I. Custom Gates — An Example

binary decomposition gate $\odot$ $\qquad \vec{c} \to \odot \to c$

$\vec{c} = [c_1, c_2, c_3] \in Bin^3$

$c = c_3 + 2c_2 + 4c_1 \quad \in \mathbb{F} \quad \longrightarrow$

$\quad = c_3 + 2(c_2 + 2(c_1 + 2\times 0))$

accumulator

$a_0 = 0$

$a_1 = c_1 + 2a_0 = c_1$

$a_2 = c_2 + 2a_1 = c_2 + 2c_1$

$a_3 = c_3 + 2a_2 = c_3 + 2c_2 + 4c_1 = c$

selector	witness table		constraints			
s	b	a	binary b	accumulate	Init	Output
0	$b_0 = c$	$a_0 = 0$			$a_0 = 0$	$b_0 - a_3 = 0$
1	$b_1 = c_1$	$a_1 = b_1 + 2a_0$	$b_1(1-b_1) = 0$	$a_1 - b_1 - 2a_0 = 0$		
1	$b_2 = c_2$	$a_2 = b_2 + 2a_1$	$b_2(1-b_2) = 0$	$a_2 - b_2 - 2a_1 = 0$		
1	$b_3 = c_3$	$a_3 = b_3 + 2a_2$ $= c$	$b_3(1-b_3) = 0$	$a_3 - b_3 - 2a_2 = 0$		
			$b_i(1-b_i) = 0$	$a_i - b_i - 2a_{i-1} = 0$	$a_0 = 0$	$b_0 - a_3 = 0$

polynomials: $s(X)$, $b(X)$, $a(X)$

constraints: $s(X)[b(X) - b^2(X)] = 0$

$+ \alpha \; s(X)[a(X) - b(X) - 2a(\omega^{-1}X)] = 0$

$+ \alpha^2 [1 - s(X)]\, a(X) = 0$

$+ \alpha^3 [1 - s(X)][b(X) - a(\omega^3 X)] = 0$

Define $F(X) = \bigcirc + \alpha \bigcirc + \alpha^2 \bigcirc + \alpha^3 \bigcirc = q(X) \cdot Z_H(X)$

Discussion: 1. useful when the same operation is repeated many times.

2. accumulator columns do not need to be wired.

3. proof size increases, because we reveal more operations

Examples: Elliptic curve multiplication, algebraic hashes

II Halo 2 Lookup

t, f, prove $f \subset t$ eg. $t = \{1, 2, 3, 4, 5, 6\}$

reorder $f' = \{1, 1, 1, 3, 4, 4\}$

$t' = \{1, \underline{2}, \underline{5}, 3, 4, \underline{6}\}$

1. f', t' are the permutation of f, t
2. $f'_i = t'_i$ or $f'_i = f'_{i-1}$ $f'_i = t'_i$

III. PLookup

t, f 3 cases: $(t_j, f_k), (f_j, f_{j+1}), (f_j, t_k)$

$s = t \cup f$ in the order of t

multi set $\{(s_i, s_{i+1})\} = \{(t_i, t_{i+1})\} \cup \boxed{\{(f_i, f_{i+1})\}}$ $\times$ $\{(f_i, f_i)\}$

$\{(s_i + \beta s_{i+1})\} = \{(t_i + \beta t_{i+1})\} \cup \{(f_i + \beta f_i)\}$

nonzero difference $\text{''} (1+\beta) f_i$