Primer PLONK-a

PLONK na primeru $x^3 + x + 5 = y$

Prover dokazuje da zna tajnu vrednost x takvu da važi sledeća jednačina:

$x^3 + x + 5 = y$

Ovde je y javni input. Na primer, za y = 35 rešenje će biti x = 3.

Aritmetizacija izraza

$$x^3 + x + 5 = y$$

Uvodimo pomoćne promenljive u i v koje predstavljaju međurezultate.

Izraz razbijamo na pojedinačna množenja i sabiranja

Početni izraz razlažemo na tri koraka (gate-a)

1. $u = x \cdot x$
2. $v = u \cdot x$
3. $v + x + 5 - y = 0$

Konkretno za y = 35:

Pošto je x = 3, onda je u = 9 i v = 27.

Witness tabela

Svaki red predstavlja jedan gate. Ova tabela se popunjava nakon što se ubace privatni i javni inputi.

a	b	c	Constraint
x	x	u	$a \cdot b - c = 0$
u	x	v	$a \cdot b - c = 0$
v	x	0	$a + b + 5 - y = 0$

Kolone **a** i **b** predstavljaju ulazne vrednosti u gate, a kolona **c** predstavlja izlazne vrednosti.

U trećem redu je c = 0 zato što je izlaz public input y

Prva dva reda računaju x^2 i x^3. Treći red proverava da li je dobijeni izraz x^3+x+5 zaista jednak javnom inputom y.

Witness tabela

U našem primeru će witness tabela izgledati ovako:

a	b	c
3	3	9
9	3	27
27	3	0

Selektor tabela

Sve constraint-e treba da napišemo u sledećem obliku: $q_l \cdot a + q_r \cdot b + q_m \cdot a \cdot b + q_o \cdot c + q_c + PI = 0$

qL	qR	qM	qO	qC	PI	Constraint
0	0	1	–1	0	0	$a \cdot b - c = 0$
0	0	1	–1	0	0	$a \cdot b - c = 0$
1	1	0	0	5	–y	$a + b + 5 - y = 0$

Od tabela do polinoma

PLONK ne proverava tabele direktno. Proverava da se odgovarajuća polinomska relacija poklapa u tačkama koje predstavljaju redove tabele.

Imamo unapred dogovorene tačke h_1, h_2, h_3.

Prvi red tabela se čita u h_1, drugi u h_2, a treći u h_3.

Interpolacija

Iz svake kolone witness tabele dobijamo po jedan polinom: A(X), B(X), C(X).
Isto radimo i za selektor tabelu i dobijamo polinome: $q_l(X)$, $q_r(X)$, $q_m(X)$, $q_o(X)$, $q_c(X)$ i PI(X).

Napomena: selektorski polinomi se računaju u fazi kompilacije (osim polinoma PI(X)).
Witness polinome prover računa tek u fazi dokazivanja, za konkretne inpute.

Od tabela do polinoma

Witness polinomi:

$A(h_1)=3, \quad A(h_2)=9, \quad A(h_3)=27$

$B(h_1)=3, \quad B(h_2)=3, \quad B(h_3)=3$

$C(h_1)=9, \quad C(h_2)=27, \quad C(h_3)=0$

Pošto imamo tri različite tačke h_1, h_2 i h_3, za svaki niz vrednosti postoji jedinstven polinom stepena najviše 2 koji uzima baš te vrednosti u tim tačkama.
Dakle i witness polinomi i selektor polinomi će biti stepena najviše 2.

Selektor polinomi:

$q_l(h_1)=0, \quad q_l(h_2)=0, \quad q_l(h_3)=1$

$q_r(h_1)=0, \quad q_r(h_2)=0, \quad q_r(h_3)=1$

$q_m(h_1)=1, \quad q_m(h_2)=1, \quad q_m(h_3)=0$

$q_o(h_1)=-1, \quad q_o(h_2)=-1, \quad q_o(h_3)=0$

$q_c(h_1)=0, \quad q_c(h_2)=0, \quad q_c(h_3)=5$

$PI(h_1)=0, \quad PI(h_2)=0, \quad PI(h_3)=-35$

Copy constraints

Gate constraints proveravaju samo da je svaki red lokalno ispravan.

Bez dodatnih uslova, redovi ne moraju da dele iste vrednosti, pa tabela može biti lokalno tačna, a ceo račun pogrešan. Zato su nam potrebni i copy constraints.

Beležimo vrednosti iz kola koje su iste:

$a_1 = b_1 = b_2 = b_3 = x$

$c_1 = a_2 = u$

$c_2 = a_3 = v$

Za proveru ispunjenosti copy constraint-a konstruiše se polinom Z(X). Za opis konstrukcije ovog polinoma možete pogledati originalni PLONK rad.

Šta se dalje radi sa polinomima?

Sve relacije iz PLONK tabele želimo da spojimo u jedan polinom G(X).
Napomena: radi jednostavnosti, nećemo posmatrati polinom Z(X), koji bi takođe trebalo da se na neki način pojavi u polinomu G(X).

Definišemo polinom:
$G(X) = q_l(X) \cdot A(X) + q_r(X) \cdot B(X) + q_m(X) \cdot A(X) \cdot B(X) + q_o(X) \cdot C(X) + q_c(X) + PI(X)$

Ideja je sledeća: ako su svi constraint-i ispunjena, onda polinom G(X) mora da bude jednak nuli u h_1, h_2, h_3, tj. mora da važi: $G(h_1) = 0$, $G(h_2) = 0$, $G(h_3) = 0$.

Sada uvodimo polinom Z_h:
$Z_h(X) = (X - h_1)(X - h_2)(X - h_3)$

Ovaj polinom je konstruisan tako da važi:
$Z_h(h_1) = Z_h(h_2) = Z_h(h_3) = 0$

Pošto G(X) takođe ima nule u tačkama h_1, h_2 i h_3, i većeg je stepena od $Z_h(X)$, postojaće polinom T(X) takav da važi:
$G(X) = Z_h(X) \cdot T(X)$

Otvaranje polinoma

Verifier bira random tačku z, a prover pomoću KZG commitment šeme dokazuje da zna polinome A(X), B(X), C(X), T(X) i Z(X), bez slanja celih polinoma.

Verifier zatim proverava njihova otvaranja u tački z i koristeći vrednosti A(z), B(z), C(z), T(z) i Z(z) proverava da li važi relacija:
$G(z) = Z_h(z) \cdot T(z)$
Ovde je G(X) ukupan constraint polinom: u njega su uključeni i gate constraints i copy constraints. Ako relacija važi u random izabranoj tački z, verifier dobija uverenje da su constraint-i iz kola zadovoljeni.

Napomena: Da bi dokaz bio non-interactive, izazovi se ne moraju stvarno slati. Umesto toga se koristi Fiat–Shamir transformacija.