_M(X)$ and $T_M(X,\sigma')$ both have degree m-1 while $|H|=m$, this is equivalent to checking $P_M(X) = \Sigma_{\sigma'}\ T_M(X,\sigma')\ z_{\sigma'}$.
  - Enough to check $P_M(\beta) = \Sigma_{\sigma'}\ T_M(\beta,\sigma')\ z_{\sigma'}$ for $\beta \leftarrow \mathbb{F}$
    - Given 1+..+1 (n times) ≠ 0 in $\mathbb{F}$, let $U(Y) = T_M(\beta,Y)\ P_Z(Y) - P_M(\beta)\cdot n^{-1}$. Then to check $\Sigma_{\sigma' \in H'}\ U(Y) = 0$. Univariate sum check.
    - U needs to be evaluated at a random β'. Need $T_M(\beta,\beta')$.

Polynomial IOP for R1CS

- Need to check $\forall \sigma \in H$, $P_M(\sigma) = (Mz)_\sigma$ for $M \in \{A,B,C\}$ and also $P_A(\sigma)P_B(\sigma) = P_C(\sigma)$, without going through elements of H individually
  - Encode each $M \in \{A,B,C\}$ as a polynomial $T_M(X,Y)$ of degree m-1 in X and n-1 in Y s.t. $\forall \sigma \in H, \sigma' \in H'$ $T_M(\sigma,\sigma') = M_{\sigma,\sigma'}$ for $M \in \{A,B,C\}$
  - Need to evaluate $T_M(\beta,\beta')$ at $\beta,\beta' \leftarrow \mathbb{F}$
  - Though M has mn entries, often it is sparse.
  - Goal: a polynomial commitment scheme for T_M in which the prover's complexity is proportional to the number of non-zero entries in M, say k
  - Will work with m×m square matrices and let H=H'
  - Idea: Write $T_M(\beta,\beta')$ as a univariate sum
  - Encode the k non-zero entries in M using degree k-1 polynomials V_{row}, V_{col} , and V_{val} and indexed using entries in a multiplicative subgroup K of size k, so that a non-zero M_{ij} $(i,j \in H)$ is indexed using $\kappa \in K$, $i=V_{row}(\kappa)$, $j=V_{row}(\kappa)$, $M_{ij} = c_\kappa V_{val}(\kappa)$

Polynomial IOP for R1CS

- Let $W(X,Y) = \Sigma_{i=0 \text{ to } m-1} X^i Y^{m-1-i}$. Note $W(X,Y)(X-Y) = X^m - Y^m$. Then $W(x,y) = 0$ for distinct $x,y \in H$. $W(x,x) = mx^{m-1} \neq 0$.
- A non-zero M_{ij} ($i,j \in H$) is indexed using $\kappa \in K$, $i = V_{row}(\kappa)$, $j = V_{col}(\kappa)$, $M_{ij} = c_\kappa \, V_{val}(\kappa)$, where $c_\kappa = W(i,i).W(j,j)$ where κ indexes M_{ij}
- Claim: $T_M(X,Y) = \Sigma_{\kappa \in K} W(X,V_{row}(\kappa)) \, W(Y,V_{col}(\kappa)) \, V_{val}(\kappa)$
  - They agree on $H \times H$ and have degree $m-1$ on X,Y
- Let $D(Z) = W(\beta,V_{row}(Z)) \, W(\beta',V_{col}(Z)) \, V_{val}(Z))$
- D satisfies $T_M(\beta,\beta') = \Sigma_{\kappa \in K} D(\kappa)$
- Use univariate sum-check to evaluate $\Sigma_{\kappa \in K} D(\kappa)$
  - For that, need to evaluate D at a random point. Use oracles for V_{row}, V_{col}, V_{val} and compute $W(x,y) = (x^m - y^m)(x-y)^{-1}$