Modulo-$(2^n + 3)$ Parallel Prefix Addition via Diminished-3 Representation of Residues

Authors: Ghassem Jaberipur, Sahar Moradi Cherati

Arith 26

Kindly presented by: Paulo Sérgio Alves Martins

Contents

INTRODUCTION

- Residue number systems (RNS)
  - $\mathcal{R} = \{m_1, m_2 \ldots m_k\}$, $m_i (1 \le i \le k)$
  - $M = \prod_{i=1}^{k} m_i$
- Applications
  - Cryptography
  - digital signal/image processing
- RNS Features
  - High Speed
  - Low Power

$X, Y \in \mathcal{R}$
$X = (x_1, x_2 \ldots, x_k), Y = (y_1, y_2 \ldots, y_k),$
where $x_i = |X|_{m_i}, \; y_i = |Y|_{m_i}$
$Z = X \circledast Y$, $z_i = x_i \circledast y_i$, where $\circledast \in \{+, -, \times\}$

- Popular $\tau = \{2^n - 1, 2^n, 2^n + 1\}$
- General form: $2^n \pm \delta (1 \le \delta < 2^{n-1})$

Parallel prefix modulo-$(2^n - \delta)$ adders:

- $\delta = 1$
- $\delta = 3$ [Jaberipur,2015]
- $\delta = 2^q + 1$ [Langroudi,2015]

Delay
$(3 + 2 \log n)\Delta$
$(4 + 2 \log n)\Delta$
$(5 + 2 \log n)\Delta$

- $2^n + \delta = 2^{n+1} - \delta'$

, where $1 < \delta' = 2^n - \delta < 2^n$

No direct fast solution

DIMINISHED-1 ADDERS

Diminished-1 encoding

X: A modulo-$(2^n + 1)$ residue $\in [0, 2^n]$
$X = X' + z_X$, where $X' = X - 1 \in [0, 2^n - 1]$ for $X > 0$
$z_X = 0(1)$, if and only if $X = 0(> 0)$

$z_S = (z_A \vee z_B) \wedge \overline{z_A z_B \wedge \xi}$
$S' = |A' + B' + z_A + z_B - z_S|_{2^n+1}$
$= \left|\widehat{W}' + z_A z_B \overline{w_n'}\right|_{2^n}$

$w_n' = G_{n-1:0}$
$\xi = P_{n-1:0}\overline{G_{n-1:0}} = 1$, Iff $A' + B' = 2^n - 1$

Diminished-1 addition

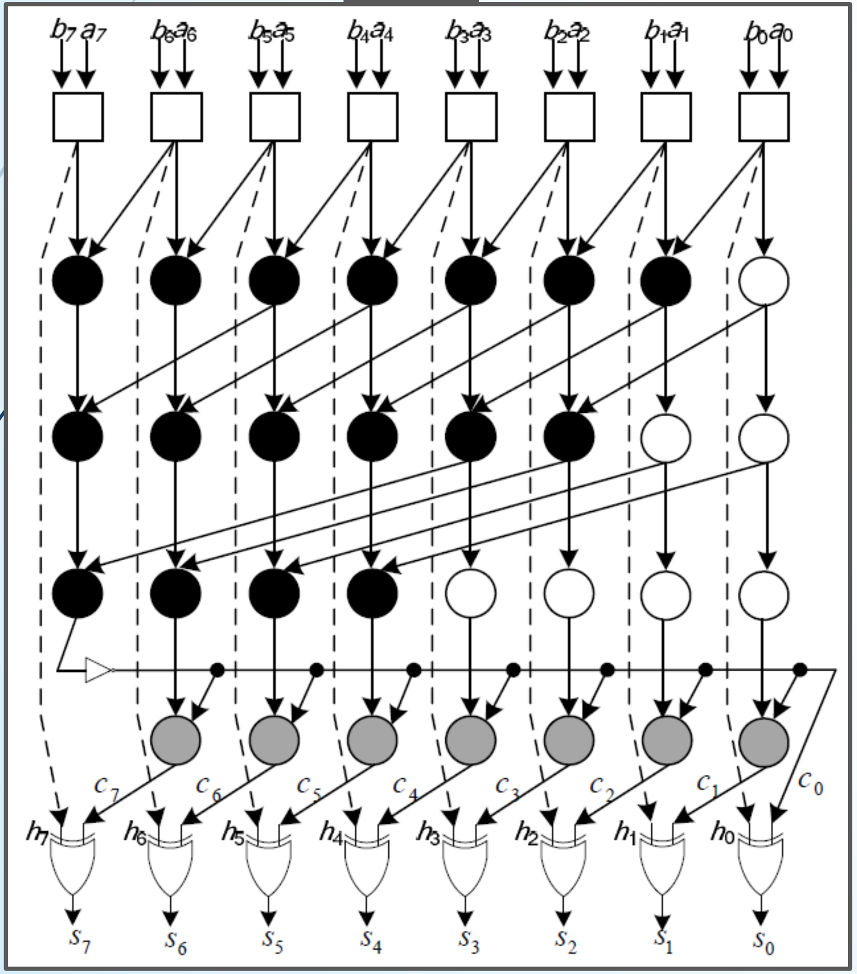
$S = |A + B|_{2^n+1} = S' + z_S$, $A = A' + z_A$, $B = B' + z_B$
$S' = S - 1$, $A' = A - 1$, $B' = B - 1$ for $S, A, B > 0$
z_S, z_A, z_B: zero-indicator bits

$A' + B' = 2^n w_n' + \widehat{W}'$, where $\widehat{W}' = w_{n-1}' \ldots w_0'$

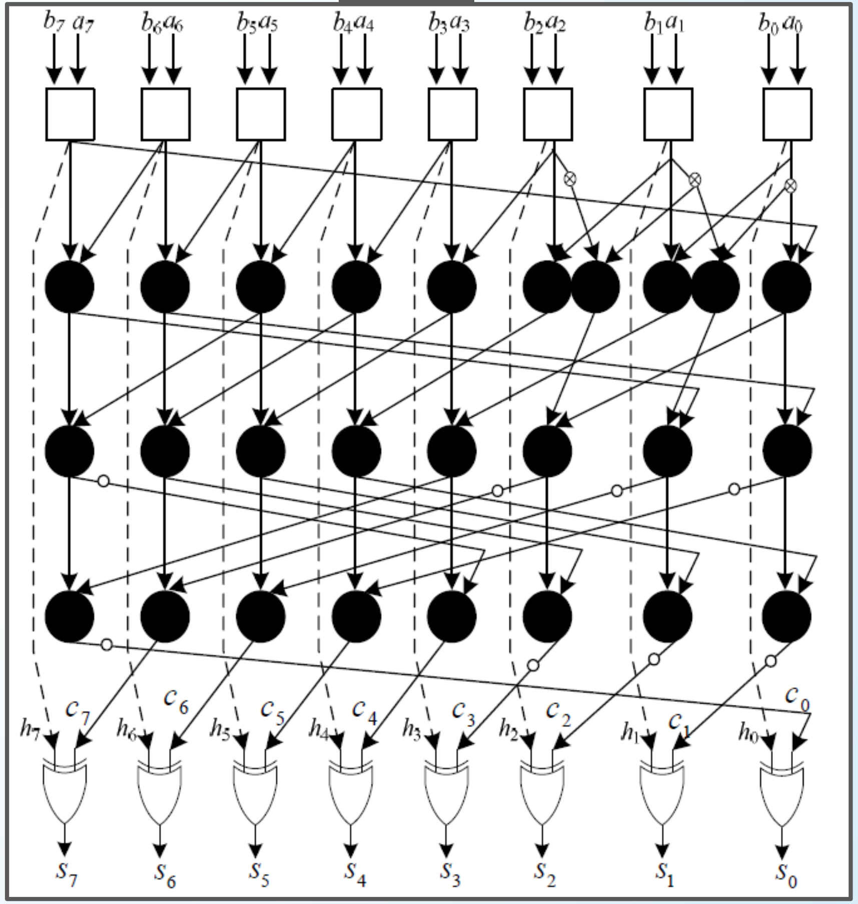
$S' = S - 1 = |A + B|_{2^n+1} - 1$
$= |A' + 1 + B' + 1 - 1|_{2^n+1} = \left|2^n w_n' + \widehat{W}' + 1\right|_{2^n+1}$
$= \left|\widehat{W}' + 1 - w_n'\right|_{2^n+1} = \widehat{W}' + \overline{w'_n}$

Related Work: Modulo-$(2^n + 1)$ D1 adder

RPP



TPP



DIMINISHED-3 REPRESENTATION AND ADDITION

DIMINISHED-3 REPRESENTATION

X: **Modulo**$-(2^n+3)$ **residue** $\in [0, 2^n+2]$

- $\{0, 1, 2\}$
- $[3, 2^n+2]$

D3 Representation

$T_X \in \{0, 1, 2\}$-indicator	$T_X = t_1 t_0$	$X = X' + T_X$
$X' \in [0, 2^n-1]$	X' : n bit	

$T_X = 0 \Leftrightarrow X = 0, X' = 0$
$T_X = 1 \Leftrightarrow X = 1, X' = 0$
$T_X = 2 \Leftrightarrow X = 2, X' = 0$
$T_X = 3 \Leftrightarrow 3 \leq X \leq 2^n+2, X' \in [0, 2^n-1]$

Modulo-(2^n+3) D3 ADDITION

$A \in [0, 2^n+2]$	$A = A' + T_A$
$B \in [0, 2^n+2]$	$B = B' + T_B$

$A' =$	$\boldsymbol{a_{n-1}}$	$\dots$	$\boldsymbol{a_2}$	$\boldsymbol{a_1}$	$\boldsymbol{a_0}$
$B' =$	$\boldsymbol{b_{n-1}}$	$\dots$	$\boldsymbol{b_2}$	$\boldsymbol{b_1}$	$\boldsymbol{b_0}$
w'_n	w'_{n-1}	$\dots$	w'_2	w'_1	w'_0

$A, B, S \geq 3$

$S' = S - 3 = |A+B|_{2^n+3} - 3$

$= |A' + 3 + B' + 3 - 3|_{2^n+3} = \left|2^n w'_n + \widehat{W'} + 3\right|_{2^n+3}$

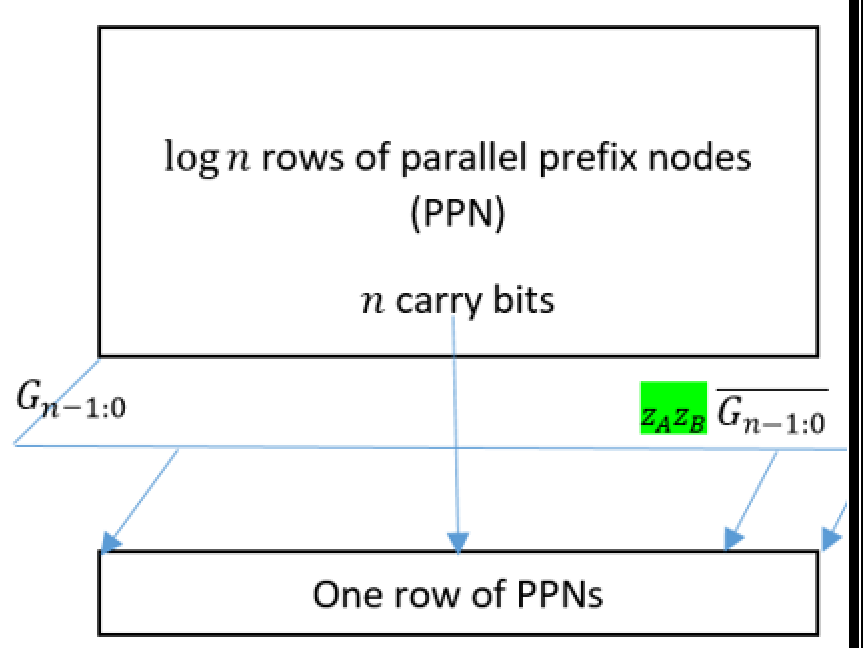
$= \left|\widehat{W'} + 3(1 - w'_n)\right|_{2^n+3} = \widehat{W'} + 3\overline{w'_n}$

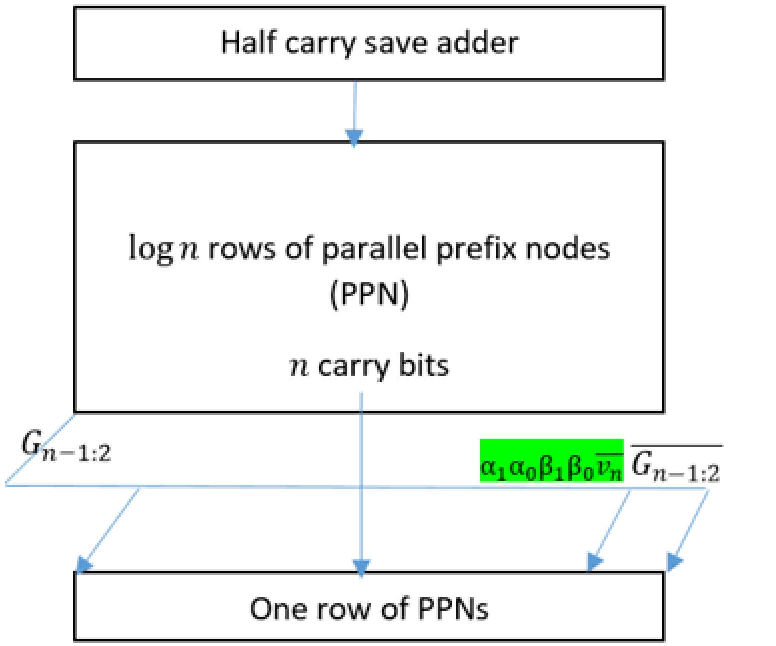
Comparison D1 and D3

$(3 + 2\,log\,n)\Delta$

$(5 + 2\,log\,n)\Delta$

Diminished-1 Adder		Diminished-3 Adder	
$A = A' + z_A,\quad B = B' + z_B,$ $S = \lvert A + B \rvert_{2^n+1} = S' + z_S$		$A = A' + \alpha_1\alpha_0,\quad B = B' + \beta_1\beta_0,$ $S = \lvert A + B \rvert_{2^n+3} = S' + T_S$	
$z_S = (z_A \vee z_B) \wedge \overline{z_A z_B \wedge \xi}$	$S' = \lvert A' + B' + z_A z_B \overline{G_{n-1:0}} \rvert_{2^n}$	$T_S = 2\sigma_1 + \sigma_0$	$S' = \lvert A' + B' + \alpha_1\alpha_0\beta_1\beta_0\overline{v_n}\,\overline{G_{n-1:2}} + \delta' \rvert_{2^n}$
$\xi = P_{n-1:0}\overline{G_{n-1:0}}$		$\sigma_1 = (\alpha_1\beta_1 \vee \alpha_0\beta_0)P_{n-1:2}\overline{G_{n-1:2}} \vee f_1(\alpha_1, \beta_1, \alpha_0, \beta_0, u_1, v_1, u_0)$	$\sigma_0 = (\alpha_1\beta_0 \vee \alpha_0\beta_1)P_{n-1:2}\overline{G_{n-1:2}} \vee f_0(\alpha_1, \beta_1, \alpha_0, \beta_0, u_1, v_1, u_0)$





Detect Special Cases

$$S = |A+B|_{2^n+3} \in \{0,1,2\}$$

IF $A' + B' = 2^n - 1$ THEN $\xi_1 = 1$ ELSE $\xi_1 = 0$

IF $A' + B' = 2^n - 2$ THEN $\xi_2 = 1$ ELSE $\xi_2 = 0$

IF $A' + B' = 2^n - 3$ THEN $\xi_3 = 1$ ELSE $\xi_3 = 0$

$D1$

$$S = |A+B|_{2^n+1} = 0$$

IF $A' + B' = 2^n - 1$ THEN $\xi = 1$ ELSE $\xi = 0$

A'		a_{n-1}	…	a_2	a_1	a_0
B'		b_{n-1}	…	b_2	b_1	b_0
U		u_{n-1}	…	u_2	u_1	u_0
V	v_n	v_{n-1}	…	v_2	v_1	
2^n-1	0	1	…	1	1	1

$\xi_1 = P_{n-1:2}\overline{G_{n-1:2}}h_1u_0$

	a_{n-1}	…	a_2	a_1	a_0
	b_{n-1}	…	b_2	b_1	b_0
	u_{n-1}	…	u_2	u_1	u_0
v_n	v_{n-1}	…	v_2	v_1	1
0	1	…	1	1	1

$\xi_2 = P_{n-1:2}\overline{G_{n-1:2}}h_1\overline{u_0}$

	a_{n-1}	…	a_2	a_1	a_0
	b_{n-1}	…	b_2	b_1	b_0
	u_{n-1}	…	u_2	u_1	u_0
v_n	v_{n-1}	…	v_2	v_1	
				1	
0	1	…	1	1	1

$\xi_3 = P_{n-1:2}\overline{G_{n-1:2}}\overline{u_1}u_0$

DERIVATION OF T_S

T_B \ T_A	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	$3\overline{\xi_1}$
2	2	3	3	$\xi_1 + 3\,\overline{\xi_1}\,\overline{\xi_2}$
3	3	$3\overline{\xi_1}$	$\xi_1 + 3\overline{\xi_1}\,\overline{\xi_2}$	$2\xi_1 + \xi_2 + 3\,\overline{\xi_1}\,\overline{\xi_2}\,\overline{\xi_3}$

a: $T_S \in \{0,1,2,3\}$

$\alpha_1\alpha_0 \downarrow$	$\beta_1\beta_0 \rightarrow$	**00**	**01**	**11**	**10**
00		0,0	0,1	1,1	1,0
01		0,1	1,0	$\overline{\xi_1}, \overline{\xi_1}$	1,1
11		1,1	$\overline{\xi_1}, \overline{\xi_1}$	$\xi_1 \vee \overline{\xi_2}\,\overline{\xi_3}, \xi_2 \vee \overline{\xi_1}\,\overline{\xi_3}$	$\overline{\xi_1}\,\overline{\xi_2}, \overline{\xi_2}$
10		1,0	1,1	$\overline{\xi_1}\,\overline{\xi_2}, \overline{\xi_2}$	1,1

b: $\sigma_1\sigma_0 \in \{00,01,11,10\}$

$$\mathcal{K} = P_{n-1:2}\overline{G_{n-1:2}}, \quad \xi_1 = \mathcal{K}h_1u_0, \quad \xi_2 = \mathcal{K}h_1\overline{u_0}, \quad \xi_3 = \mathcal{K}\overline{u_1}u_0$$

- $\sigma_1 = (\alpha_1\beta_1 \vee \alpha_0\beta_0)\overline{\mathcal{K}} \vee f_1(\alpha_1, \beta_1, \alpha_0, \beta_0, u_1, v_1, u_0)$
- $\sigma_0 = (\alpha_1\beta_0 \vee \alpha_0\beta_1)\overline{\mathcal{K}} \vee f_0(\alpha_1, \beta_1, \alpha_0, \beta_0, u_1, v_1, u_0)$

Impact of ξ-dependent noise terms on T_S

T_A	T_B	ξ_1	ξ_2	ξ_3	T_S	S	Justification
3	0	X	X	X	3	≥ 3	$S = A + B = A \leq 2^n + 2$
$T_S = 3$							

T_A	T_B	ξ_1	ξ_2	ξ_3	T_S	S	Justification
3	1	0	X	X	3	≥ 4	$A' + B' = A' < 2^n - 1 \Longrightarrow S = A + B = A' + 3 + 1 < 2^n + 3$
3	1	1	X	X	0	0	$A' + B' = 2^n - 1 \Longrightarrow A + B = 2^n + 3, S = \lvert A + B \rvert_{2^n+3} = 0$
$T_S = 3\overline{\xi_1}$							

T_A	T_B	ξ_1	ξ_2	ξ_3	T_S	S	Justification
3	2	0	0	X	3	≥ 5	$A' + B' = A' < 2^n - 2 \Longrightarrow S = A + B = A' + 3 + 2 < 2^n + 3$
3	2	0	1	X	0	0	$A' + B' = 2^n - 2 \Longrightarrow A + B = 2^n + 3, S = \lvert A + B \rvert_{2^n+3} = 0$
3	2	1	0	X	1	1	$A' + B' = 2^n - 1 \Longrightarrow A + B = 2^n + 4, S = \lvert A + B \rvert_{2^n+3} = 1$
$T_S = \xi_1 + 3\,\overline{\xi_1}\,\overline{\xi_2}$							

T_A	T_B	ξ_1	ξ_2	ξ_3	T_S	S	Justification
3	3	0	0	0	3	≥ 6	$A' + B' < 2^n - 3 \Longrightarrow S = A + B = A' + B' + 6 < 2^n + 3$
3	3	0	0	0	3	≥ 3	$2^n \leq A' + B' \leq 2^n + 2^n - 2 \Longrightarrow 3 \leq S = \lvert A + B \rvert_{2^n+3} \leq 2^n + 1$
3	3	0	0	1	0	0	$A' + B' = 2^n - 3 \Longrightarrow A + B = 2^n + 3, S = \lvert A + B \rvert_{2^n+3} = 0$
3	3	0	1	0	1	1	$A' + B' = 2^n - 2 \Longrightarrow A + B = 2^n + 4, S = \lvert A + B \rvert_{2^n+3} = 1$
3	3	1	0	0	2	2	$A' + B' = 2^n - 1 \Longrightarrow A + B = 2^n + 5, S = \lvert A + B \rvert_{2^n+3} = 2$
$T_S = 2\xi_1 + \xi_2 + 3\,\overline{\xi_1}\,\overline{\xi_2}\,\overline{\xi_3}$							

DERIVATION OF S'

$$S' = |A' + T_A + B' + T_B - T_S|_{2^n+3} = |A' + B' + T_A + T_B - T_S|_{2^n+3}$$

$$= \left|2^n w_n' + \widehat{W}' + T\right|_{2^n+3} = \left|\widehat{W}' + T - 3w_n'\right|_{2^n+3} = \left|\widehat{W}' + \boldsymbol{\delta}'\right|_{2^n+3}, \qquad \boldsymbol{\delta}' = T - 3w_n'$$

T_B \ T_A	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	0	0	$3\xi_1 + 1$
2	0	0	1	$2\xi_1 + 3\xi_2 + 2$
3	0	$3\xi_1 + 1$	$2\xi_1 + 3\xi_2 + 2$	$\xi_1 + 2\xi_2 + 3\xi_3 + 3$

THE NOISE TERM $T = T_A + T_B - T_S$ IN TERMS OF T_A, T_B, AND ξ BITS

Compound RPP realization of S'

$$\boldsymbol{S' = \left|\widehat{W'} + z\overline{w'_n} + {\color{red}\delta'}\right|_{2^n}}$$

$$\delta' = \delta'_1\delta'_0 \in \{0,1,2\}$$

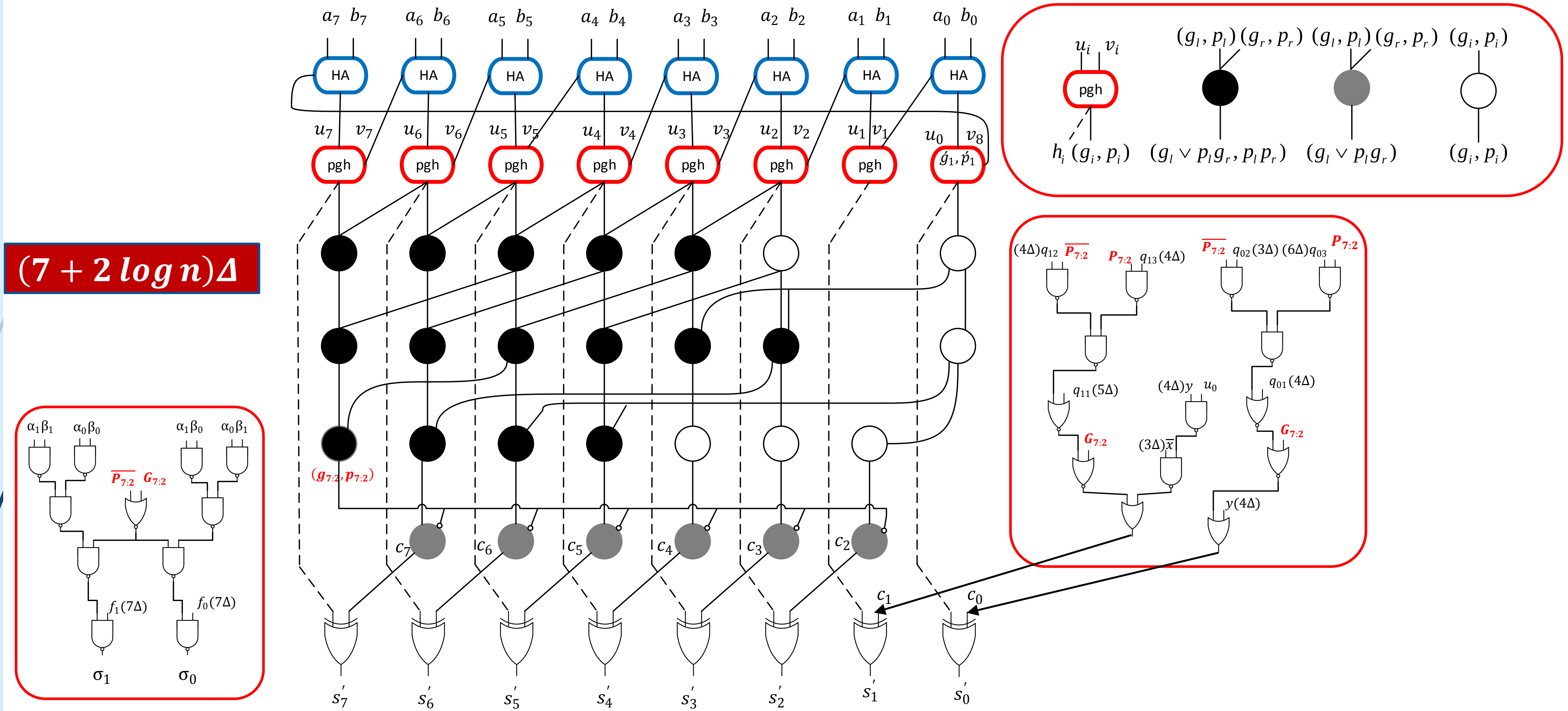
$$\delta'_1 = \bar{\xi}_1\alpha_1\beta_1(\alpha_0 \oplus \beta_0) \vee \bar{\xi}_1\,\bar{\xi}_2 z\overline{w'_n},$$

$$\delta'_0 = \xi_1 x \vee \xi_2 z \vee \alpha_0\beta_0(\alpha_1 \oplus \beta_1) \vee \alpha_1\beta_1\overline{\alpha_0 \vee \beta_0}$$

$$z = \alpha_1\beta_1\alpha_0\beta_0$$

The required RPP circuitry

$(7 + 2\,log\,n)\Delta$



Carry Bits for RPP Architecture

$$c_i = G_{i-1:2} \vee P_{i-1:2} c_2 = G_{i-1:2} \vee P_{i-1:2}\left(g_1' \vee p_1' \overline{G_{n-1:2}}\right) = G_{i-1:2} \vee P_{i-1:2}\left(g_1' \vee p_1' \overline{G_{n-1:i}}\right)$$

$$c_2 = g_1' \vee p_1' \overline{G_{7:2}}, \quad (g_1', p_1') \circ \left(\overline{G_{7:2}}, 1\right)$$

$$c_3 = g_2 \vee p_2\left(g_1' \vee p_1' \overline{G_{7:3}}\right), \quad (g_2, p_2) \circ (g_1', p_1') \circ \left(\overline{G_{7:3}}, 1\right)$$

$$c_4 = G_{3:2} \vee P_{3:2}\left(g_1' \vee p_1' \overline{G_{7:4}}\right), \quad (G, P)_{3:2} \circ (g_1', p_1') \circ \left(\overline{G_{7:4}}, 1\right)$$

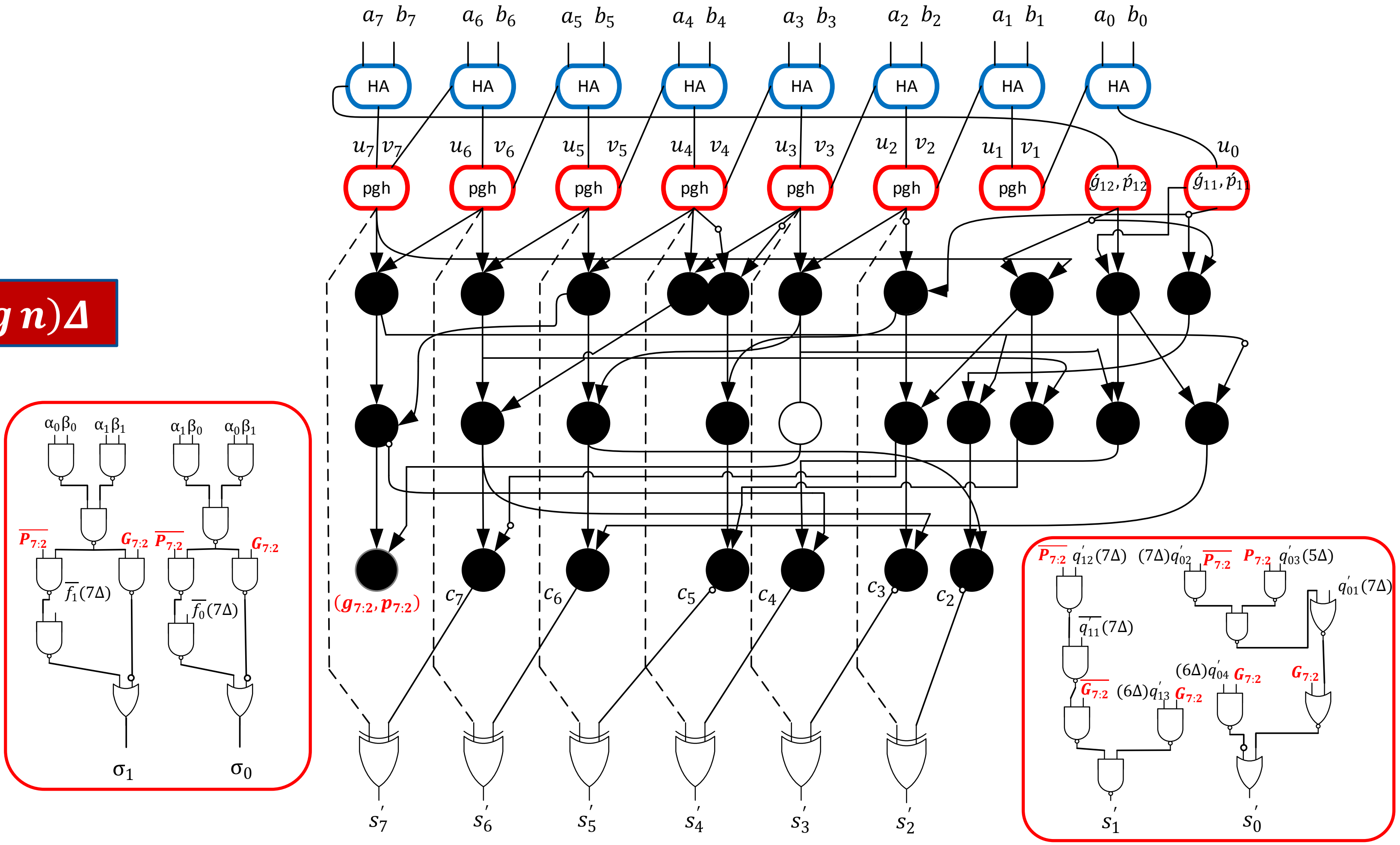
$$c_5 = G_{4:2} \vee P_{4:2}\left(g_1' \vee p_1' \overline{G_{7:5}}\right), \quad (G, P)_{4:2} \circ (g_1', p_1') \circ \left(\overline{G_{7:5}}, 1\right)$$

$$c_6 = G_{5:2} \vee P_{5:2}\left(g_1' \vee p_1' \overline{G_{7:6}}\right), \quad (G, P)_{5:2} \circ (g_1', p_1') \circ \left(\overline{G_{7:6}}, 1\right)$$

$$c_7 = G_{6:2} \vee P_{6:2}\left(g_1' \vee p_1' \overline{g_7}\right), \quad (G, P)_{6:2} \circ (g_1', p_1') \circ \left(\overline{g_7}, 1\right)$$

The required TPP circuitry

$(5 + 2\log n)\Delta$



Carry Bits for TPP Architecture

$$c_{2},\ \overline{(((\overline{p'},\overline{g'})_{11} \circ (\overline{p'},\overline{g'})_{12}) \circ ((g,p)_7 \circ (g,p)_6)) \circ (((g,p)_5 \circ (g,p)_4) \circ ((g,p)_3 \circ (g,p)_2))}$$

$$c_{3},\ \overline{(((\overline{p},\overline{g})_2 \circ (\overline{p'},\overline{g'})_{11}) \circ ((\overline{p'},\overline{g'})_{12} \circ (g,p)_7)) \circ (((g,p)_6 \circ (g,p)_5) \circ ((g,p)_4 \circ (g,p)_3))}$$

$$c_{4},\ \left(((g,p)_3 \circ (g,p)_2) \circ ((g',p')_{11} \circ (g',p')_{12})\right) \circ \overline{(((g,p)_7 \circ (g,p)_6) \circ ((g,p)_5 \circ (g,p)_4))}$$

$$c_{5},\ \overline{(((\overline{p},\overline{g})_4 \circ (\overline{p},\overline{g})_3) \circ ((\overline{p},\overline{g})_2 \circ (\overline{p'},\overline{g'})_{11})) \circ (((\overline{p'},\overline{g'})_{12} \circ (g,p)_7) \circ ((g,p)_6 \circ (g,p)_5))}$$

$$c_{6},\ (((g,p)_5 \circ (g,p)_4) \circ ((g,p)_3 \circ (g,p)_2)) \circ (((g',p')_{11} \circ (g',p')_{12}) \circ \overline{((g,p)_7 \circ (g,p)_6)})$$

$$c_{7},\ \left(((g,p)_6 \circ (g,p)_5) \circ ((g,p)_4 \circ (g,p)_3)\right) \circ \overline{(((\overline{p},\overline{g})_2 \circ (\overline{p'},\overline{g'})_{11}) \circ ((\overline{p'},\overline{g'})_{12} \circ (g_7,1)))}$$

Evaluation and comparison

RPP synthesis results

$$n = 8$$

Design(RPP)	Delay		Area		Power	
	ns	$Ratio$	μm^2	$Ratio$	mw	$Ratio$
D3	0.76	1.00	25318	1.00	0.682	1.00
D1 [1]	0.59	0.77	10128	0.40	0.328	0.48
$2^n - 3$ [2]	0.72	0.94	13227	0.52	0.467	0.68

$$n = 16$$

Design(RPP)	Delay		Area		Power	
	ns	$Ratio$	μm^2	$Ratio$	mw	$Ratio$
D3	0.81	1.00	42043	1.00	1.19	1.00
D1 [1]	0.72	0.88	23776	0.56	0.716	0.60
$2^n - 3$ [2]	0.78	0.96	30637	0.73	1.01	0.85

[1] Jaberipur,2011
[2] Jaberipur,2015

TPP Results

DELAY AND AREA MEASURES

Design(TPP)	Delay(Δ)	Area (# of gates)
D3	$(5 + 2\log n)$	$3n\,log\,n + 15n + 39$
D1 [1]	$(3 + 2\log n)$	$3n\,log\,n + 12n - 1$
$2^n - 3$ [2]	$(4 + 2\log n)$	$3n\,log\,n + 12n + 4$

SYNTHESIS RESULTS FOR $n = 8$

Design(TPP)	Delay		Area		Power	
	ns	*Ratio*	μm^2	*Ratio*	*mw*	*Ratio*
D3	0.65	1.00	30686	1.00	0.956	1.00
D1 [1]	0.57	0.88	14227	0.46	0.375	0.39
$2^n - 3$ [2]	0.64	0.98	14152	0.46	0.500	0.52

SYNTHESIS RESULTS FOR $n = 16$

Design(TPP)	Delay		Area		Power	
	ns	*Ratio*	μm^2	*Ratio*	*mw*	*Ratio*
D3	0.73	1.00	51121	1.00	1.60	1.00
D1 [1]	0.64	0.88	34441	0.67	0.939	0.59
$2^n - 3$ [2]	0.73	1.00	32712	0.64	1.081	0.67

[1] Jaberipur,2011
[2] Jaberipur,2015

Conclusions

- Implemented the required parallel prefix (RPP and TPP architectures) adders based on the novel diminished-3 representation of residues in $\{3, 2^n + 2\}$ and 2-bit $\{0,1,2\}$ indicator
- The adder delay is only 2Δ more than the modulo-$(2^n + 1)$ diminished-1 adder, and 1Δ more than that of the companion modulo-$(2^n - 3)$ adder
- Same speed (synthesis result) for the proposed designs and those of the modulo-$(2^n - 3)$ adders
- Area and Power overhead reduces as n grows larger

Thank You

jaberipur@sbu.ac.ir
saha.moradi@mail.sbu.ac.ir