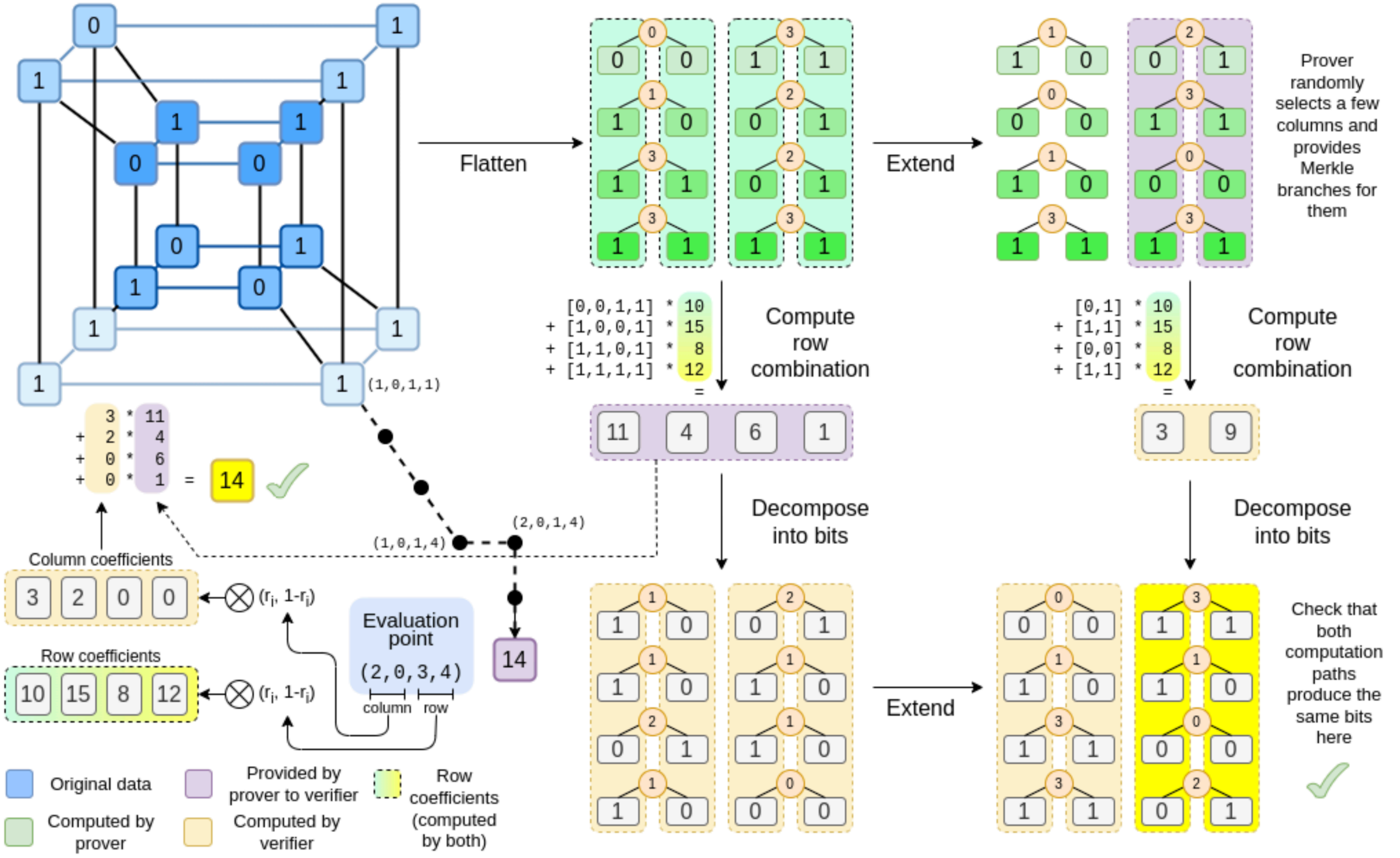
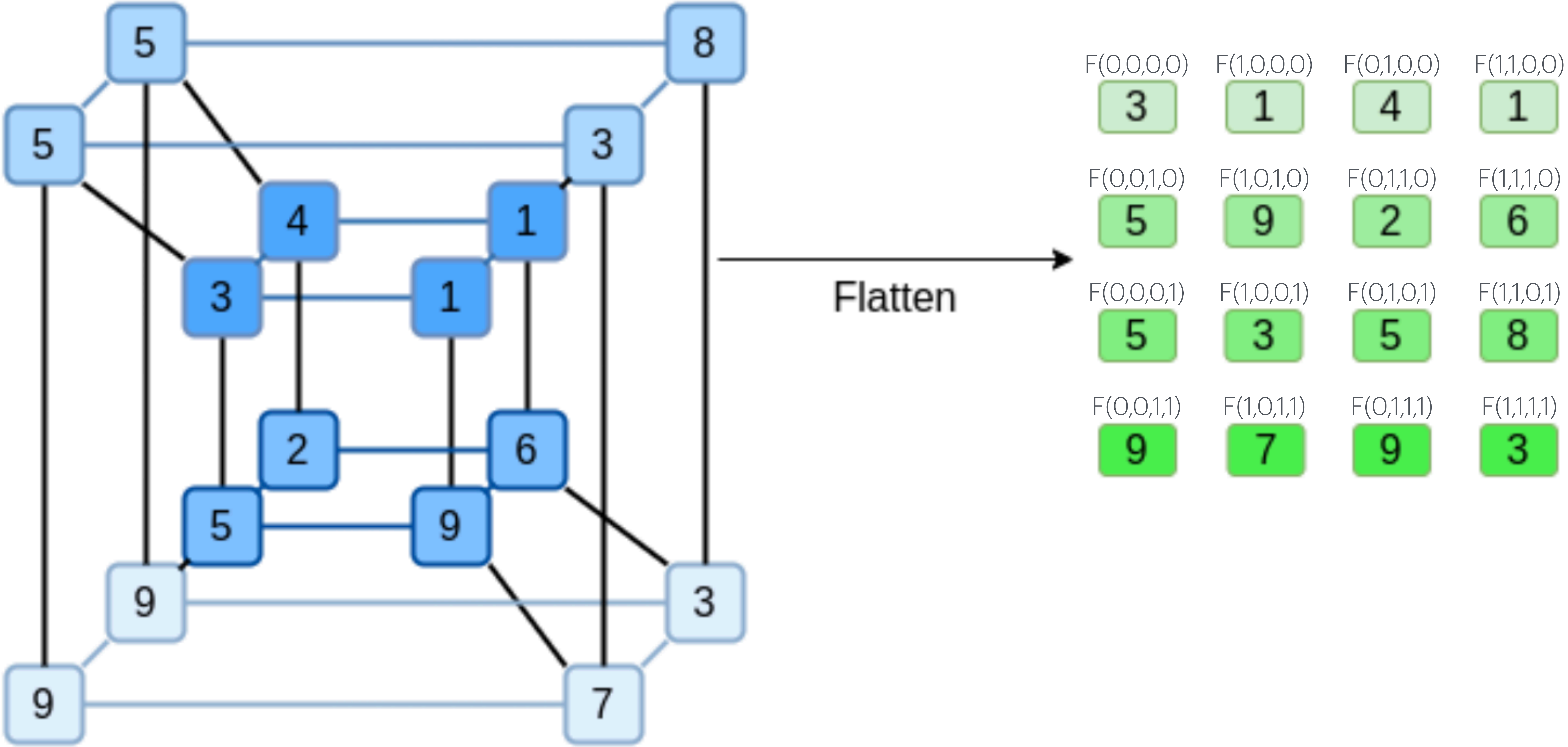
Binius



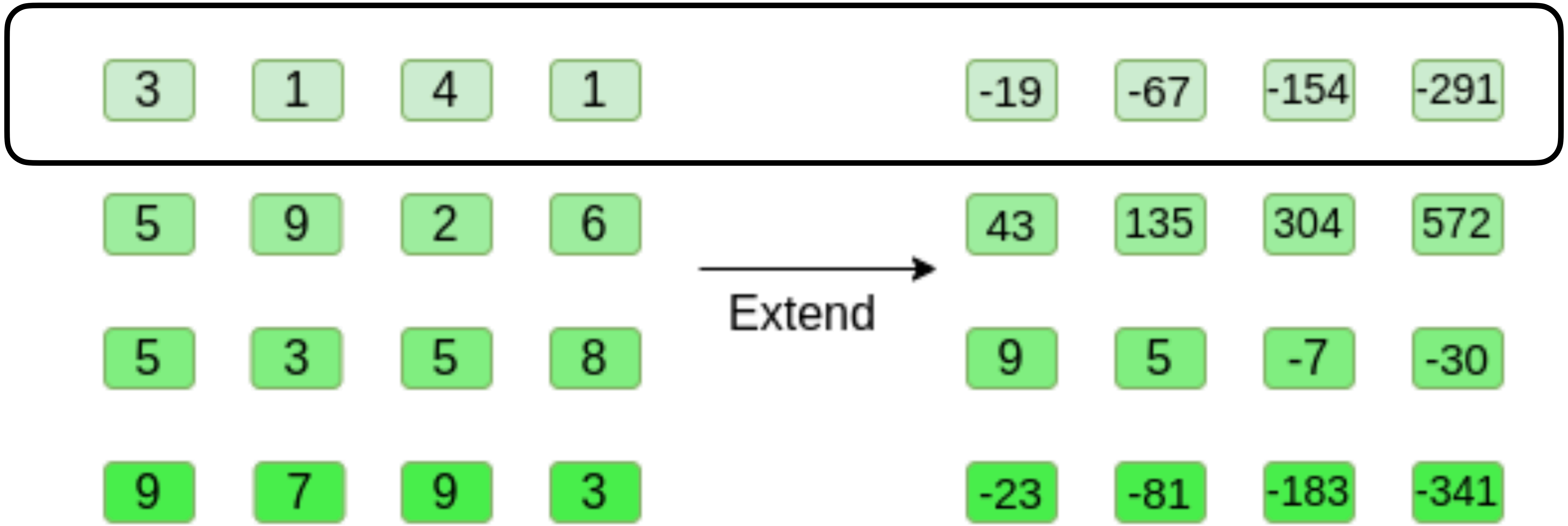
Dana Ben Porath, Ingonyama. May 2024

Flatten


5
8
5
3
4
1
3
1
2
6
5
9
9
3
9
7
Flatten
F(0,0,0,0)
3
F(1,0,0,0)
1
F(0,1,0,0)
4
F(1,1,0,0)
1
F(0,0,1,0)
5
F(1,0,1,0)
9
F(0,1,1,0)
2
F(1,1,1,0)
6
F(0,0,0,1)
5
F(1,0,0,1)
3
F(0,1,0,1)
5
F(1,1,0,1)
8
F(0,0,1,1)
9
F(1,0,1,1)
7
F(0,1,1,1)
9
F(1,1,1,1)
3

Extend

Lagrange polynomials / Reed-Solomon extension



$$(0,3), (1,1), (2,4), (3,1) - - - - > (4, -19), (5, -67), (6, -154), (7, -291)$$

Extend

The commitment is the root of the Merkle tree of the columns

Lagrange polynomials / Reed-Solomon extension

3	1	4	1		-19	-67	-154	-291
5	9	2	6	$\longrightarrow$	43	135	304	572
5	3	5	8	Extend	9	5	-7	-30
9	7	9	3		-23	-81	-183	-341

$$(0{,}3), (1{,}1), (2{,}4), (3{,}1) - - - - > (4, -19), (5, -67), (6, -154), (7, -291)$$

Extend

Lagrange polynomials / Reed-Solomon extension

Given $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, the Lagrange interpolating polynomial is:

$$L(x) = \sum_{j=0}^{n} y_j l_j(x), \text{ where } l_j(x) = \prod_{\substack{0 \leqslant m \leqslant n \\ m \neq j}} \frac{x - x_m}{x_j - x_m}$$

Extend

Lagrange polynomials / Reed-Solomon extension

Given $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, the Lagrange interpolating polynomial is:

$$L(x) = \sum_{j=0}^{n} y_j l_j(x), \text{ where } l_j(x) = \prod_{\substack{0 \leqslant m \leqslant n \\ m \neq j}} \frac{x - x_m}{x_j - x_m}$$

Barycentric form:

$$L(x) = l(x) \sum_{j=0}^{n} \frac{w_j}{x - x_j} y_j, \text{ where}$$

$$l(x) = \prod_{0 \leqslant m \leqslant n} (x - x_m) \ \& \ w_j(x) = \prod_{\substack{0 \leqslant m \leqslant n \\ m \neq j}} \frac{1}{x_j - x_m}$$

Extend

Lagrange polynomials / Reed-Solomon extension

Given $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, the Lagrange interpolating polynomial is:

$$L(x) = \sum_{j=0}^{n} y_j l_j(x), \text{ where } l_j(x) = \prod_{\substack{0 \leqslant m \leqslant n \\ m \neq j}} \frac{x - x_m}{x_j - x_m}$$

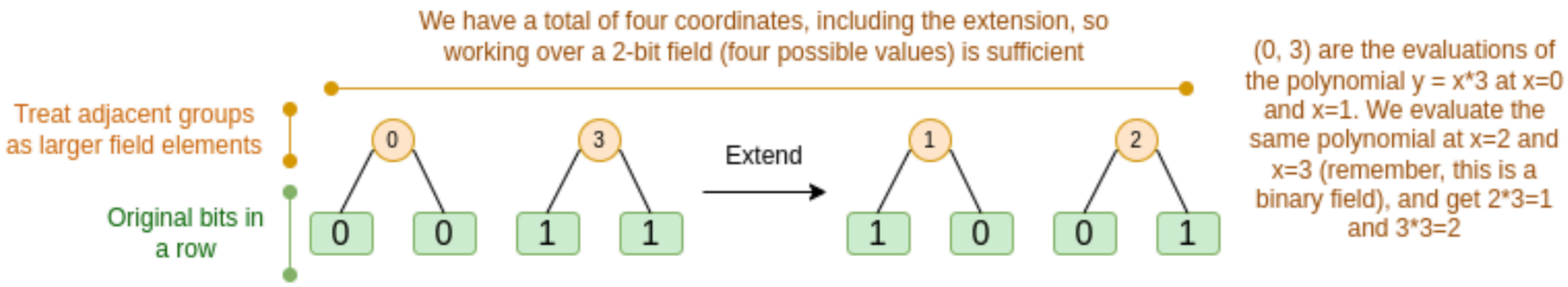
Barycentric form:

$$L(x) = l(x) \sum_{j=0}^{n} \frac{w_j}{x - x_j} y_j, \text{ where}$$

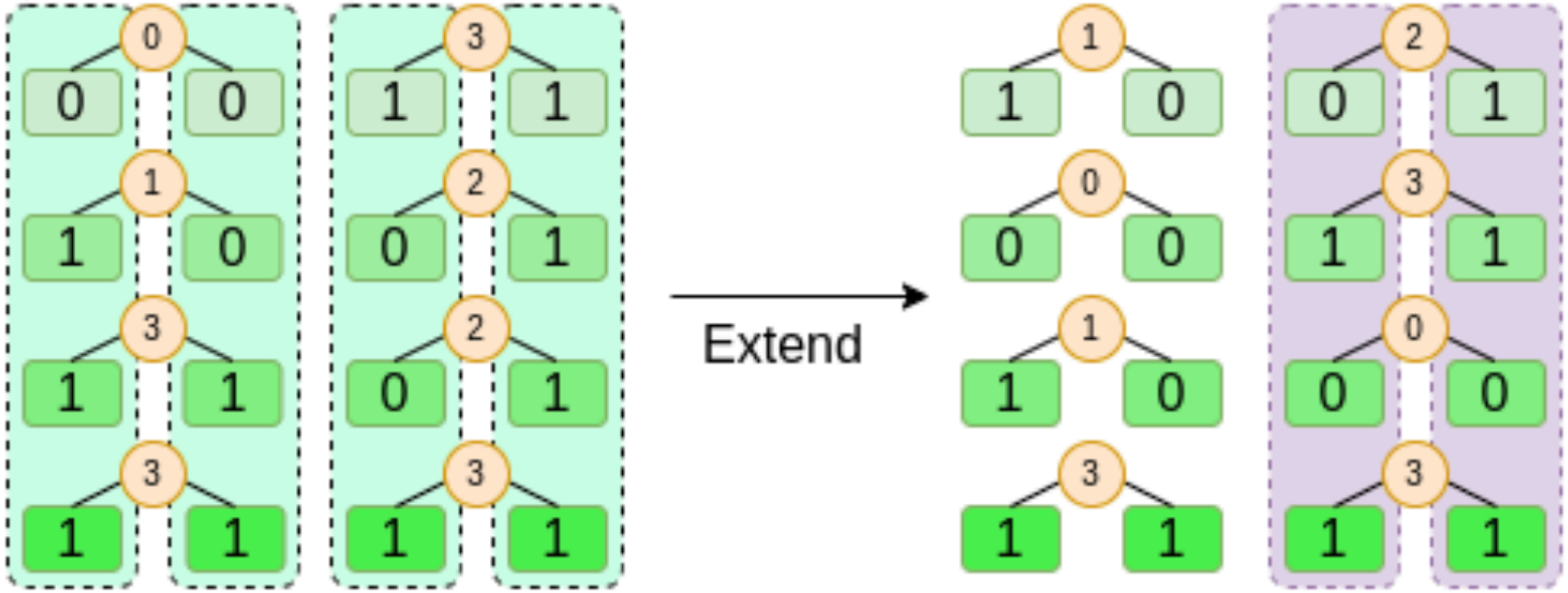
$$l(x) = \prod_{0 \leqslant m \leqslant n} (x - x_m) \ \& \ w_j(x) = \prod_{\substack{0 \leqslant m \leqslant n \\ m \neq j}} \frac{1}{x_j - x_m}$$

A limitation - if you are extending n values to kn values, you need to be working in a field that has kn different values that you can use as coordinates.

Extend - binary fields

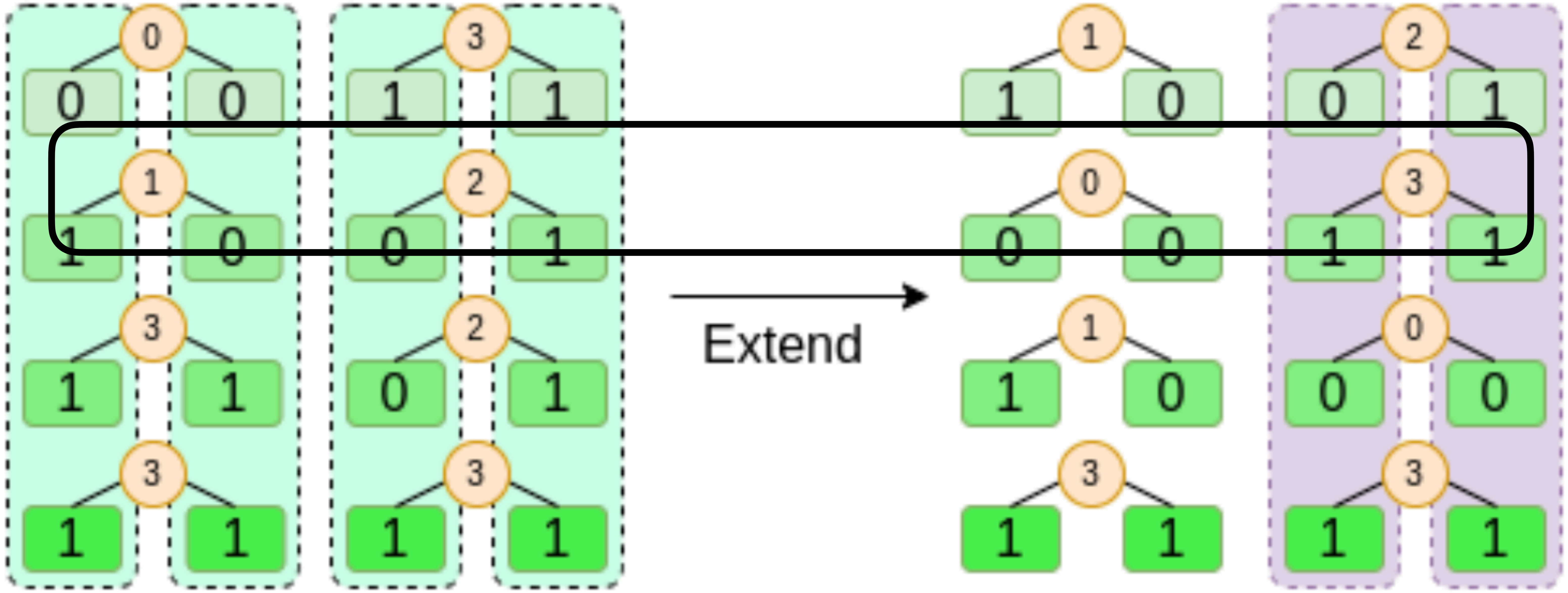


Extend - binary fields



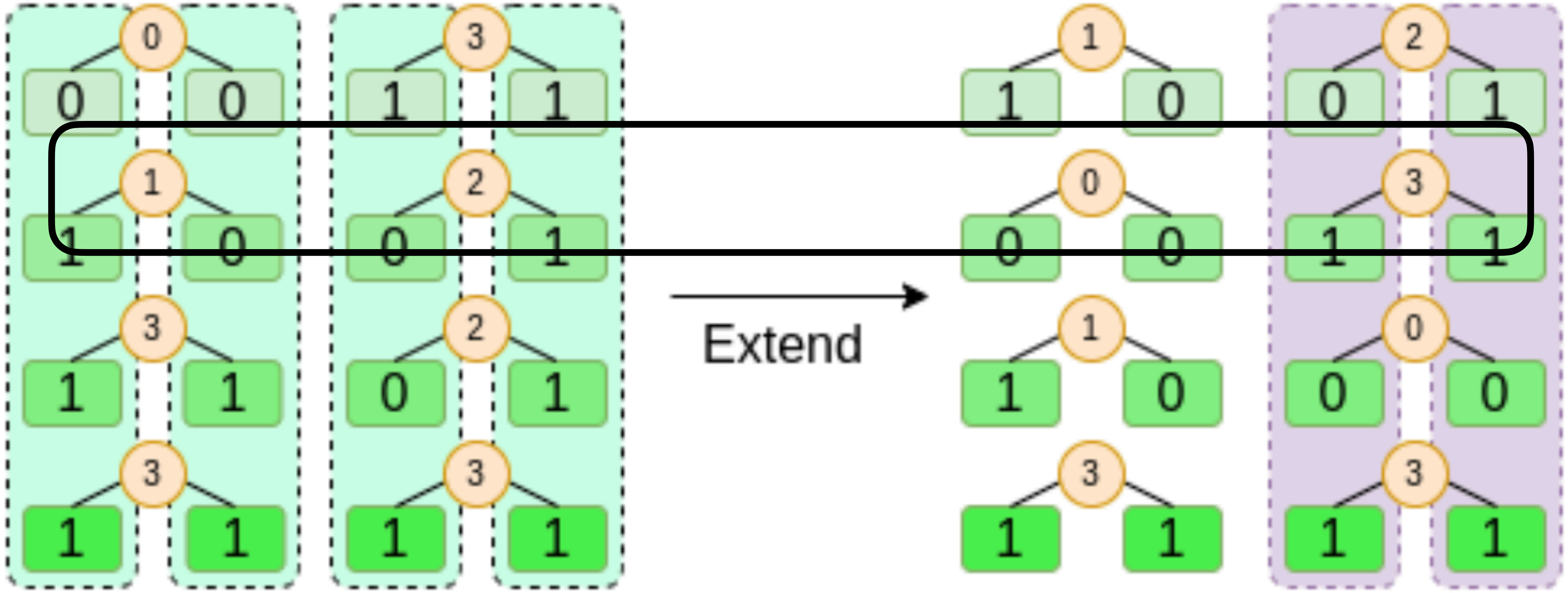
Extend - binary fields

(0,1), (1,2) – – – – > (2,0), (3,3)



Extend - binary fields

(0,1), (1,2) – – – – – > (2,0), (3,3)



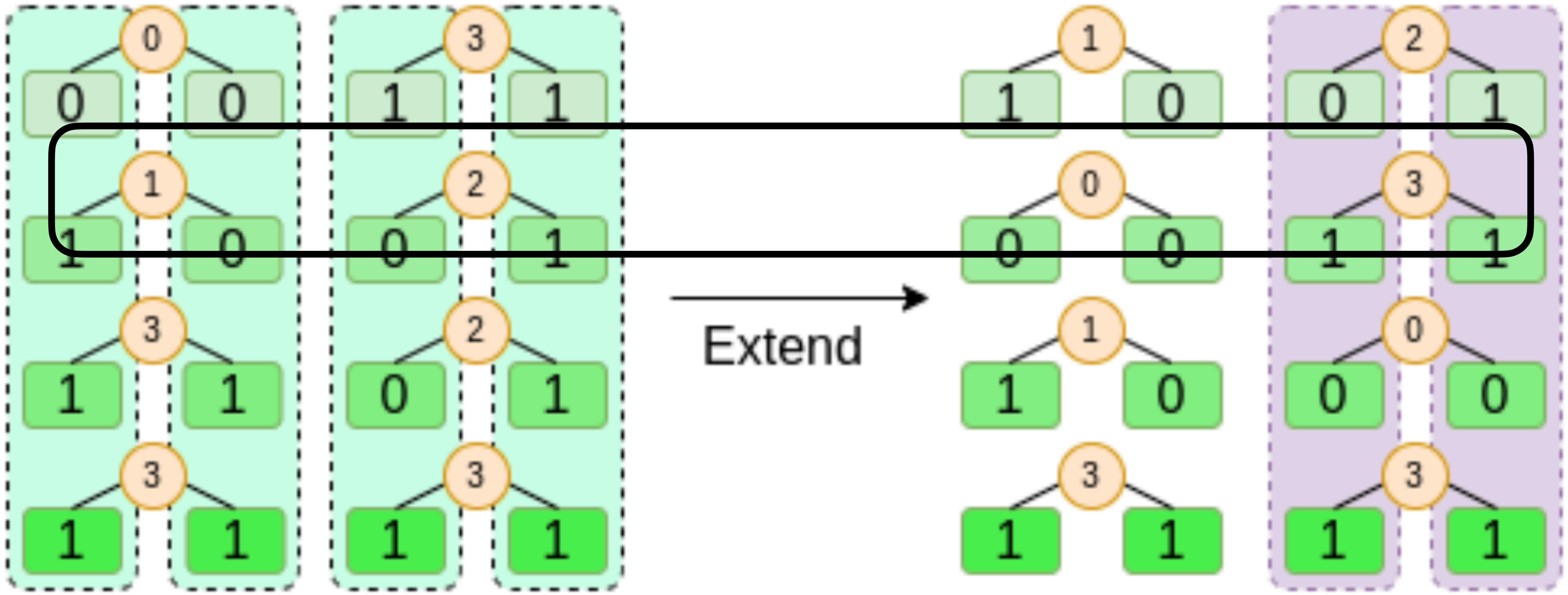
+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$$L(x) = l(x)\sum_{j=0}^{n}\frac{w_j}{x-x_j}y_j, \text{ where } l(x) = \prod_{0\leqslant m\leqslant n}(x-x_m) \;\&\; w_j(x) = \prod_{\substack{0\leqslant m\leqslant n\\ m\neq j}}\frac{1}{x_j-x_m}$$

Extend - binary fields

$(0,1), (1,2) ----> (2,0), (3,3)$



+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

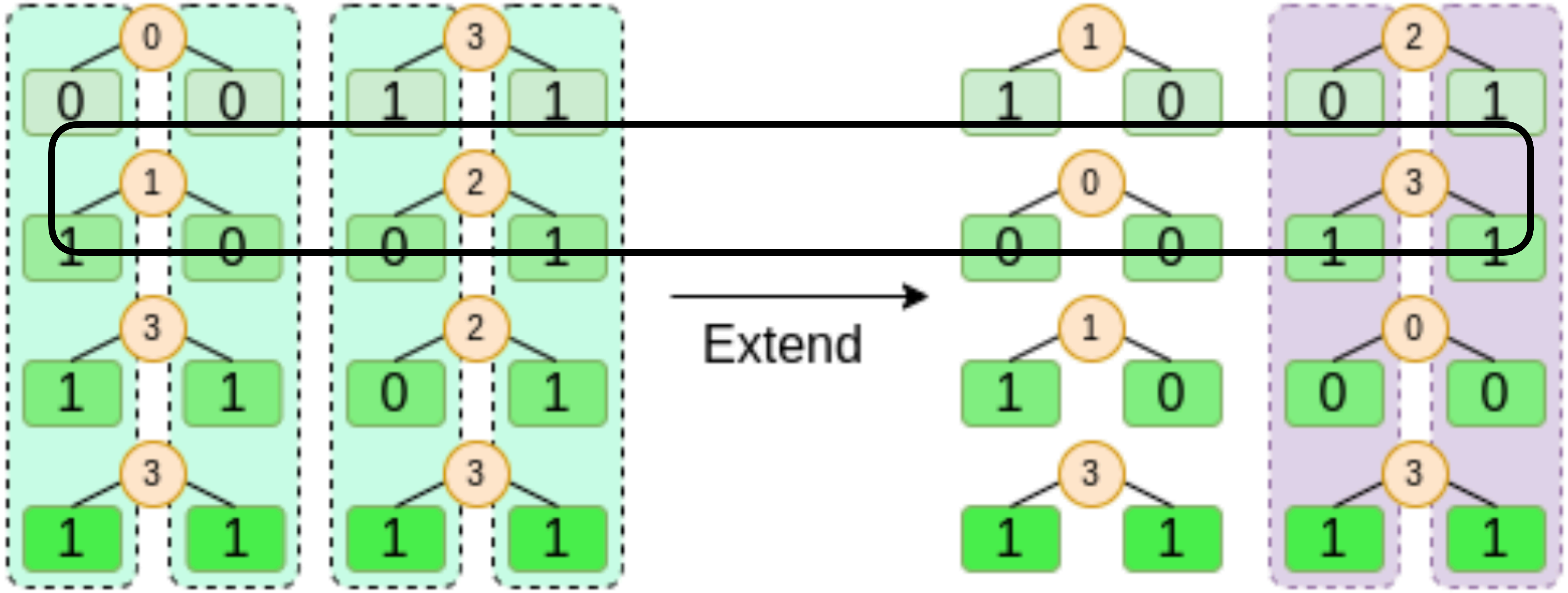
*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$$L(x) = l(x)\sum_{j=0}^{n} \frac{w_j}{x - x_j} y_j, \text{ where } l(x) = \prod_{0 \leqslant m \leqslant n} (x - x_m) \;\&\; w_j(x) = \prod_{\substack{0 \leqslant m \leqslant n \\ m \neq j}} \frac{1}{x_j - x_m}$$

$$\Rightarrow \quad l(x) = x(x-1), w_0 = \frac{1}{0-1} = 1, w_1 = \frac{1}{1-0} = 1$$

Extend - binary fields

$(0,1),(1,2) - - - - > (2,0),(3,3)$



+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

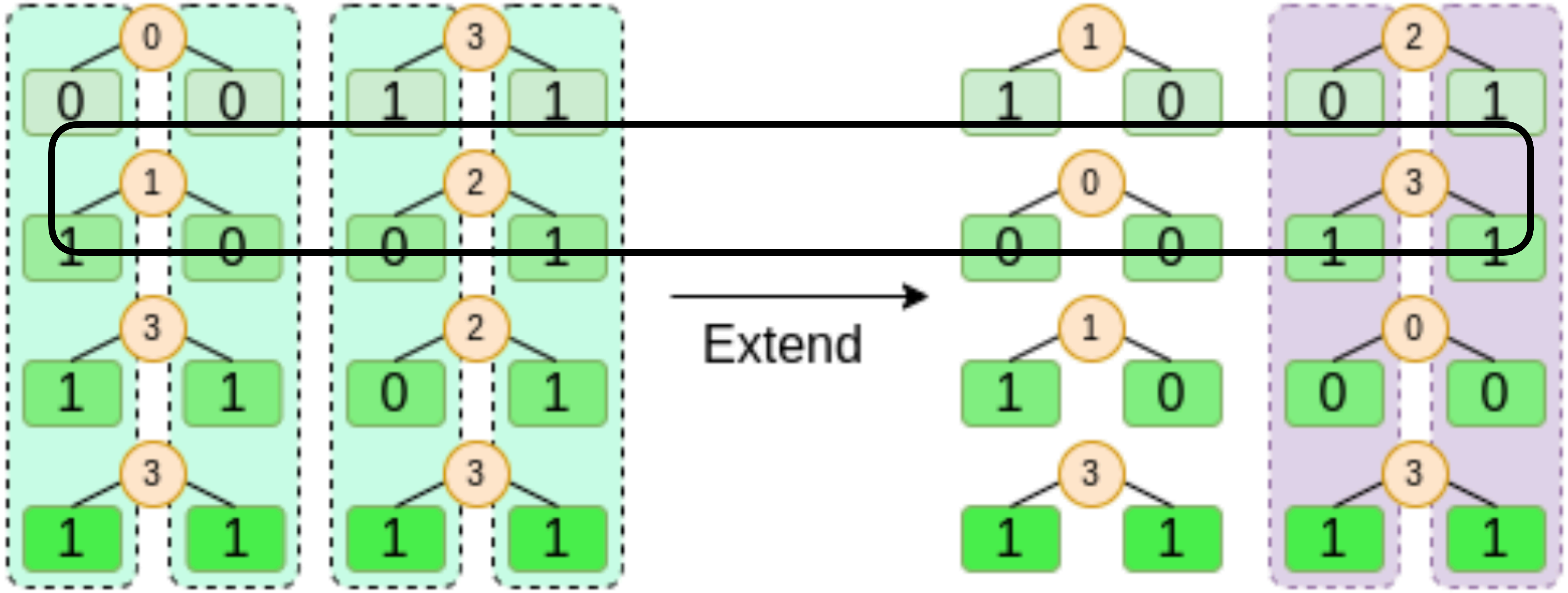
$$L(x) = l(x)\sum_{j=0}^{n}\frac{w_j}{x-x_j}y_j, \text{ where } l(x) = \prod_{0\leqslant m\leqslant n}(x-x_m) \ \& \ w_j(x) = \prod_{\substack{0\leqslant m\leqslant n \\ m\neq j}}\frac{1}{x_j-x_m}$$

$$\Rightarrow \quad l(x) = x(x-1), w_0 = \frac{1}{0-1} = 1, w_1 = \frac{1}{1-0} = 1$$

$$\Rightarrow \quad L(x) = x(x-1)\left[\frac{1\cdot 1}{x} + \frac{1\cdot 2}{x-1}\right] = (x-1) + 2x = -1 + (1+2)x = 1 + 3x$$

Extend - binary fields

$(0,1), (1,2) - - - - > (2,0), (3,3)$



+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$$L(x) = l(x)\sum_{j=0}^{n} \frac{w_j}{x-x_j} y_j, \text{ where } l(x) = \prod_{0\leqslant m\leqslant n}(x-x_m) \ \&\ w_j(x) = \prod_{\substack{0\leqslant m\leqslant n\\ m\neq j}} \frac{1}{x_j-x_m}$$

$$\rightarrow \quad l(x) = x(x-1), w_0 = \frac{1}{0-1} = 1, w_1 = \frac{1}{1-0} = 1$$

$$\rightarrow \quad L(x) = x(x-1)\left[\frac{1\cdot 1}{x} + \frac{1\cdot 2}{x-1}\right] = (x-1) + 2x = -1 + (1+2)x = 1 + 3x$$

$$\rightarrow \quad L(2) = 0, L(3) = 3$$

Compute row combination

In the evaluation point $(r_o, r_1, r_2, r_3) = (2,0,3,4)$

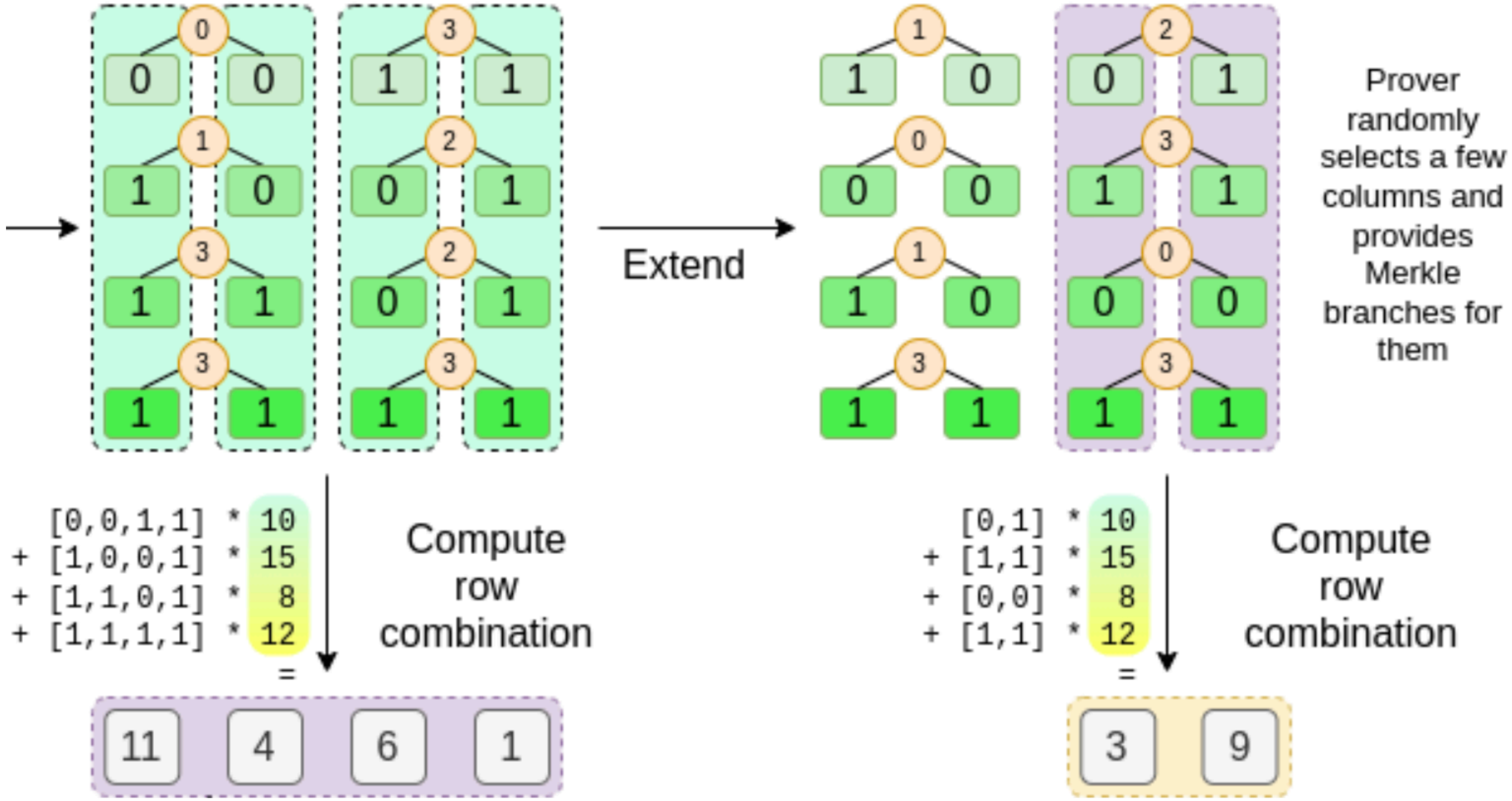
$$\otimes_{i=2,3}(1-r_i, r_i) = [(1-r_2)\cdot(1-r_3), r_2\cdot(1-r_3), (1-r_2)\cdot r_3, r_2\cdot r_3] = [(1-3)\cdot(1-4), 3\cdot(1-4), (1-3)\cdot 4, 3\cdot 4]$$

$$= [2\cdot 5, 3\cdot 5, 2\cdot 4, 3\cdot 4] = [10,15,8,12]$$

Compute row combination

In the evaluation point $(r_o, r_1, r_2, r_3) = (2,0,3,4)$

$$\otimes_{i=2,3}(1-r_i, r_i) = [(1-r_2)\cdot(1-r_3), r_2\cdot(1-r_3), (1-r_2)\cdot r_3, r_2\cdot r_3] = [(1-3)\cdot(1-4), 3\cdot(1-4), (1-3)\cdot 4, 3\cdot 4]$$
$$= [2\cdot 5, 3\cdot 5, 2\cdot 4, 3\cdot 4] = [10,15,8,12]$$

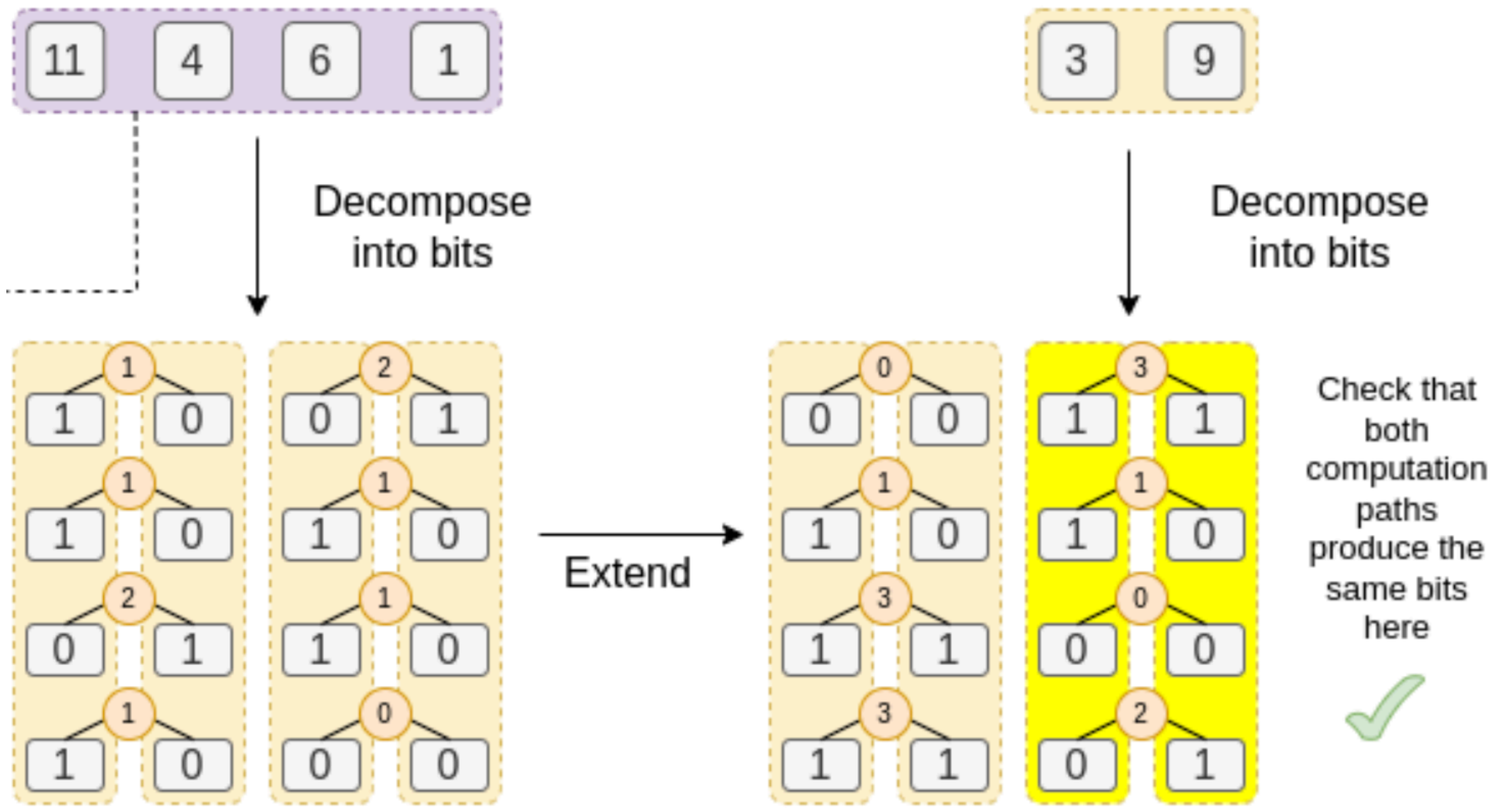


The linearity of the extension

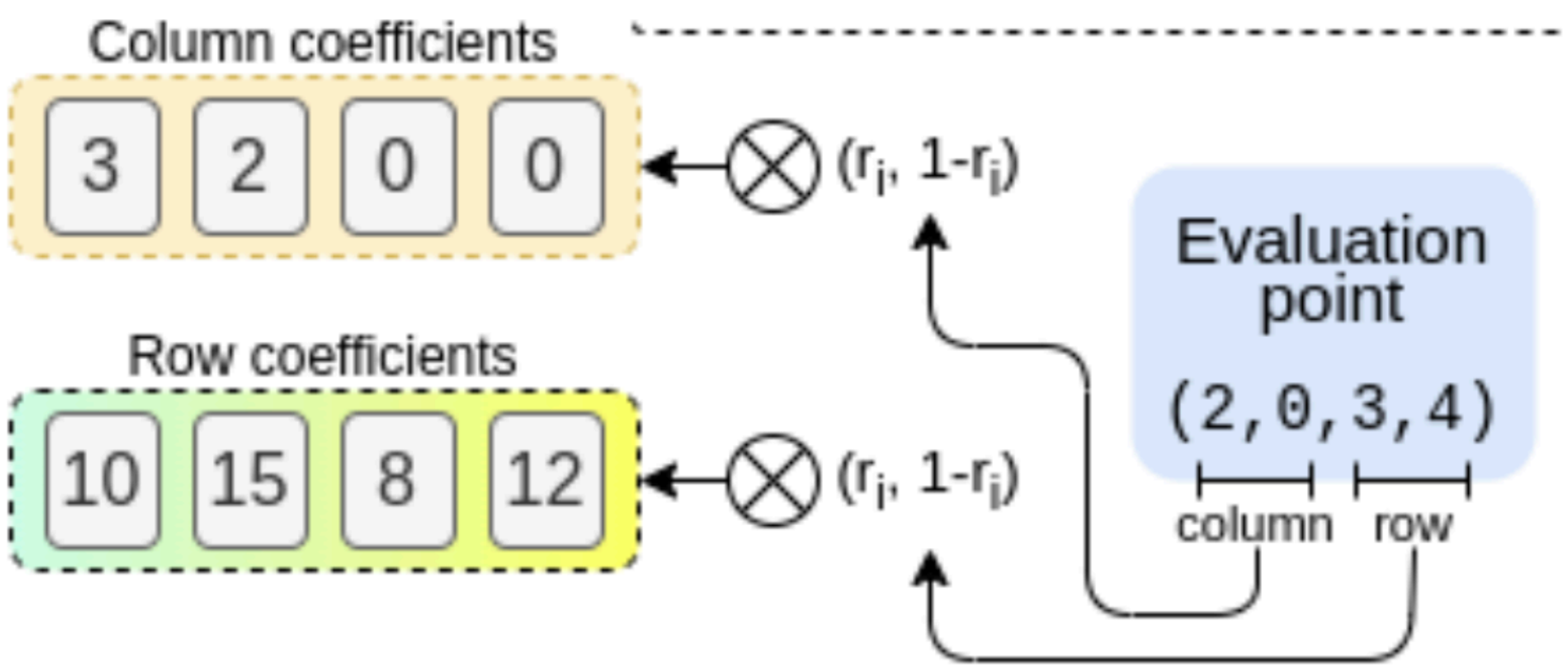
A linear combination of the extension = the extension of a linear combination

The linearity of the extension

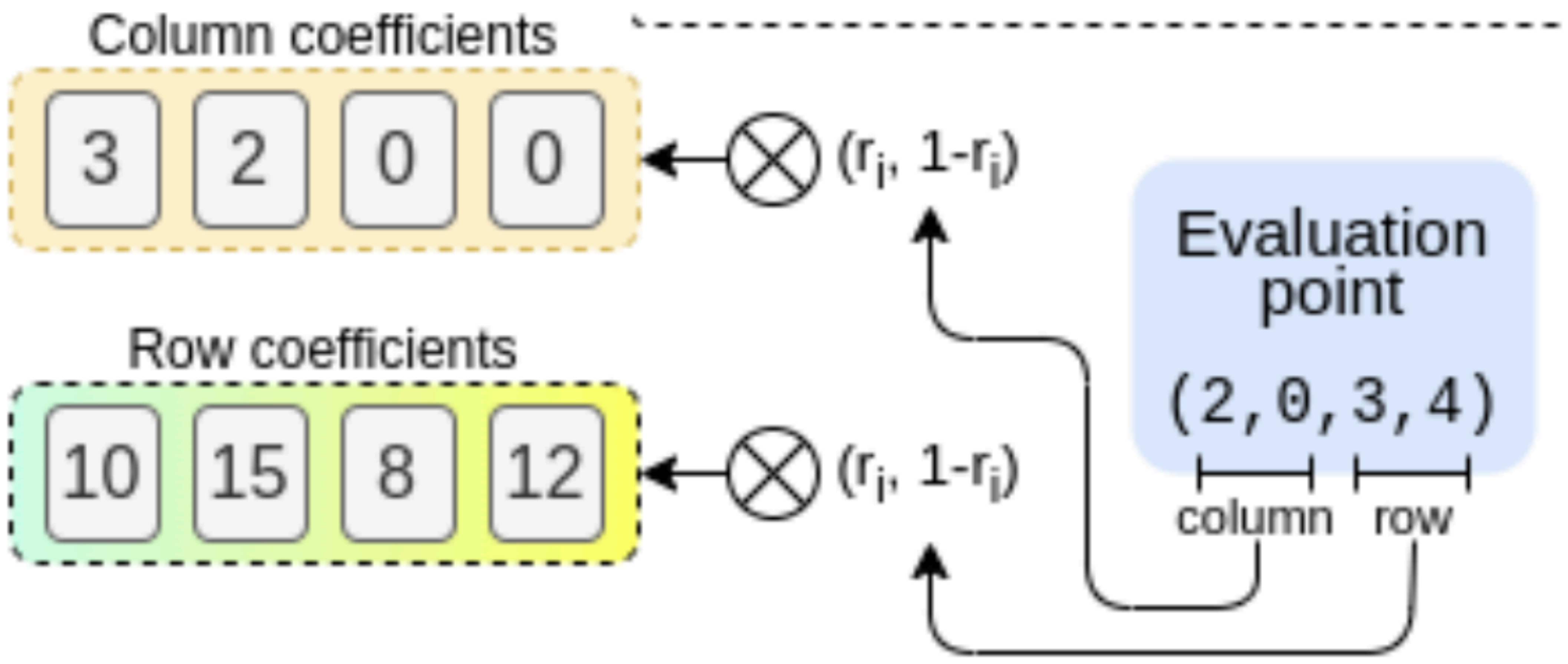
A linear combination of the extension = the extension of a linear combination



Checking the answer 14



Checking the answer 14



$$3 * 11 + 2 * 4 + 0 * 6 + 0 * 1 = \boxed{14}$$