

Universidade Federal de Santa Catarina

EEL7123/EEL510269

Semestre: 2019/2 – Lab3a

Multiplicador RNS

1 Introdução e objetivos

O objectivo deste laboratório consiste em projetar em FPGA uma unidade aritmética multiplicadora RNS vistas nas aulas teóricas. Estas unidades serão reutilizadas nas seguintes aulas experimentais para o desenvolvimento de unidades RNS completas com funcionalidade aritmética soma e multiplicação. A Figura 1 descreve os três níveis de operação das unidades RNS usando o conjunto de módulos $\{m_1, m_2, m_3\} = \{2^n, 2^n - 1, 2^n + 1\}$: i) Conversores binário a RNS (Binary-to-RNS converters) vistas na aula 1a, ii) unidades aritméticas RNS (RNS arithmetic units) sobre a qual estamos trabalhando e iii) conversores RNS a binário (RNS-to-Binary converters) vistas na aula 1b.

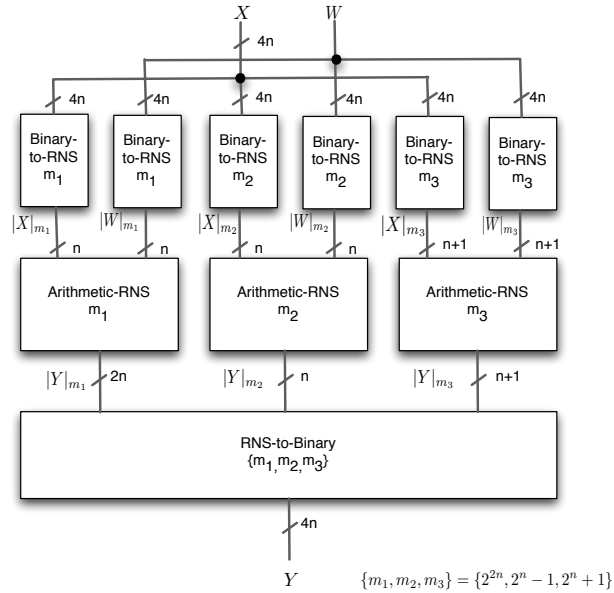


Figura 1: Unidade RNS completa usando conjunto de módulos $\{m_1, m_2, m_3\} = \{2^n, 2^n - 1, 2^n + 1\}$.

2 Multiplicação RNS

As operações de multiplicação em RNS são feitas por canal residual. De esta forma, para o moduli set usado nas aulas anteriores $\{m_1 m_2 m_3\} = \{2^{2n}, 2^n - 1, 2^n + 1\}$ três multiplicadores são necessários de modo a obter a representação do RNS, um para cada elemento de base. Estes multiplicadores podem ser obtidos fazendo deslocação de bits, truncamento de arrays e soma de factores correctores quando necessário tal e como mostrado na Figura 2.

- **Canal $m_1 = 2^{2n}$:** O canal mais simples é o conversor usando o modulo m_1 . O valor da multiplicação $S_1 = |Y|_{m_1} = |R_1 \times Q_1|_{m_1}$, onde $R_1 = |X|_{m_1} = \{r_{1,(2n-1)}, \dots, r_{1,0}\}$ e $Q_1 = |W|_{m_1} = \{q_{1,(2n-1)}, \dots, q_{1,0}\}$ pode ser obtido por médio de truncar o valor de acarreo da multiplicação, uma vez que $|2^{2n}|_{2^{2n}} = 0$ como mostrado na Figura 2(a).
- **Canal $m_1 = 2^n - 1$:** Em este caso o valor da multiplicação $S_2 = |Y|_{m_2} = |R_2 + Q_2|_{m_2}$, onde $R_2 = |X|_{m_2} = \{r_{2,(n-1)}, \dots, r_{2,0}\}$ e $Q_2 = |W|_{m_2} = \{q_{2,(n-1)}, \dots, q_{2,0}\}$ pode ser obtido por médio de fazer uma rotação do acarreo da soma, uma vez que $|2^n|_{2^n-1} = 1$ como mostrado na Figura 2(b).
- **Canal $m_1 = 2^n + 1$:** Em este caso o valor da multiplicação $S_3 = |R_3 + Q_3|_{m_3}$, onde $R_3 = |X|_{m_3} = \{r_{3,(n)}, \dots, r_{3,0}\}$ e $Q_3 = |W|_{m_3} = \{q_{3,(n)}, \dots, q_{3,0}\}$ pode ser obtido por médio de fazer uma rotação do acarreo da soma com complemento, uma vez que $|2^n|_{2^n+1} = -1$ como mostrado na Figura 2(c). Além disso vamos precisar de incluir um factor corrector da mesma forma que fizemos no laboratório 2a para o canal $2^n + 1$.

3 Implementação em VHDL do multiplicador RNS

- Com a placa em funcionamento, baixe o arquivo "*ProjetoLab03a.zip*" disponível no site da disciplina e descompacte esse arquivo na pasta "*/Alunos/EEL510269/lab03*". Atenção: o caminho do diretório para o qual o arquivo será descompactado não deve conter espaços.
- Agora, execute o software Quartus II 13.0sp1 Web Edition (a versão 12.0sp2 também pode ser utilizada). Com o software em funcionamento, acesse o menu File e a opção Open File para abrir os três arquivos VHDL *Multiplier_2_2n.vhd*, *Multiplier_2_n_neg1.vhd* e *Multiplier_2_n_pos1.vhd* disponíveis na pasta destino da descompactação. Os VHDL correspondem com os multiplicadores RNS modulo $\{2^{2n}, 2^n - 1, 2^n + 1\}$.

3.1 Tarefa a ser realizada na sala de aula

O foco desta aula consiste na interpretação dos códigos VHDL dos três canais modulares para obter um multiplicador RNS usando o conjunto de modulos $\{2^{2n}, 2^n - 1, 2^n + 1\}$ e $n = 4$.

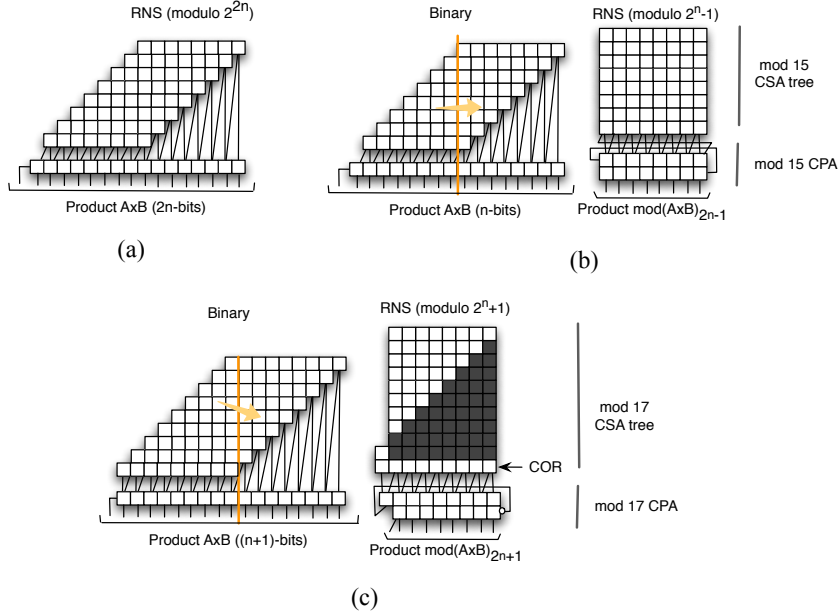


Figura 2: Operação de multiplicação em RNS para canal a) $m_1 = \{2^{2n}\}$, b) $m_2 = \{2^n - 1\}$ e c) $m_3 = \{2^n + 1\}$.

A implementação dos canais $m_1 = \{2^{2n}\}$, $m_2 = \{2^n - 1\}$, $m_3 = \{2^n + 1\}$ com $n = 4$ estão nos arquivos *Multiplier_2_2n.vhd*, *Multiplier_2_neg1.vhd* e *Multiplier_2_pos1.vhd*, respectivamente.

Os produtos parciais estão em *Multiplier_2_2n.vhd*, *Multiplier_2_n_neg1.vhd* e *Multiplier_2_n_pos1.vhd* a partir da linha 40. As somas dos produtos parciais estão sendo feitas usando compressores modulares *MatrixModAdd_2_2n.vhd*, *MatrixModAdd_2_n_neg1.vhd* e *MatrixModAdd_2_n_pos1.vhd*.

O aluno deve explicar ao professor o funcionamento dos blocos *rotate_l_2_2n.vhd*, *rotate_l_2_n_pos1.vhd*, e *rotate_l_2_n_neg1.vhd*, e como foi obtido o factor corrector da linha 56 de *Multiplier_2_pos1.vhd*.

O aluno deve explicar ao professor a linha 72 dos três compressores existentes no projeto *MatrixModAdd_2_2n.vhd*, *MatrixModAdd_2_n_neg1.vhd* e também *MatrixModAdd_2_n_pos1.vhd*.

O seguinte passo consiste na implementação do sistema completo Binário-RNS, multiplicação RNS e volta a binário como indicado na Fig. 1. Para isso vamos precisar de incluir um registrador para introduzir a componente X e W de forma sequencial. Um registrador de 4 bits é fornecido no site da disciplina *REG4.vhd* com reset assíncrono (RST) e enable (EN). **O aluno devesa estender a 16 bits este registrador e incluir o sinal de enable.** Uma vez feita dita extensão, o seguinte passo consiste em descarregar o projeto da aula 1b e incluir os multiplicadores, os registradores e os

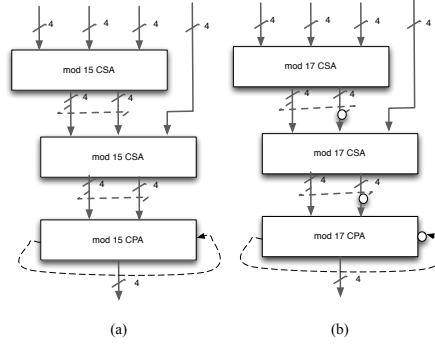


Figura 3: Exemplo de CSA-tree modulo a) $m_2 = \{2^n - 1\}$ e b) $m_3 = \{2^n + 1\}$.

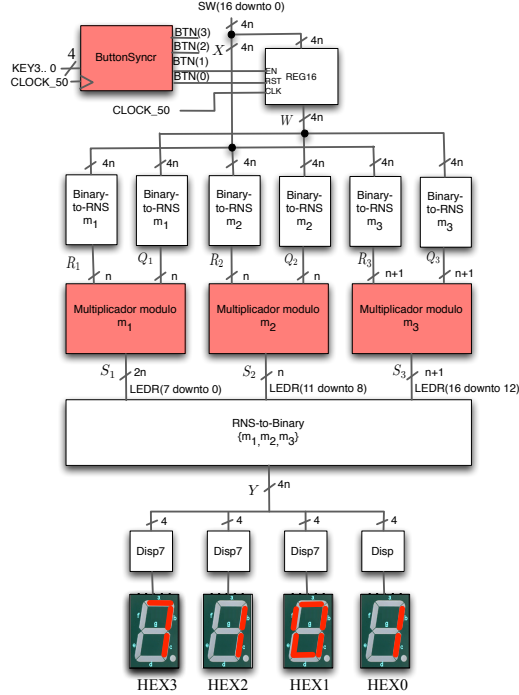


Figura 4: Bloco RNS com soma aritmética com associação de pinos entrada-saída.

três conversores binário-RNS para a entrada W .

A Figura 4 apresenta o mapa de pinos de entrada e saída para dita implementação. Use o sinal $CLOCK_{50}$ como relógio do registrador, o sinal $BTN(0)$ como reset assín-

crono, e BTN(1) como botão de enable para introduzir a entrada W. O sincronizador de botão *buttonSyncr.vhd* deve ser incluído para obter os sinais BTN(1) e BTN(0) a partir dos botões de pressão KEY(1) e KEY(0).

Uma vez compilado sem erros abra modelsim e simule o circuito. Dica: use o script .do para forçar as entradas. **Preencha a tabela 1 com os dados da simulação.**

Uma vez terminada a simulação implemente na placa DE2 o circuito e preencha a tabela 2 com os resultados obtidos nos LEDs vermelhos. Importante: antes de desligar o computador, guarde a pasta lab3a em um pendrive ou envie por e-mail já que este circuito poderia ser usado nos seguintes laboratórios.

Tabela 1: Tabela de resultados de simulação

R_1	R_2	R_3	Q_1	Q_2	Q_3	S_1	S_1	S_1	Y
0	0	0	0	0	0				
255	1	1	255	1	1				
252	0	0	255	1	1				
162	10	5	252	0	0				

Tabela 2: Tabela de resultados na placa DE2

R_1	R_2	R_3	Q_1	Q_2	Q_3	S_1	S_1	S_1	Y
0	0	0	0	0	0				
255	1	1	255	1	1				
252	0	0	255	1	1				
162	10	5	252	0	0				

3.2 Questões finais

- **Pergunta 1:** Qual é o benefício de fazer a multiplicação em RNS em comparação com binário?.
- **Pergunta 2:** O que esperas obter quando multiplicas $X = W = 2^{16} - 1$?
- **Pergunta 3:** Qual foi o valor de factor corretor no canal RNS $m_3 = \{2^n + 1\}$?