EE 486 lecture 4: Residue Arithmetic

M. J. Flynn

The Chinese Remainder theorem

- Given a set of relatively prime (r.p.) moduli (m_1,m_2,…m_n) then for any x < M the set of residues {Xmod m_i, i between 1and n} is unique, where $M = \Pi\ m_i$; i range is from 1 to n.

Residue operations

- (a op b) mod m = ((a mod m) op (b mod m)) mod m;
- for ops add, subtract (with complement adjustment) and multiply
- So "carry free" operation is possible where we concurrently execute i operations.
- But results must not exceed M

Subtraction and complementation

- Since residue is the least positive remainder, we use a complement representation.
- As before if we define the upper range of M/2 to M as the negative numbers we can affect subtraction.
- So that $\{[x_i^c]\}=\{[x_i]\}^c= X^c$
- Overflow detection remains a problem, both for r > M and for negative result assuming a positive representation.

RNS terminology

- For n moduli the ith residue is x_i =X mod m_i
- $X = [x_1, x_2, x_3]_{m1,m2,m3}$; where the m_i are relatively prime, eg , $9=[4,0,1]_{5,3,2}$
- Then [a] + [b] = [a + b], etc.

Moduli selection

- Considerations:
  - Relatively prime
  - Minimize maximum carry (the max modulus)
  - Efficiency (or capacity) of the representation in a fixed number of bits
  - Compatibility with binary (radix) ALUs.
- Two systems:
  - Optimal: minimizes the maximum modulus
  - Binary: binary efficient representation & ALU

Optimal RNS

- Goal: given M, find product of primes and *prime powers* to minimize (max m_i) and result is equal to or greater than M.
- 2x3x5 is not an optimal sequence since any power of 2 (eg, 4) must be r.p. to 3 and smaller than 5…so 4x3x5 is an optimal sequence… 4x3x5x7; 3x5x7x8; 5x7x8x9 are sample optimal sequences.
- Max $\{m_i\} = \alpha(M)$; the alpha function.

Conversion into RNS

- Table based, using $(x_i \beta^i)$ as entry into a table of size β. Then sum the results mod m_i, again using tables for determining the sums.

Binary (or Merrill) RNS

- Binary ALU compatible and bit efficient
- Select mods of the form 2^n (largest) and others of the form $2^k - 1$; $k_1 = n$; then select k_2, etc. to be r.p. and provide capacity M.
- Advantages:
  - Easy, use binary type ALUs with "end around" carry.
  - "Almost" the capacity of 2^p where $n + \Sigma k_i = p$

Merrill mods

Modulus	Prime factors
3	Prime
7	Prime
15	3,5
31	Prime
63	3,7
127	Prime
255	3,5
511	7,73

Some sample Merrill mod sets

Bits to represent	Moduli set
17	32,31,15,7
25	128,127,63,31
28	256,255,127,31

Binary to binary RNS conversion

- X mod 2^n is just the low order n bits of X
- X mod 2^k-1 is the sum of the k bit digits of X, again mod 2^k with $r = 2^k - 1$ set to 0
- X mod $2^k - 1 = \Sigma (x_i \beta^i)$ mod $2^k - 1$ but βmod $2^k - 1 = 1$ since $\beta = 2^k$ and β^i mod$2^k - 1 = 1$, so $(x_i \beta^i)$ mod $2^k - 1 = x_i$

Conversion out of RNS

- For each modulus, i , find w_i the wpns number that has an rns with 1 in the ith position and 0 elsewhere, w_i=[0,0,1,0]
- Then X mod M = $(\Sigma (w_i\, x_i))$ mod M

RSN difficulties

- Conversion back into binary
- Compares
- Overflows (r > M)
- Subtractive overflows
- Division

RNS as an arithmetic check

- Residue check based on computation of k – bit check digit
- A mod 2^k-1 =[a] = $(\Sigma\, a_i)$ mod 2^k-1
- A + B = C must correspond to [a]+[b]=[c]
- Sum of the residues equal the residue of the sum.
- Usually k= 3,4 or 5.

Optimal RNS

- Basis for bounds on add and multiply
- If we keep the largest modulus to a minimum then the carry propagation will also be minimized.