

Universidade Federal de Santa Catarina

EEL7123/EEL510457

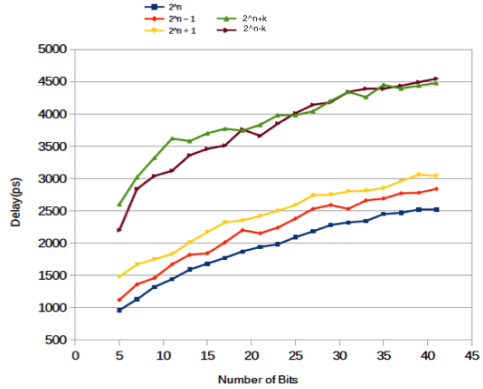
Solução Problema 4.9

Problema 4.9. Na figura seguinte se mostram os resultados de síntese em ASIC para uma tecnologia de 65nm do atraso de multiplicadores RNS e estimativas de unidades binário-RNS e RNS-binário. Caso quisermos fazer m multiplicações com uma faixa dinâmica de saída de 128-bits em serie usando a binaria e RNS:

	Moduli set	DR (bits)	Delay (ps) Bin-RNS	Delay (ps) RNS-Bin
3	$2^{43}, 2^{43}_-1, 2^{43}_+1$	129	3100	5000
4	$2^{32}, 2^{32}_-1, 2^{32}_+1, 2^{32}_-3$	128	2800	5000
5	$2^{26}, 2^{26}_-1, 2^{26}_+1, 2^{26}_-3, 2^{26}_+3$	130	2600	5000
6	$2^{22}, 2^{22}_-1, 2^{22}_+1, 2^{22}_-3, 2^{22}_+3, 2^{22}_-5$	132	2400	5000
7	$2^{19}, 2^{19}_-1, 2^{19}_+1, 2^{19}_-3, 2^{19}_+3, 2^{19}_-5, 2^{19}_+7$	133	2300	5000
8	$2^{16}, 2^{16}_-1, 2^{16}_+1, 2^{16}_-3, 2^{16}_+3, 2^{16}_-5, 2^{16}_+7, 2^{16}_+9$	128	2200	5000
9	$2^{15}, 2^{15}_-1, 2^{15}_+1, 2^{15}_-3, 2^{15}_+3, 2^{15}_-5, 2^{15}_+7, 2^{15}_-9, 2^{15}_+9$	135	2100	5000
10	$2^{13}, 2^{13}_-1, 2^{13}_+1, 2^{13}_-3, 2^{13}_+3, 2^{13}_-5, 2^{13}_+5, 2^{13}_+11, 2^{13}_-13, 2^{13}_+15, 2^{13}_-17$	130	2000	5000

Delay (ps) Modular Multipliers

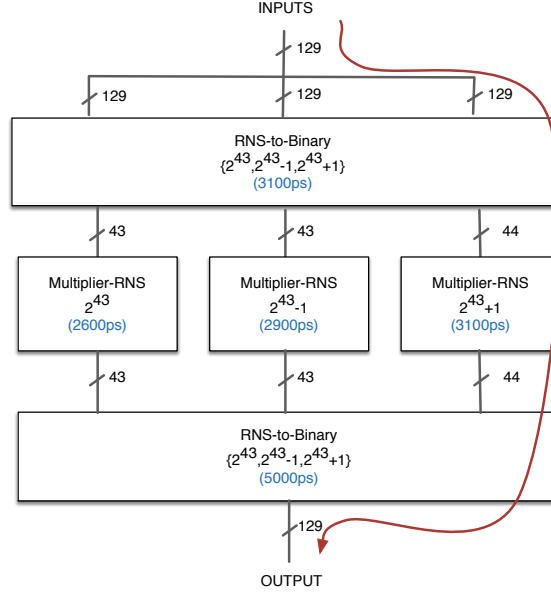
# bits	2^n	$2^n - 1$	$2^n + 1$	$2n-k$	2^n+k
5	960	1120	1480	2200	2600
7	1130	1360	1670	2840	3020
9	1320	1460	1750	3040	3320
11	1440	1670	1830	3120	3620
13	1590	1820	2010	3360	3580
15	1680	1840	2170	3460	3700
17	1770	2010	2320	3510	3770
19	1870	2200	2350	3760	3740
21	1940	2150	2420	3660	3830
23	1980	2240	2500	3850	3980
25	2090	2380	2590	4010	3980
27	2180	2530	2740	4140	4040
29	2280	2590	2750	4180	4200
31	2320	2530	2800	4340	4340
33	2340	2660	2810	4390	4260
35	2450	2690	2850	4390	4450
37	2470	2770	2960	4435	4393
39	2520	2780	3060	4491	4436
41	2520	2840	3040	4544	4477
43	2600	2900	3100	4600	4500



(a) Sabendo que o atraso para um multiplicador de 128-bits usando abordagem binaria convencional é de 22,5ns. Qual é o ganho obtido para $m=1$ comparado com RNS usando um conjunto de 3 módulos?

O atraso da multiplicação RNS incluindo as conversões $binrio \rightarrow RNS$ e $RNS \rightarrow binrio$ vem dado pelo caminho critico da Figura mostrada abaixo $\Delta_{RNS(3modulos)} = 3.10 + 3.10 + 5.0 = 11.2ns$. Comparado com o atraso da

multiplicação binária $\Delta_{BIN} = 22.5ns$, o ratio de ganho será $\frac{11.2}{22.5} = 2.01$, logo em RNS a operação de multiplicação será aproximadamente $\times 2$ mais rápido.



(b) Obtenha o atraso para $m=3$ em binário e em RNS usando um conjunto de 3 módulos.

Seguindo o mesmo raciocínio do apartado anterior, o atraso da multiplicação RNS incluindo as conversões $binrio \rightarrow RNS$ e $RNS \rightarrow binrio$ será $\Delta_{RNS(3modulos)} = 3.10 + (m \times 3.10) + 5.0$, onde $m = 3$, logo $\Delta_{RNS(3modulos)} = 17.4ns$. Comparado com o atraso de 3 multiplicações binárias em série $\Delta_{BIN} = 3 \times 22.5 = 67.5ns$, o ratio de ganho será $\frac{67.5}{17.4} = 3.88$, logo em RNS a operação de multiplicação será quase $\times 4$ mais rápido.

(c) Faça uma tabela com os ganhos obtidos para $m=1$ em comparação com binário para os conjuntos de módulos apresentados (faça as aproximações que ache necessário).

# módulos	Bin → RNS	Multiplicação	RNS → Bin	Atraso Total RNS	Ganho
3	3.1ns	3.1ns	5.0ns	11.2ns	2.01
4	2.8ns	4.35ns	5.0ns	12.15ns	1.85
5	2.6ns	4.05ns	5.0ns	11.65ns	1.93
6	2.4ns	3.9ns	5.0ns	11.3ns	1.99
7	2.3ns	3.76ns	5.0ns	11.06ns	2.03
8	2.2ns	3.75ns	5.0ns	10.95ns	2.05
9	2.1ns	3.7ns	5.0ns	10.8ns	2.08
10	2.0ns	3.58ns	5.0ns	10.58ns	2.13

Atraso multiplicação binária 22.5ns

(d) Faça uma tabela com os ganhos obtidos para o conjunto de três módulos e valores de m de 3 a 10.

Bin → RNS	Multiplicações (m)	RNS → Bin	Atraso Total RNS	Atraso Total Bin	Ganho
3.1ns	3x3.1ns	5.0ns	17.4ns	3x22.5	3.88
3.1ns	4x3.1ns	5.0ns	20.5ns	4x22.5	4.39
3.1ns	5x3.1ns	5.0ns	23.6ns	5x22.5	4.77
3.1ns	6x3.1ns	5.0ns	26.7ns	6x22.5	5.06
3.1ns	7x3.1ns	5.0ns	29.8ns	7x22.5	5.28
3.1ns	8x3.1ns	5.0ns	32.9ns	8x22.5	5.47
3.1ns	9x3.1ns	5.0ns	36ns	9x22.5	5.63
3.1ns	10x3.1ns	5.0ns	39.1ns	10x22.5	5.75