technology
from seed

Efficient Method for Magnitude Comparison in RNS Based on Two Pairs of Conjugate Moduli

Leonel Sousa

INSTITUTO SUPERIOR TÉCNICO

Outline

1. Motivation
2. Class of Moduli Sets
3. Method for comparing magnitude in RNS
4. Typical application: RNS motion estimator
5. Conclusions and future work

Motivation

technology
from seed

inesc id lisboa

- Carry free arithmetic
  - Residue Number Systems (RNS) allows to parallelize +, -, *
- No general efficient method for comparison in RNS
  - to convert from residues to positional code: CRT requires modulo M operations and MRC is a sequential method!
  - [Miller 86, Dimauro 93, Wang 99]: computationally demanding, not suitable for hardware implementation
- To propose a method for comparing RNS numbers considering a representative class of moduli sets.

Class of Moduli Sets

- New class of multi-moduli sets that rely on pairs of conjugate moduli:

  $$S = \{m_1, m_1^*, \ldots, m_k, m_k^*\} = \{2^{n1}-1, 2^{n1}+1, \ldots, 2^{nk}-1, 2^{nk}+1\}$$

  – Only Mersenne rings and Fermat rings

- S is not a set of pairwise relatively prime, however modified CRT [Wang98] allows to obtain an integer from residues

- This class of multi-moduli leads to two-level residue number systems

- Important sub-class S': two pairs of balanced conjugate moduli sets

$$S' = \{m_1, m_1^*, m_2, m_2^*\} = \{2^n-1, 2^n+1, 2^{n+1}-1, 2^{n+1}+1\}$$

Class of Moduli Sets

technology
from seed

inesc id lisboa

- For each of the two level we can use the modified CRT to compute RNS-to-binary

$$X = X_1 + m_1 \left\langle \left(\frac{m_1}{d}\right)^{-1} \frac{X_2 - X_1}{d} \right\rangle_{\frac{m_2}{d}}$$

  – d = GCD(m1,m2) ⇒ pairwise relatively prime CRTIII≡MRC

$$d = 1 \rightarrow X_1 = x_1^* + (2^n + 1)\left\langle 2^{n-1}(x_1 - x_1^*) \right\rangle_{2^{n-1}}$$

$$d = 3 \rightarrow X = X_2 + \left\langle \left(\frac{2^{2(n+1)} - 1}{3}\right)^{-1} \frac{X_1 - X_2}{3} \right\rangle_{\frac{2^{2n-1}}{3}}$$

- Very important for us is that the range is **odd**

$$M = \frac{(2^{2n} - 1)(2^{2n+2} - 1)}{3}$$

INSTITUTO SUPERIOR TÉCNICO

Comparing magnitude in RNS

- Unsigned integer numbers (*A,B)* can be compared by subtraction:

$$C = \begin{cases} A - B & \text{for } A \geq B \\ M - A - B & \text{for } A < B \end{cases}$$

- Based on the well known mathematical axiom:
  - *the subtraction of two numbers with the same parity leads to an even number and the subtraction of two numbers with different parities leads to an odd number*

- and taking advantage that M is **odd** we can answer the question :
  - is A ≥ B or not?

Comparing magnitude in RNS

- PREPOSITIONS

- $A \geq B$ *iff:*
  - A and B have the same parity and C is an even number
  - A and B have different parities but C is an odd number.

- $A < B$ *iff:*
  - A and B have the same parity and C is an odd number
  - A and B have different parities but C is an even number.

So we have to compute the parity of A, B and C!

Comparing magnitude in RNS

- Problem: how to directly compute the parity of a RNS number?
  - without computing the number back to a traditional weighted system!

- The parity of an integer X in the range [0, M−1] represented on the $\{2^n-1, 2^n+1, 2^{n+1}-1, 2^{n+1}+1\}$ moduli set can be computed by:

$$\langle X \rangle_2 = \left\langle \langle X_2 \rangle_2 \oplus \left\langle \langle X_1 - X_2 \rangle_{2^{2n-1}} \right\rangle_2 \right\rangle_2$$

- by converting X1 and X2 in the 1st-level we also just need shift and one's complement addition

$$X_1 = x_1^* + (2^n + 1) \times \left\langle 2^{n-1}(x_1 - x_1^*) \right\rangle_{2^n - 1}$$

$$X_2 = x_2^* + (2^{n+1} + 1) \times \left\langle (2^n(x_2 - x_2^*) \right\rangle_{2^{n+1} - 1}$$

Comparing magnitude in RNS

technology
from seed

inesc id lisboa

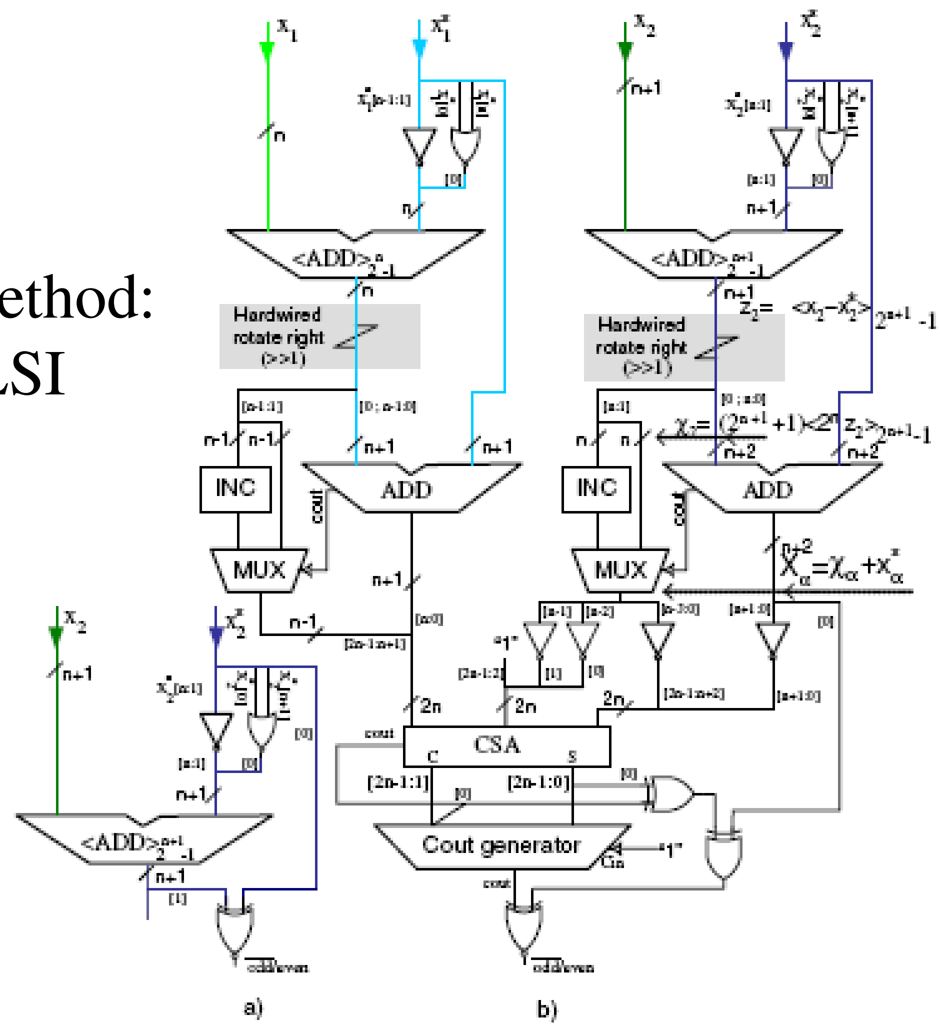
Algorithm 1 Comparison of the numbers A, B represented in RNS $(a_1, a_1^*, a_2, a_2^*, b_1, b_1^*, b_2, b_2^*)$.

$c_1 = \langle a_1 - b_1 \rangle_{2^n-1}; c_1^* = \langle a_1^* - b_1^* \rangle_{2^n+1};$
$c_2 = \langle a_2 - b_2 \rangle_{2^{n+1}-1}; c_2^* = \langle a_2^* - b_2^*; \rangle_{2^{n+1}+1};$
$(A_1, A_2) =$ 1st-level-converter(a_1, a_1^*, a_2, a_2^*); {(15) and (16)}
$(B_1, B_2) =$ 1st-level-converter(b_1, b_1^*, b_2, b_2^*); {(15) and (16)}
$(C_1, C_2) =$ 1st-level-converter(c_1, c_1^*, c_2, c_2^*); {(15) and (16)}
$\overline{P_A} = LSB(\langle A_1 - A_2 \rangle_{2^{2n}-1}) \oplus LSB(A2);$ {'1' if X even}
$\overline{P_B} = LSB(\langle B_1 - B_2 \rangle_{2^{2n}-1}) \oplus LSB(B2);$
$\overline{P_C} = LSB(\langle C_1 - C_2 \rangle_{2^{2n}-1}) \oplus LSB(C2);$
if $P_A \oplus P_B \oplus P_C =$ '1' **then**
  $A \geq B$ is TRUE;
else
  $A < B$ is TRUE;
end if

INSTITUTO SUPERIOR TÉCNICO

Comparing magnitude in RNS

Parity detection method: suitable for VLSI



INSTITUTO SUPERIOR TÉCNICO

Comparing magnitude in RNS

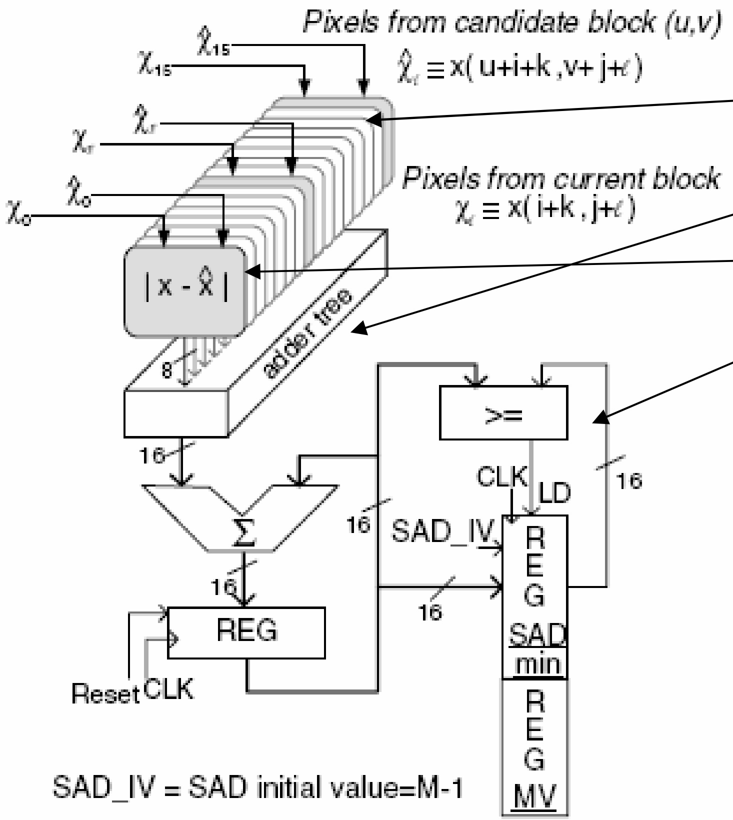
technology
from seed

inesc id lisboa

Maximum Operation Size (MOS)		
Algorithm	MOS (n,M)	MOS (n=4)
Miller	≅4M	≅86955
Dimauro	modulo(≅ 2^{3n}+2)	modulo(≅ 4098)
Wang	modulo(2^{2n}-1)	modulo(255)
Proposed	modulo(2^{n+1}+1)	modulo(33)

Typical application: RNS motion estimator

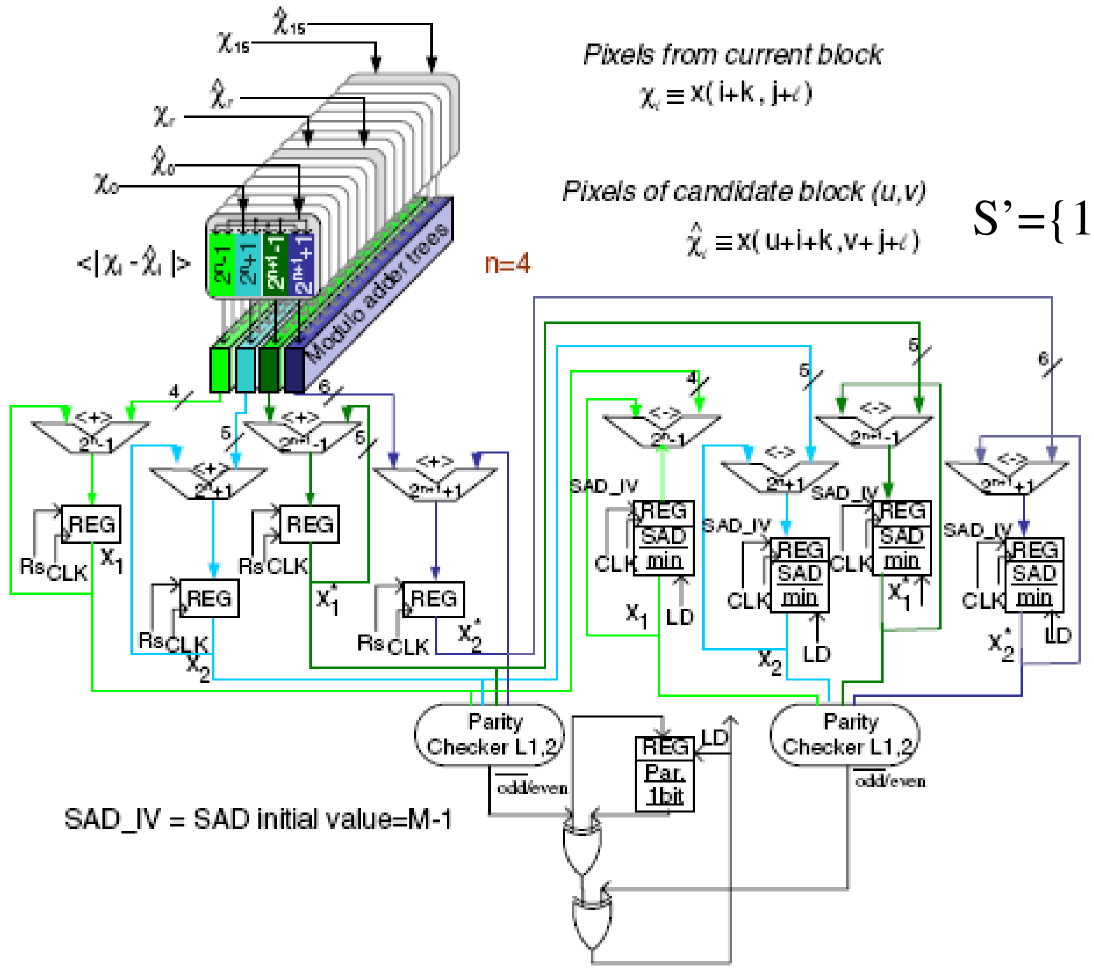
- Tradicional architecture



Subtractors and Adders

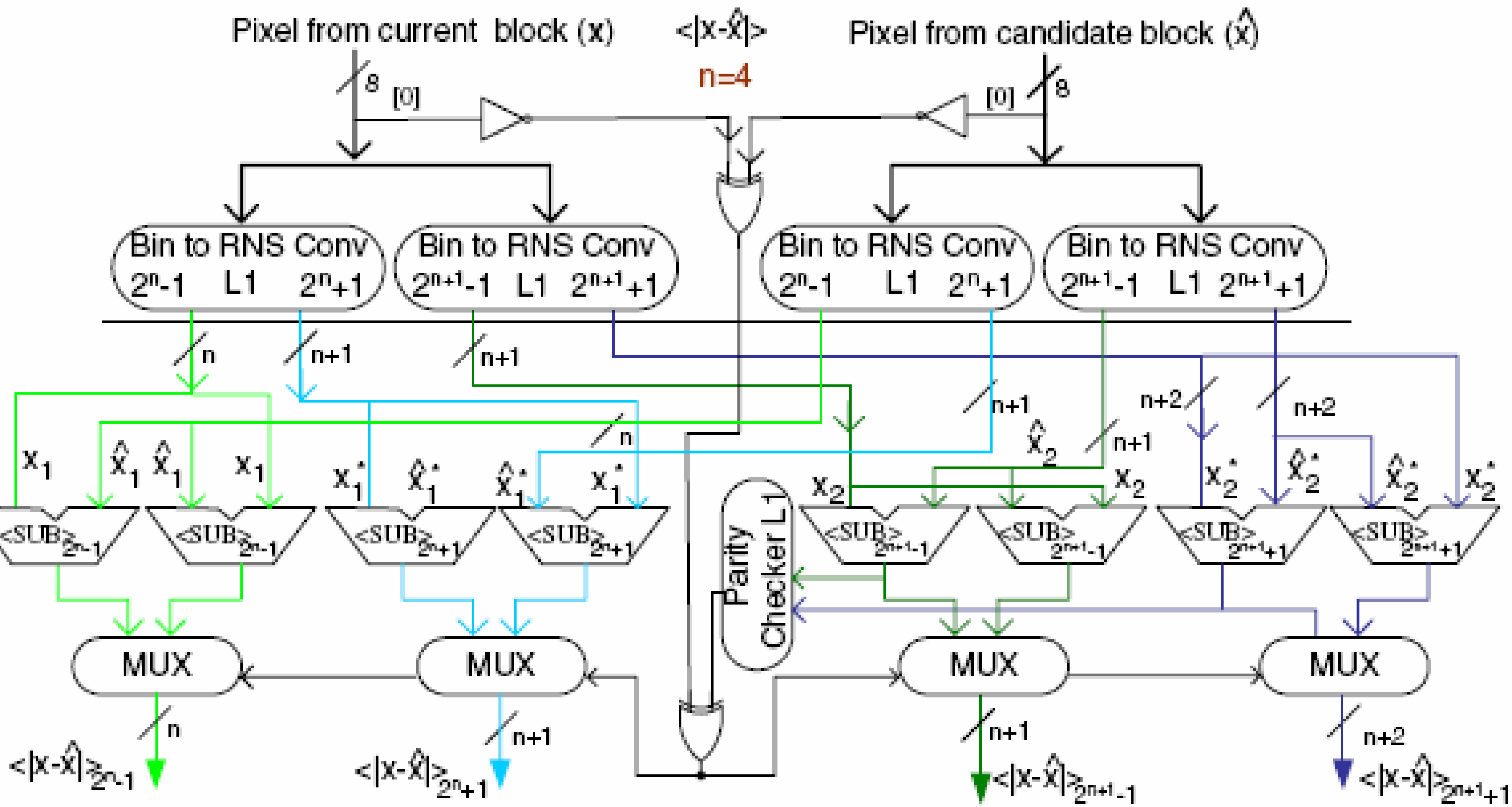
Comparators: proposed hardware

RNS motion estimator



S'={15,17,31,33}

RNS motion estimator



Experimental Results: RNS motion estimator

- SAD unit implemented in a FPGA with arithmetic units directly mapped on Look-Up-Tables (LUT)
- FPGA Xilinx VirtexII Pro (xc2vp50-7)
- Synthesis with ISE (8.2) tools

Slices (% total)	BRAMs (% total)	Freq. MHz	Latency Cycles	Throughput Blocks/s
246 (1%)	211 (90%)	254	12	1.5×10^7

Conclusions and future work

- New efficient method is proposed for magnitude comparison in RNS based on two pairs of conjugate moduli

- This is the first method leading to VLSI architectures with practical interest for comparing the magnitude of numbers in RNS
  - Efficient RNS minimum SAD unit was already implemented in FPGA
  - We are implementing a SAD unit on an ASIC (0.18μm CMOS)

- We are now extending the idea to other moduli sets, all with a common characteristic: M odd


technology
from seed
inesc id
lisboa