4 SISTEMAS DE NUMERAÇÃO RESIDUAL

Metas:

Estudar uma maneira de codificar grandes números como uma coleção de números menores para simplificar e acelerar algumas operações

Destaques do capítulo:

Conjuntos de módulos, gama, operações aritméticas
Muitos conjuntos de módulos possíveis: *tradeoffs*
Conversões entre RNS e binário
Teorema chinês do resto
Por que os aplicações de RNS são limitados?

4 SISTEMAS DE NUMERAÇÃO RESIDUAL

4.1 Fundamentação RNS.
4.2 Codificação e Decodificação em RNS.
    4.2.1 Conversão Binário para RNS.
    4.2.2 Conversão RNS para Binário.
4.3 Aritmética em RNS.
4.4 Escolhendo o Módulo RNS.
4.5 Implementação em hardware.

4 SISTEMAS DE NUMERAÇÃO RESIDUAL

4.1 Fundamentação RNS.

4.2 Codificação e Decodificação em RNS.

4.2.1 Conversão Binário para RNS.

4.2.2 Conversão RNS para Binário.

4.3 Aritmética em RNS.

4.4 Escolhendo o Módulo RNS.

4.5 Implementação em hardware.

4.1. FUNDAMENTAÇÃO – RNS

No Sistema Numérico de Resíduos um número binário é convertido em paralelo para um conjunto de **resíduos** correspondente aos restos da divisão por um conjunto de **módulos**.

$$M = \{m_1, m_2, \ldots, m_n\}$$

Os módulos devem ser primos entre si para permitir a conversão do valor residual para uma solução binária final.

$$MDC(m_i, m_j) = 1 \quad , \quad \text{onde } i \neq j$$

A faixa dinâmica (DR) é dada por:

$$DR = m_1 \times m_2 \times \ldots \times m_n$$

Assim:

Residuos para os modulos m_i

$$X = (R_1, R_2, \ldots, R_n)$$

Binaria

$$R_i = X \bmod m_i = |X|_{m_i} \quad , \quad 0 \leq R_i < m_i$$

4.1. FUNDAMENTAÇÃO – RNS

EXEMPLO 4.1: Para $M = \{5,8,11\}$, as representações de 32_{10} e 48_{10} seriam:

$$|32|_5 = 2, \qquad |32|_8 = 0, \qquad |32|_{11} = 10$$
$$|48|_5 = 3, \qquad |48|_8 = 0, \qquad |48|_{11} = 4.$$

A soma de 32_{10} e 48_{10}, utilizando RNS, seria:

$$|2+3|_5 = |0|_5, \qquad |0+0|_8 = |0|_8, \qquad |10+4|_{11} = |3|_{11}$$

Fazendo a verificação ($32_{10}+48_{10} = 80_{10}$):

$$|80|_5 = 0, \qquad |80|_8 = 0, \qquad |80|_{11} = 3$$

O intervalo de representação (DR) é a multiplicação dos módulos 5x8x11=440 ou *[0, DR-1] = [0, 439]**

* O DR também pode ser representado pelo número de bits da multiplicação.

4.1. FUNDAMENTAÇÃO – RNS

O produto M do módulo k relativamente primo é o intervalo dinâmico

$M = m_{k-1} \times \ldots \times m_1 \times m_0$

Para RNS(8 | 7 | 5 | 3), $M = 8 \times 7 \times 5 \times 3 = 840$

Números negativos: complemento relativo a M

$\langle -x \rangle_{m_i} = \langle M - x \rangle_{m_i}$

$1 = (1 \mid 1 \mid 1 \mid 1)_{RNS}$

$-1 = (840 - 1 \mid 840 - 1 \mid 840 - 1 \mid 840 - 1)_{RNS} = (7 \mid 6 \mid 4 \mid 2)_{RNS}$

Here are some example numbers in our default RNS(8 | 7 | 5 | 3):

$(0 \mid 0 \mid 0 \mid 0)_{RNS}$	Representa 0 ou 840 ou -840. . .
$(1 \mid 1 \mid 1 \mid 1)_{RNS}$	Representa 1 ou 841 ou -839. . .
$(2 \mid 2 \mid 2 \mid 2)_{RNS}$	Representa 2 ou 842 ou -838. . .
$(0 \mid 1 \mid 3 \mid 2)_{RNS}$	Representa 8 ou 848 ou -832. . .
$(5 \mid 0 \mid 1 \mid 0)_{RNS}$	Representa 21 ou 861 ou -819. . .
$(0 \mid 1 \mid 4 \mid 1)_{RNS}$	Representa 64 ou 904 ou -776. . .
$(2 \mid 0 \mid 0 \mid 2)_{RNS}$	Representa 770 ou 1610 ou -70. . .
$(7 \mid 6 \mid 4 \mid 2)_{RNS}$	Representa 839 ou 1679 ou -1 . . .

Podemos considerar o intervalo de RNS (8 | 7 | 5 | 3) como [-420, 419] ou qualquer outro conjunto de 840 inteiros consecutivos

4.1. FUNDAMENTAÇÃO – RNS

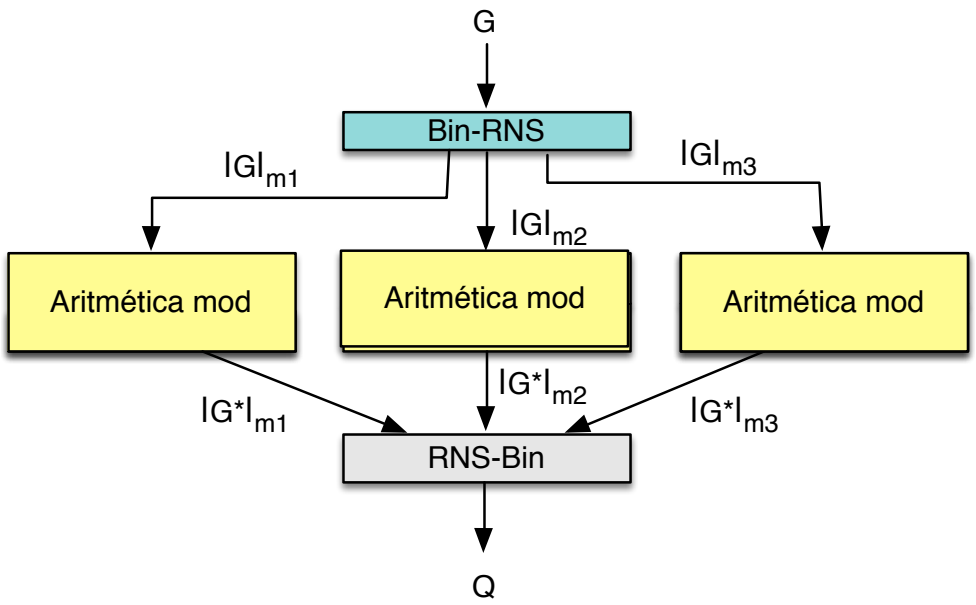
Nos Sistemas de Números de Resíduos, um número binário é convertido em paralelo para um conjunto de palavras residuais correspondentes aos restos de valores de módulos:

$\{m_1, m_2, m_3\}$

$|G|_m = R$

G | m

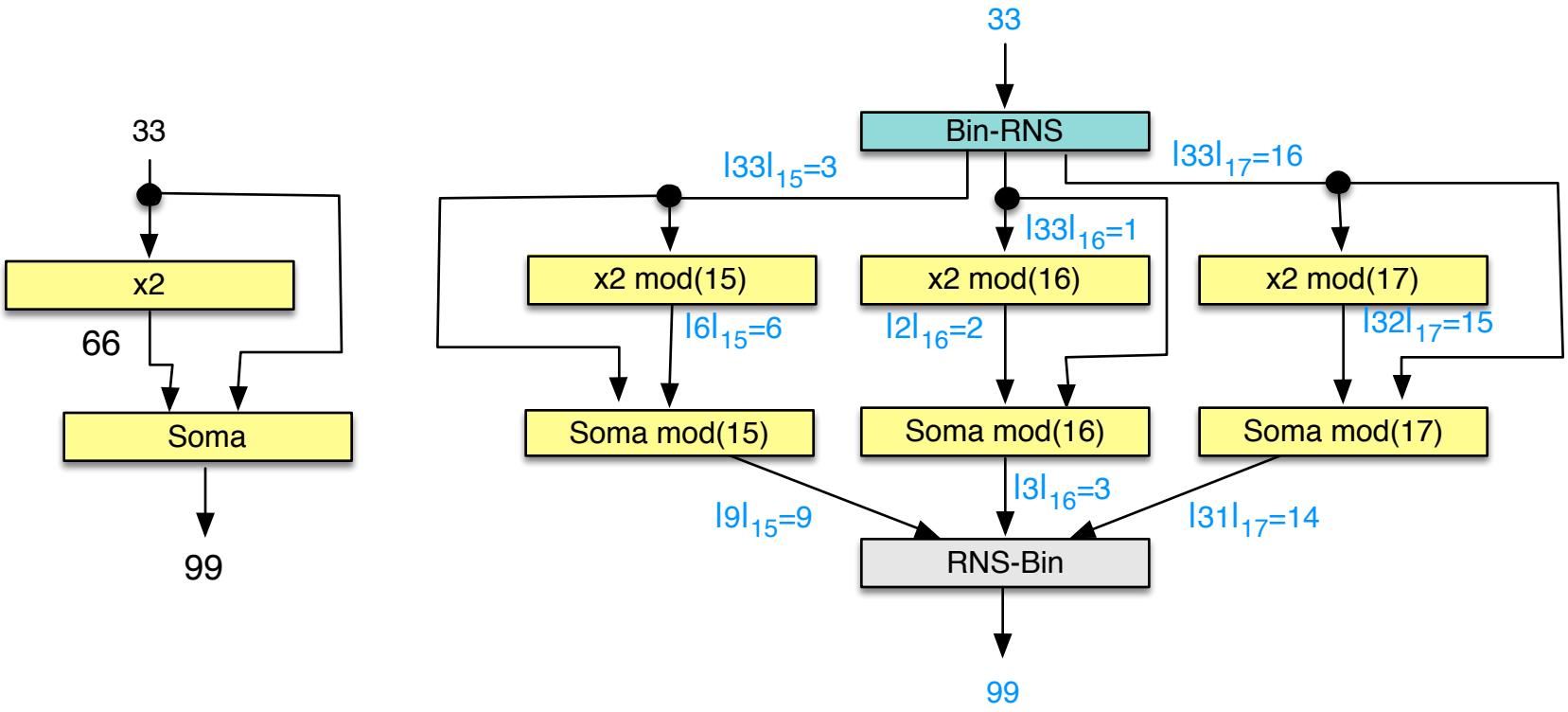
R C



4.1. FUNDAMENTAÇÃO – RNS

Para o conjunto de módulos {15,16,17}={2^4-1, 2^4, 2^4+1} e uma entrada G=33, a solução para a operação Q=33*2+33=99.

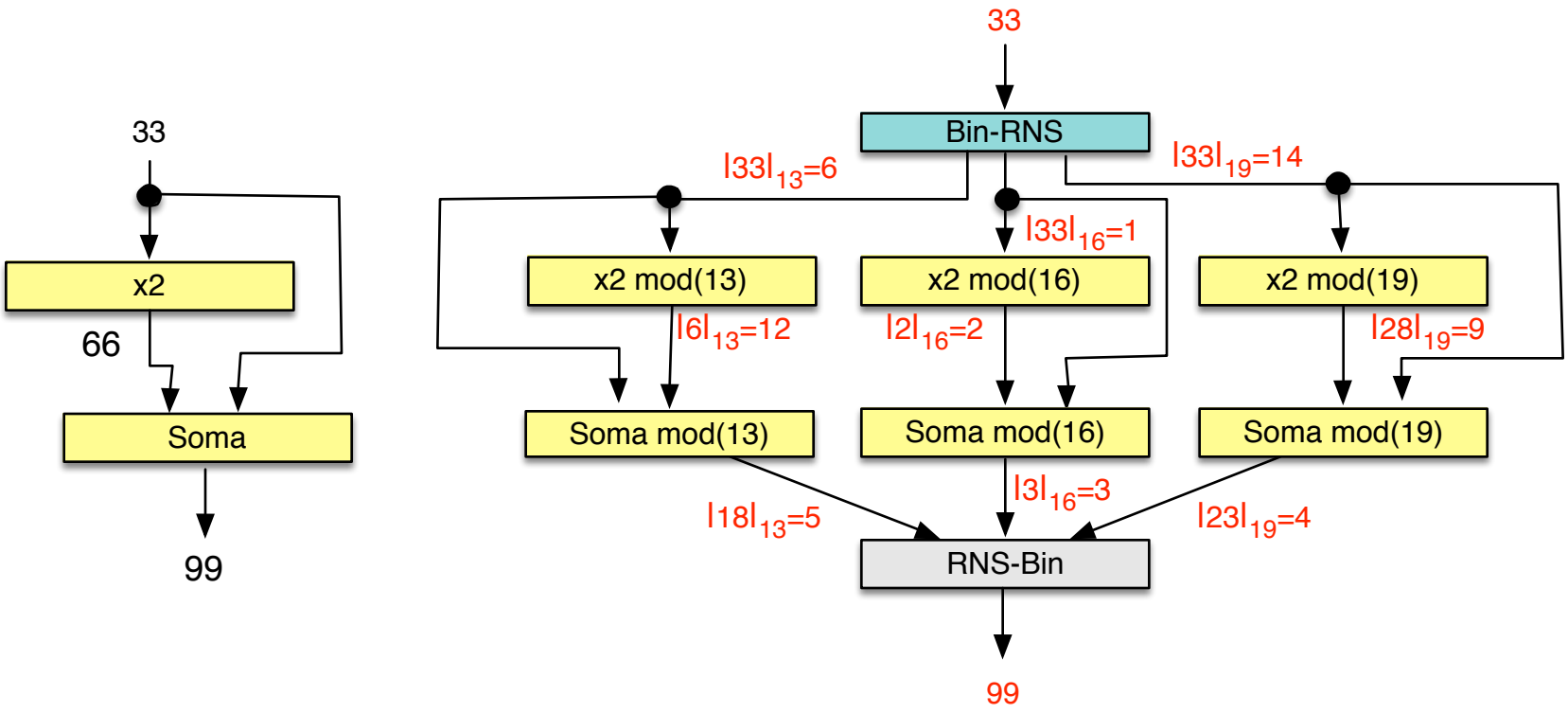
A solução binária requer grandes multiplicadores e somadores em comparação com a solução RNS.



4.1. FUNDAMENTAÇÃO – RNS

Para o conjunto de módulos {13,16,19}={2^4-3, 2^4, 2^4+3} e uma entrada G=33, a solução para a operação Q=33*2+33=99.

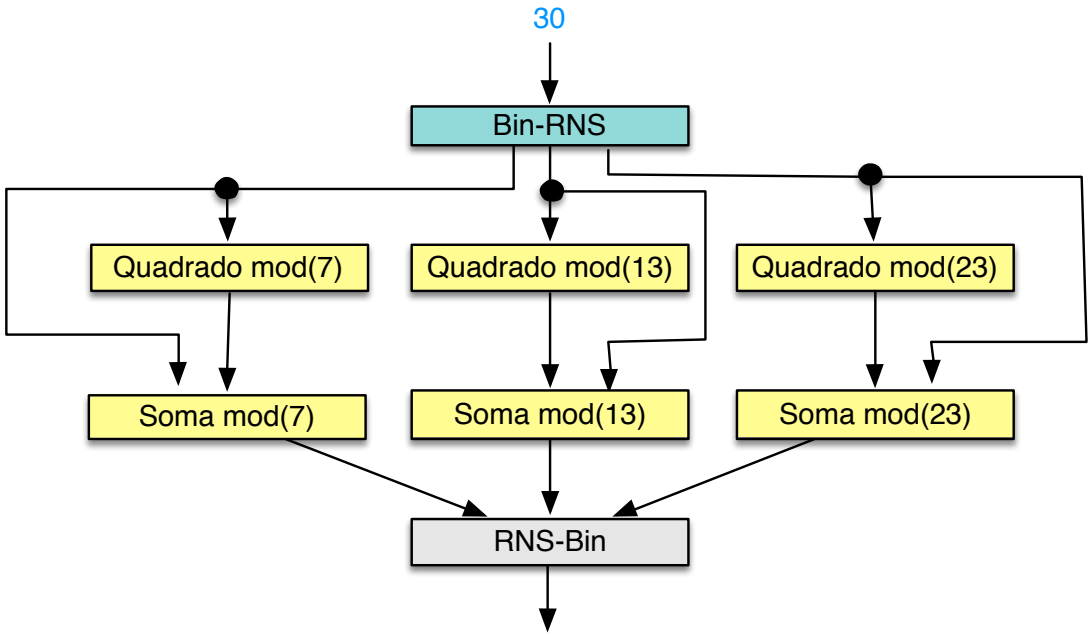
A solução binária requer grandes multiplicadores e somadores em comparação com a solução RNS.



PROBLEMAS

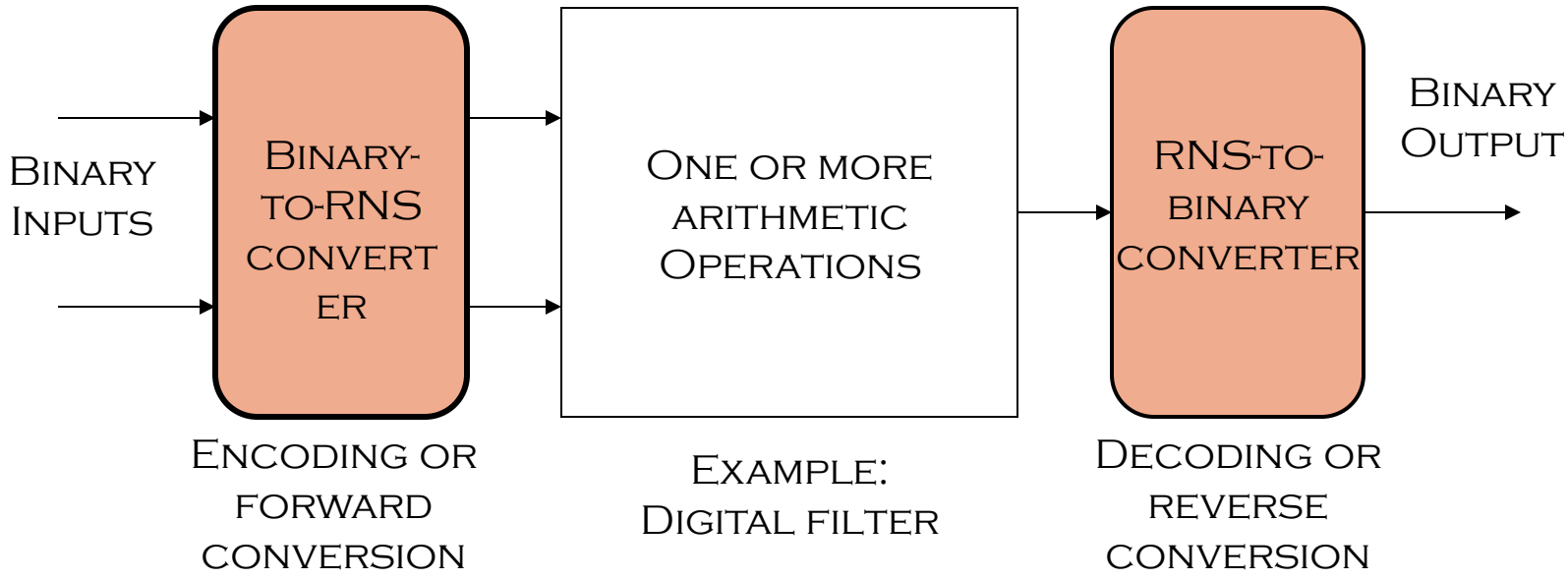
Problema 4.1. Obtenha as faixas dinâmicas para os seguintes conjuntos de módulos: a) M1={3,5,7,17}; b) M2= {15,16,17}; c) M3= {7,13, 23}.

Problema 4.2. Indique os valores de saída para todos os blocos. A saída final está na faixa dinâmica permitida para o modulo?



4 SISTEMAS DE NUMERAÇÃO RESIDUAL

4.2 CODIFICAÇÃO E DECODIFICAÇÃO EM RNS



Quanto mais a quantidade de computação executada entre o conversão inicial e conversão inversa final (reconversão), maiores são os benefícios da representação RNS.

4.2.1 Conversão Binaria-RNS

Exemplo 4.2: Represente o número $y = (1010\ 0100)_2 = (164)_{10}$ em RNS (8 | 7 | 5 | 3)

Obtemos $y = 2^7+2^5+2^2$;

$$x_3 = \langle y \rangle_8 = \langle 4 + 0 + 0 \rangle_8 = 4$$
$$x_2 = \langle y \rangle_7 = \langle 2 + 4 + 4 \rangle_7 = 3$$
$$x_1 = \langle y \rangle_5 = \langle 3 + 2 + 4 \rangle_5 = 4$$
$$x_0 = \langle y \rangle_3 = \langle 2 + 2 + 1 \rangle_3 = 2$$

Tabela 4.1 Resiiduos das 10 primeiras potencias 2

i	2^i	$\langle 2^i \rangle_8$	$\langle 2^i \rangle_7$	$\langle 2^i \rangle_5$	$\langle 2^i \rangle_3$
0	1	1	1	1	1
1	2	2	2	2	2
2	4	4	4	4	1
3	8	0	1	3	2
4	16	0	2	1	1
5	32	0	4	2	2
6	64	0	1	4	1
7	128	0	2	3	2
8	256	0	4	1	1
9	512	0	1	2	2

4.2.1 Conversão Binaria-RNS

Exemplo 4.3: Represente o número $y = (1010\ 0100)_2 = (164)_{10}$ em RNS(15 | 16 | 17)

Obtemos $y = 2^7+2^5+2^2$;

$$x_3 = \langle y \rangle_{15} = \langle 8 + 2 + 4 \rangle_{15} = 14$$
$$x_2 = \langle y \rangle_{16} = \langle 0 + 0 + 4 \rangle_{16} = 4$$
$$x_1 = \langle y \rangle_{17} = \langle 9 + 15 + 4 \rangle_{17} = 11$$

Tabela 4.2 Resiiduos das 10 primeiras potencias 2

I	2^I	$\langle 2^I \rangle_{15}$	$\langle 2^I \rangle_{16}$	$\langle 2^I \rangle_{17}$
0	1	1	1	1
1	2	2	2	2
2	4	4	4	4
3	8	8	8	8
4	16	1	0	16
5	32	2	0	15
6	64	4	0	13
7	128	8	0	9
8	256	1	0	1
9	512	2	0	2

4.2.2 Conversão RNS-Binario

Quebra-cabeça, devido ao estudioso chinês Sun Tzu, há mais de 1500 anos

Que número tem os restos de 2, 3 e 2?
quando dividido por 7, 5 e 3, respectivamente?

$$x = (2 \mid 3 \mid 2)_{RNS(7|5|3)} = (?)_{TEN}$$

4.2.2 Conversão RNS-Binario

A representação RNS pode ser convertida de volta para binário (X) usando:

a) Teorema Chinês do Resto (CRT):

$$X = \left| \sum_{i=1}^{n} \hat{m}_i \left| \hat{m}_i^{-1} \right|_{m_i} \times R_i \right|_M$$

, onde

$$M = \prod_{i=1}^{n} m_i$$

$$\hat{m}_i = M / m_i$$

$$\left| \left| \hat{m}_i^{-1} \right|_{m_i} \hat{m}_i \right|_{m_i} = 1$$

$\left| \hat{m}_i^{-1} \right|_{m_i}$ represents the multiplicative inverse of $\hat{m}_i$ with respect to modulus m_i

b) Novo CRT-I:

$$X = \left| \sum_{i=1}^{n} \left| V_i R_i \right|_{\hat{m}_1} \right|_{\hat{m}_1} m_1 + R_1$$

, onde

$$V_1 = \frac{\left| \hat{m}_1^{-1} \right|_{m_1} \hat{m}_1 - 1}{m_1}$$

$$V_i = \left| \hat{m}_i^{-1} \right|_{m_i} \frac{\hat{m}_i}{m_1} \quad \text{for} \quad 2 \le i \le n$$

4.2.2 Conversão RNS-Binario

Exemplo 4.4: $\{m_1,m_2,m_3\}=\{16,15,17\}$ e $\{R_1,R_2,R_3\}=\{15,14,16\}$:

a) Teorema Chinês do Resto (CRT):

$$X = \left| \sum_{i=1}^{n} \hat{m}_i \left| \hat{m}_i^{-1} \right|_{m_i} \times R_i \right|_M \quad \text{, onde} \quad M = \prod_{i=1}^{n} m_i$$

$$\hat{m}_i = M/m_i$$

$$\left| \left| \hat{m}_i^{-1} \right|_{m_i} \hat{m}_i \right|_{m_i} = 1$$

b) Novo CRT-I:

$$X = \left| \sum_{i=1}^{n} |V_i R_i|_{\hat{m}_1} \right|_{\hat{m}_1} m_1 + R_1 \quad \text{, onde} \quad V_1 = \frac{\left| \hat{m}_1^{-1} \right|_{m_1} \hat{m}_1 - 1}{m_1}$$

$$V_i = \left| \hat{m}_i^{-1} \right|_{m_i} \frac{\hat{m}_i}{m_1} \quad \text{for} \quad 2 \le i \le n$$

PROBLEMAS

Problema 4.3. Represente o número $y = 1010\ 0100_2 = 200_{10}$ para os seguintes conjuntos de módulos: a) M1={3,5,7,17}; b) M2= {16,15,17}; c) M3= {7,13, 23}.

Problema 4.4. Obtenha o valor de saída aplicando a equação CRT para os seguintes conjuntos de módulos:

a) $\{m_1,m_2,m3,m4\}=\{3,5,7,17\}$ e $\{R1,R2,R3,R4\}=\{2, 0, 4, 13\}$;

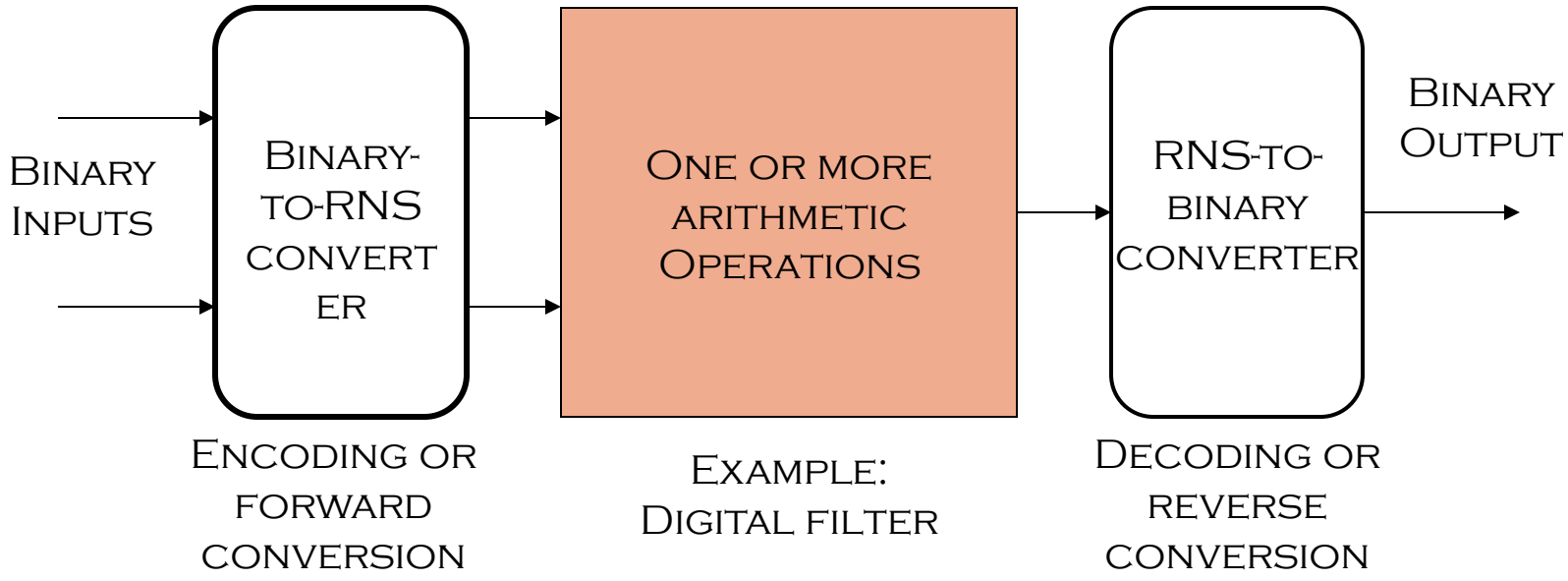
b) $\{m_1,m2,m3\}= \{16,15,17\}$ e $\{R1,R2,R3\}=\{8, 5,13\}$;

c) $\{m_1,m2,m3\}= \{7,13, 23\}$ e $\{R1,R2,R3\}=\{4, 5,16\}$.

Problema 4.5. Obtenha o valor de saída aplicando a equação Novo CRT-I para os módulos apresentados no exemplo anterior.

4 SISTEMAS DE NUMERAÇÃO RESIDUAL

4.3 ARITMÉTICA EM RNS



Quanto mais a quantidade de computação executada entre o conversão inicial e conversão inversa final (reconversão), maiores são os benefícios da representação RNS.

4.3 ARITMÉTICA EM RNS

$Y = (0100\ 0101)_2 = (69)_{10}$ em RNS(8 | 7 | 5 | 3) e
$Z = (0000\ 1100)_2 = (12)_{10}$ em RNS(8 | 7 | 5 | 3), são
$(5 \mid 6 \mid 4 \mid 0)_{RNS(8|7|5|3)}$ e $(4 \mid 5 \mid 2 \mid 0)_{RNS(8|7|5|3)}$

Multiplicação de Y e Z:
$\langle 5 \times 4 \rangle_8 = 4$; $\langle 6 \times 5 \rangle_7 = 2$; $\langle 4 \times 2 \rangle_5 = 3$; $\langle 0 \times 0 \rangle_3 = 0$
$(4 \mid 2 \mid 3 \mid 0)_{RNS(8|7|5|3)}$
Soma:
$\langle 5 + 4 \rangle_8 = 1$; $\langle 6 + 5 \rangle_7 = 4$; $\langle 4 + 2 \rangle_5 = 1$; $\langle 0 + 0 \rangle_3 = 0$
$(1 \mid 4 \mid 1 \mid 0)_{RNS(8|7|5|3)}$

PROBLEMAS

Problema 4.6. Para umas entradas $Y=13_{10}$ e $Z=15_{10}$ faça as operações $(YxZ)_{RNS}$ e $(Y+Z)_{RNS}$ para os conjunto de módulos:

a) M1={3,5,7,17};

b) M2= {16,15,17};

c) M3= {7,13, 23}.

Problema 4.7. Para umas entradas $Y=16_{10}$ e $Z=9_{10}$ faça a operação $(YxZ+Y)_{RNS}$ para os conjunto de módulos:

a) M1={3,5,7,17};

b) M2= {16,15,17};

c) M3= {7,13, 23}.

4 SISTEMAS DE NUMERAÇÃO RESIDUAL

4.4 ESCOLHENDO O CONJUNTO DE MÓDULOS

Faixa Dinámica (DR) para nosso RNS: valores decimais [0, 100 000]

Estratégia 1: Para minimizar a escolha de módulos com valores grandes, e assim garantir aritmética de alta velocidade, escolha os números primos em sequência.

Escolher $m_0 = 2$, $m_1 = 3$, $m_2 = 5$, etc. até $m_5 = 13$:

RNS(13 | 11 | 7 | 5 | 3 | 2)	$M = 30030$	Inadequado
RNS(17 | 13 | 11 | 7 | 5 | 3 | 2)	$M = 510510$	Grande demais
RNS(17 | 13 | 11 | 7 | 3 | 2)	$M = 102102$	Exato!
	5 + 4 + 4 + 3 + 2 + 1 = 19 bits	

Ajuste fino: combinar pares de módulos 2 & 13 (26) e 3 & 7 (21)

RNS(26 | 21 | 17 | 11) $M = 102102$

4.4 ESCOLHENDO O CONJUNTO DE MÓDULOS

Intervalo de destino para nosso RNS: valores decimais [0, 100 000]

Estratégia 2: Para simplificar as operações modulares (mod m_i), escolher unicamente modulos da forma 2^a or $2^a - 1$, "Modulos de baixo custo"

$$\text{RNS}(2^{a_{k-1}} \mid 2^{a_{k-2}} - 1 \mid \ldots \mid 2^{a_1} - 1 \mid 2^{a_0} - 1)$$

Podemos ter unicamente módulos impar
$2^{a_i} - 1$ e $2^{a_j} - 1$ são coprimos se a_i e a_j *são primos*

RNS($2^3 \mid 2^3-1 \mid 2^2-1$)	bases: 3, 2	M = 168
RNS($2^4 \mid 2^4-1 \mid 2^3-1$)	bases: 4, 3	M = 1680
RNS($2^5 \mid 2^5-1 \mid 2^3-1 \mid 2^2-1$)	bases: 5, 3, 2	M = 20832
RNS($2^5 \mid 2^5-1 \mid 2^4-1 \mid 2^3-1$)	bases: 5, 4, 3	M = 104160

Comparação

RNS($15 \mid 13 \mid 11 \mid 2^3 \mid 7$)	18 bits	M = 120120
RNS($2^5 \mid 2^5-1 \mid 2^4-1 \mid 2^3-1$)	17 bits	M = 104160

4.4 ESCOLHENDO O CONJUNTO DE MÓDULOS

Intervalo de destino para nosso RNS: valores decimais [0, 100 000]

Estratégia 3: Para simplificar as operações modulares (mod m_i), escolher módulos das forma 2^a, $2^a - 1$, ou $2^a + 1$

$$\text{RNS}(2^{a_{k-1}} \mid 2^{a_{k-2}} \pm 1 \mid \ldots \mid 2^{a_1} \pm 1 \mid 2^{a_0} \pm 1)$$

Podemos ter unicamente módulos impar
$2^{a_i} - 1$ e $2^{a_j} + 1$sao primos

$\text{RNS}(2^5 \mid 2^4-1 \mid 2^4+1 \mid 2^3-1)$ $M = 57120$
$\text{RNS}(2^5 \mid 2^4+1 \mid 2^3+1 \mid 2^3-1 \mid 2^2-1)$ $M = 102816$

O Modulo $2^a + 1$ não é tão conveniente como $2^a - 1$
(precisa de um bit mais de resíduo e as operações modulares não são tão simples)

4.4 ESCOLHENDO O CONJUNTO DE MÓDULOS

Foram mostradas 3 estratégias para seleção de modulo tendo em consideração os módulos mais eficientes.

A solução parece ir no uso de conjunto com muitos módulos para minimizar o número de bits por canal modular. No entanto quanto mais módulos no conjunto a conversão final RNS-bin será mais complexa.

Aqui é mostrado a escolha de conjunto de módulos para conversores RNS-bin eficientes:

Conjunto de módulos	DR	Ano
$\{2^n, 2^n \pm 1\}$	$3n$	2002
$\{2^{2n}, 2^n \pm 1\}$	$4n$	2004
$\{2^n \pm 1, 2^n \pm 3\}$	$4n$	2004
$\{2^n, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1\}$	$5n$	2005
$\{2^n, 2^n \pm 1, 2^{n\pm1} - 1\}$	$5n$	2007
$\{2^{2n}, 2^n \pm 1, 2^{2n} + 1\}$	$6n$	2010
$\{2^n, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1, 2^{n+1} + 1\}$	$6n + 1$	2013
$\{2^{2n}, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1, 2^{n+1} + 1\}$	$7n + 1$	2013
$\{2^{3n}, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1, 2^{n+1} + 1\}$	$8n + 1$	2013
$\{2^{2n}, 2^n \pm 1, 2^n \pm k_1, 2^n \pm k_2, \ldots, 2^n \pm k_f\}$	$(2f + 3)n$	2014

4.4 ESCOLHENDO O CONJUNTO DE MÓDULOS

Foram mostradas 3 estratégias para seleção de modulo tendo em consideração os módulos mais eficientes.

A solução parece ir no uso de conjunto com muitos módulos para minimizar o número de bits por canal modular. No entanto quanto mais módulos no conjunto a conversão final RNS-bin será mais complexa.

Aqui é mostrado a escolha de conjunto de módulos para conversores RNS-bin eficientes:

Vamos usar os conjuntos como estudos de caso

	Conjunto de módulos	DR	Ano
M1	$\{2^n, 2^n \pm 1\}$	$3n$	2002
	$\{2^{2n}, 2^n \pm 1\}$	$4n$	2004
M2	$\{2^n \pm 1, 2^n \pm 3\}$	$4n$	2004
	$\{2^n, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1\}$	$5n$	2005
	$\{2^n, 2^n \pm 1, 2^{n\pm1} - 1\}$	$5n$	2007
	$\{2^{2n}, 2^n \pm 1, 2^{2n} + 1\}$	$6n$	2010
	$\{2^n, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1, 2^{n+1} + 1\}$	$6n + 1$	2013
	$\{2^{2n}, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1, 2^{n+1} + 1\}$	$7n + 1$	2013
	$\{2^{3n}, 2^n \pm 1, 2^n \pm 2^{(n+1)/2} + 1, 2^{n+1} + 1\}$	$8n + 1$	2013
	$\{2^{2n}, 2^n \pm 1, 2^n \pm k_1, 2^n \pm k_2, \ldots, 2^n \pm k_f\}$	$(2f + 3)n$	2014

PROBLEMAS

Problema 4.8. Aplique as três estratégias apresentadas na teoria para obter uma Faixa Dinâmica (DR) com valores de saída [0, 200 000].

4 SISTEMAS DE NUMERAÇÃO RESIDUAL

4.5 IMPLEMENTAÇÃO EM HARDWARE

$M1=\{2^{2n}, 2^n-1, 2^n+1\}$

1. Conversor Binário-RNS (Direto)
2. Unidade aritmética RNS (somadores e multiplicadores)
3. Conversor RNS-Binário (Reverso)

A ser visto em outros capítulos

$M2=\{2^{2n}, 2^n-3, 2^n+3\}$

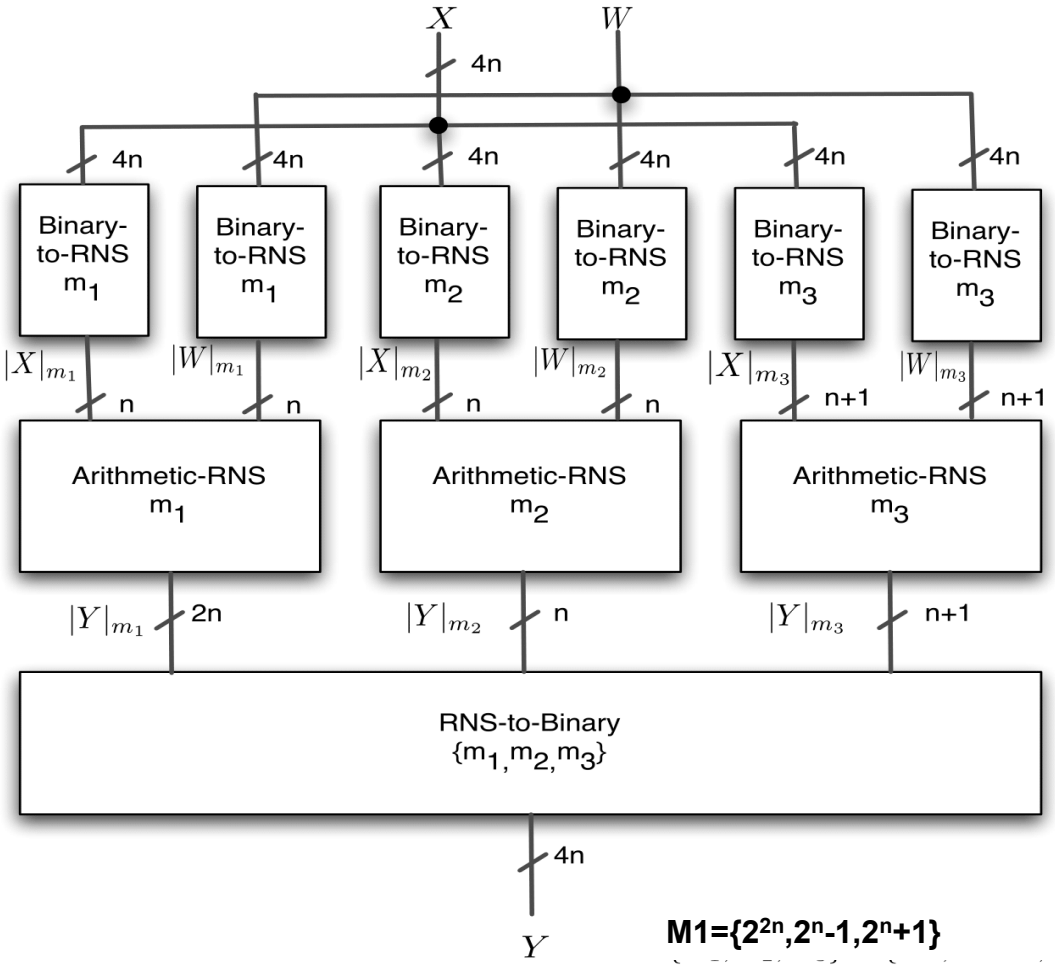
1. Conversor Binário-RNS (Direto)
2. Unidade aritmética RNS (somadores e multiplicadores)
3. Conversor RNS-Binário (Reverso)

A ser visto em outros capítulos

$M1=\{2^{2N}, 2^N-1, 2^N+1\}$: HARDWARE IMPLEMENTATION

- Blocos básicos

1. Conversor direto
2. Unidade aritmética
3. Conversor reverso



$M1=\{2^{2N}, 2^N-1, 2^N+1\}$: HARDWARE IMPLEMENTATION CONVERSÃO DIRETA

Um numero inteiro $X = \{x_{(4n-1)}, \ldots, x_1, x_0\}$ pode ser expressado em notação binaria como:

$$X = \sum_{i=1}^{4n-1} 2^i x_i = 2^{3n} N_3 + 2^{2n} N_2 + 2^n N_1 + N_0, \quad (1)$$

onde os arrays $N_3 = \{x_{(4n-1)}, \ldots, x_{(3n+1)}, x_{3n}\}$, $N_2 = \{x_{(3n-1)}, \ldots, x_{(2n+1)}, x_{2n}\}$, $N_1 = \{x_{(2n-1)}, \ldots, x_{(n+1)}, x_n\}$ e $N_0 = \{x_{(n-1)}, \ldots, x_1, x_0\}$. Usando notação binaria e conjunto de módulos $\{m_1, m_2, m_3\} = \{2^{2n}, 2^n - 1, 2^n + 1\}$, a faixa dinâmica do valor X é $[0, M-1]$, onde $M = m_1 m_2 m_3$. Três conversores são necessários de modo a obter a representação do RNS, um para cada elemento de base.

M1={2^{2N} , 2^N-1, 2^N+1}: HARDWARE IMPLEMENTATION CONVERSÃO DIRETA

- **Canal** $m_1 = 2^{2n}$**:** O canal mais simples é o conversor usando o modulo m_1. O valor $|X|_{m_1}$ pode ser obtido pelo resto da divisão do X por 2^{2n} , o que pode por conseguida por médio de truncar o valor de X, uma vez que:

$$|X|_{m_1} = \overbrace{|2^{3n}|_{m_1}}^{=0} N_3 + \overbrace{|2^{2n}|_{m_1}}^{=0} N_2 + 2^n N_1 + N_0 = \{x_{(2n-1)}, \ldots, x_1, x_0\}. \quad (2)$$

- **Canal** $m_2 = 2^n - 1$**:** Devido a que $|2^n|_{2^n-1} = 1$, podemos expressar a Eq. 1 como:

$$|X|_{m_2} = |N_3 + N_2 + N_1 + N_0|_{2^n-1} = |N_3 + |N_2 + N_1 + N_0|_{2^n-1}|_{2^n-1}. \quad (3)$$

- **Canal** $m_3 = 2^n + 1$**:** Devido a que $|2^n|_{2^n+1} = -1$, podemos expressar a Eq. 1 como:

$$|X|_{m_3} = |N_3 - N_2 + N_1 - N_0|_{2^n+1} = |-N_3 + |N_2 - N_1 + N_0|_{2^n+1}|_{2^n+1}. \quad (4)$$

M1={2^{2N} , 2^N-1, 2^N+1}: HARDWARE IMPLEMENTATION CONVERSÃO DIRETA

- **Bloco 2^{2n} :** Truncamento a partir do digito 2^{2n} , pois (2^{2n} mod 2^{2n})= 0
- **Bloco 2^n - 1 :** Soma dos N termos, posicionando o carry em 2^0 (EAC). (2^n mod 2^n – 1) = 1
- **Bloco 2^n + 1:** Somatório dos N termos, posicionando o complemento do carry em 2^0 (IEAC). (2^n mod 2^n +1) = -1

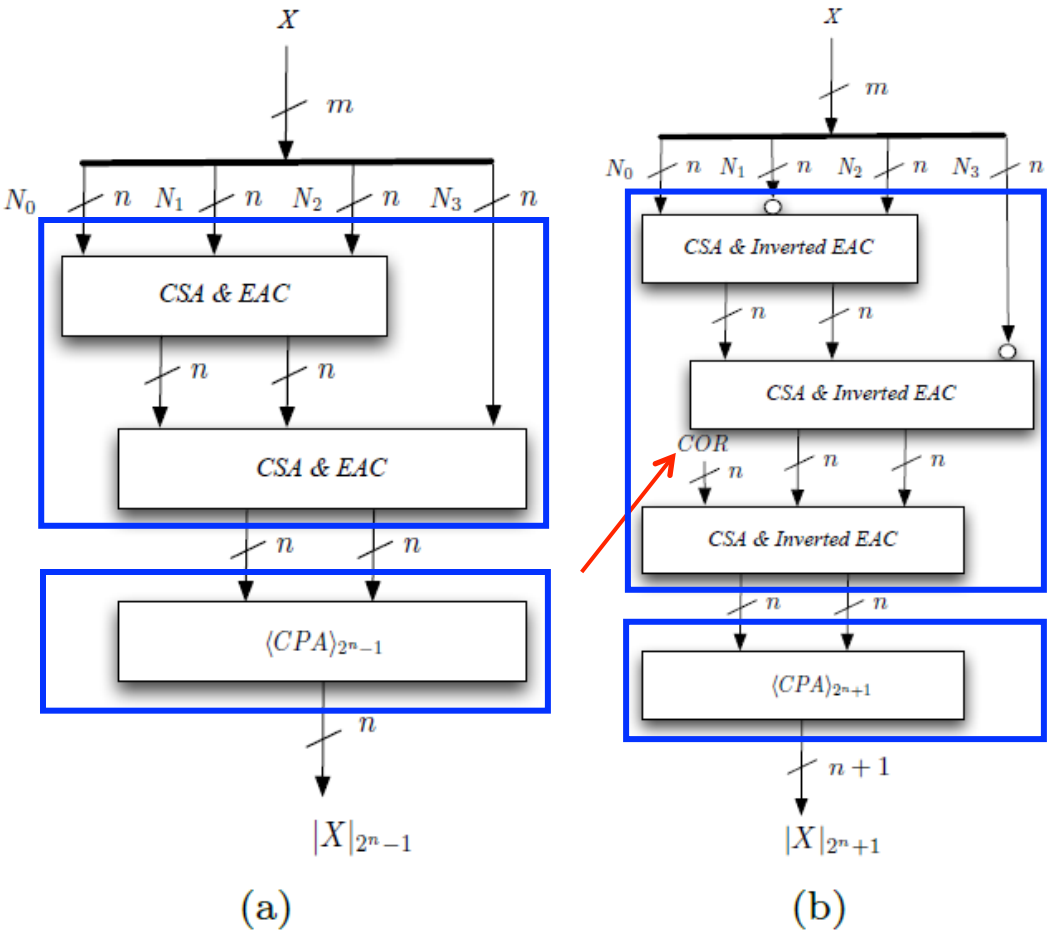
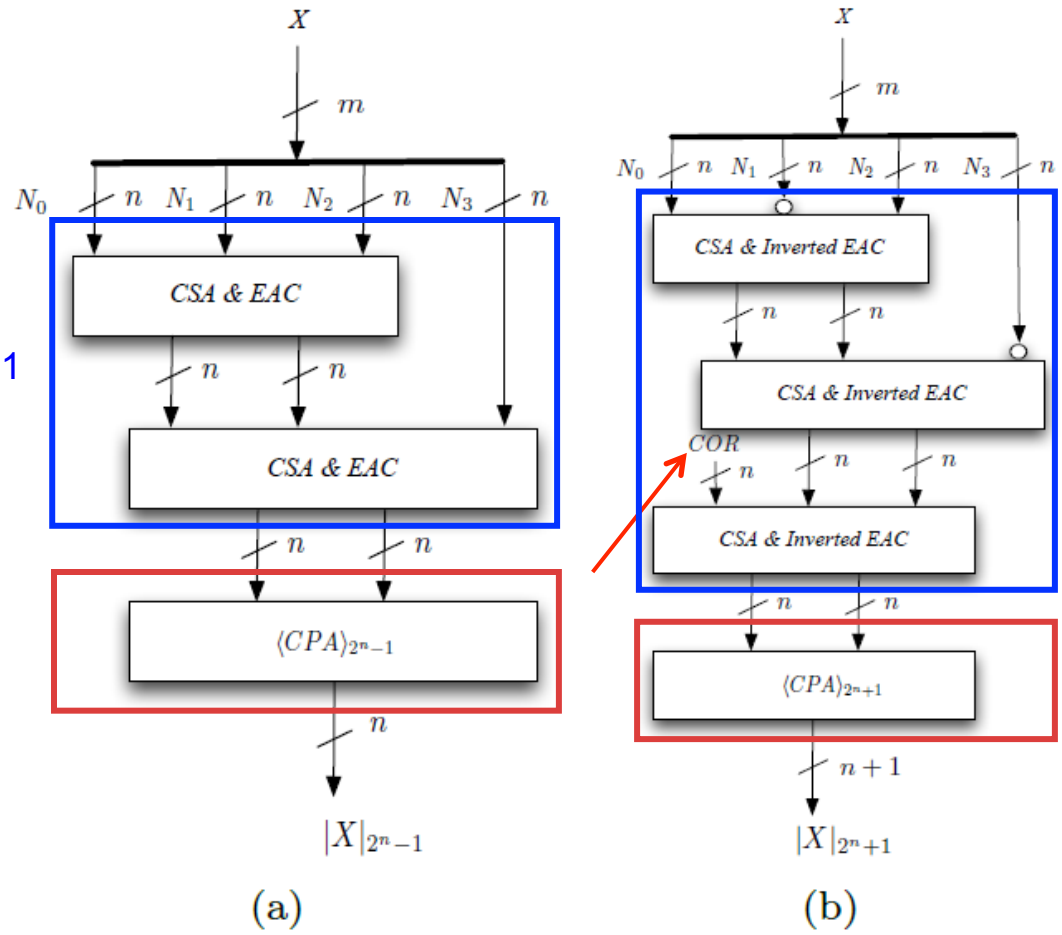


Figura 2 – Conversores diretos 2n - 1

$M1=\{2^{2N}, 2^N-1, 2^N+1\}$: HARDWARE IMPLEMENTATION CONVERSÃO DIRETA

Compressor mod 2^n-1

Somador mod 2^n-1



Compressor mod 2^n+1

Somador mod 2^n+1

Figura 2 – Conversores diretos 2n - 1

$M1=\{2^{2N}, 2^N-1, 2^N+1\}$: HARDWARE IMPLEMENTATION CONVERSÃO REVERSA

Para cada conjunto de módulos implementado, é necessário que seja projetado um conversor reverso.

Aplicando o algoritmo Novo CRT-I:

$$X = \left| \sum_{i=1}^{n} |V_i R_i|_{\hat{m}_1} \right|_{\hat{m}_1} m_1 + R_1 \quad \text{, onde} \quad V_1 = \frac{\left|\hat{m}_1^{-1}\right|_{m_1} \hat{m}_1 - 1}{m_1}$$

$$V_i = \left|\hat{m}_i^{-1}\right|_{m_i} \frac{\hat{m}_i}{m_1} \quad \text{for} \quad 2 \le i \le n$$

Solução obtida no Problema 4.5 para n=4

PROBLEMAS

Problema 4.10. Considere o seguinte conjunto de módulos $\{2^{2n},2^n-1,2^n+1\}$, para n=4 e uma entrada-saída de $4n$ bits:

a) Obtenha a estrutura para fazer a conversão binário-RNS (use compressores e somadores modulo 15 e 17).

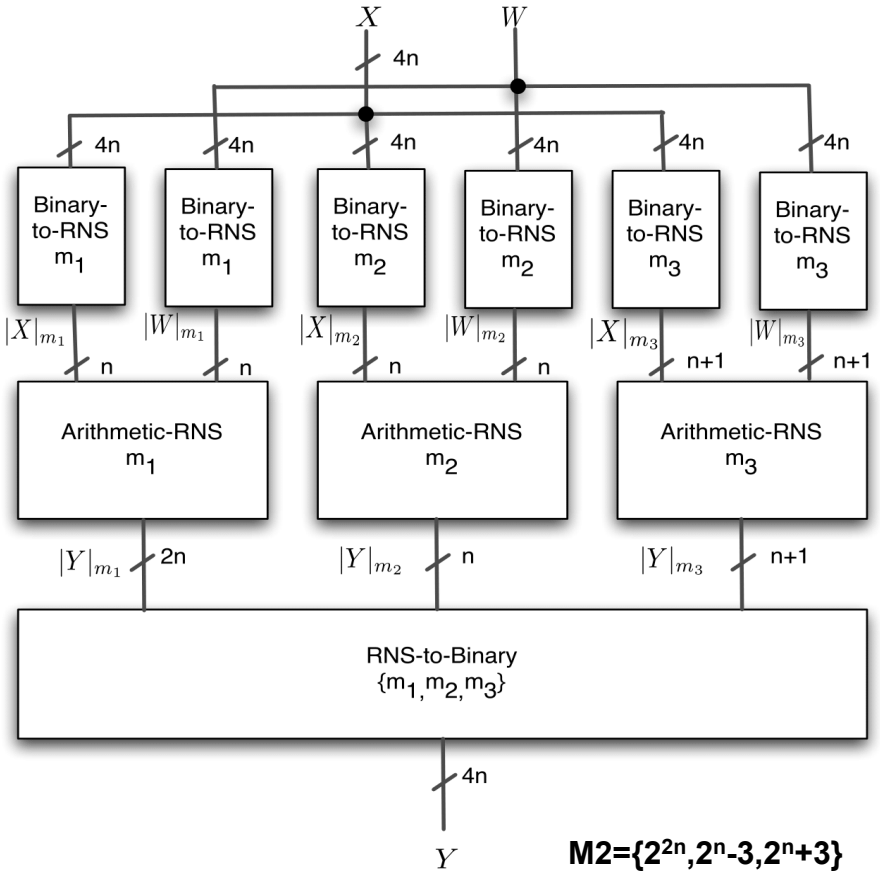
b) Obtenha a estrutura para fazer a conversão RNS-binário (use o algoritmo novo CRT-I, compressores e somadores módulo 255).

c) Indique a faixa dinâmica da estrutura RNS e compare com a eficiência da representação com binário.

$M2=\{2^{2N}, 2^N-3, 2^N+3\}$: HARDWARE IMPLEMENTATION

- Blocos básicos

1. Conversor direto
2. Unidade aritmética
3. Conversor reverso



$M2=\{2^{2n},2^n-3,2^n+3\}$

M2: HARDWARE IMPLEMENTATION
CONVERSÃO DIRETA

Para conjunto :

- **Bloco 2^{2n} :** Truncamento a partir do digito 2^{2n} , pois (2^{2n} mod 2^{2n})= 0
- **Bloco 2^{n} - k :** Soma dos N termos, cada *carry* tem um peso k. (2^{n} mod 2^{n} – 1) = k
- **Bloco 2^{n} + k:** Somatório dos N termos, cada *carry* tem um peso -k (2^{n} mod 2^{n} +1) = -k

M2: HARDWARE IMPLEMENTATION CONVERSOR RNS-BIN

A representação RNS pode ser convertida de volta para binário (X) usando:

a) Teorema Chinês do Resto (CRT):

$$X = \left| \sum_{i=1}^{n} \hat{m}_i \left| \hat{m}_i^{-1} \right|_{m_i} \times R_i \right|_M \quad \text{, onde} \quad M = \prod_{i=1}^{n} m_i \qquad \hat{m}_i = M/m_i$$

$\left|\hat{m}_i^{-1}\right|_{m_i}$ represents the multiplicative inverse of $\hat{m}_i$ with respect to modulus m_i

b) Novo CRT-I:

$$X = \left| \sum_{i=1}^{n} |V_i R_i|_{\hat{m}_1} \right|_{\hat{m}_1} m_1 + R_1 \quad \text{, onde} \quad V_1 = \frac{\left|\hat{m}_1^{-1}\right|_{m_1} \hat{m}_1 - 1}{m_1}$$

$$V_i = \left|\hat{m}_i^{-1}\right|_{m_i} \frac{\hat{m}_i}{m_1} \quad \text{for} \quad 2 \le i \le n$$

PROBLEMAS

Problema 4.11. Considere o seguinte conjunto de módulos $\{2^n, 2^n-3, 2^n+3\}$, para n=4 e uma entrada-saída de $3n$ bit:

a) Obtenha a estrutura para fazer a conversão binário-RNS (use compressores e somadores modulo 13 e 19).

b) Obtenha a estrutura para fazer a conversão RNS-binário binário (use novo CRT-I, compressores e somadores módulo 247).

c) Indique a faixa dinâmica da estrutura RNS e compare com a eficiência da representação com binário.

Problema 4.12. Obtenha um conjunto modular válido com faixa dinâmica DR=[0, 1048576) e n=5 bits por canal (máximo):

a) Obtenha a estrutura para fazer a conversão binário-RNS.

b) Obtenha a estrutura para fazer a conversão RNS-binário.

c) Indique a faixa dinâmica da estrutura RNS e compare com a eficiência da representação com binário.