北海道大学工学部研究報告
第135号（昭和62年）

Bulletin of the Faculty of Engineering,
Hokkaido University. No. 135 (1987)

中国人の剰余定理を用いた新しい剰余数の逆変換法

三関　公生*　北島　秀夫*
下野　哲雄*　小川　吉彦*

（昭和61年12月27日受理）

A New Residue Decoding Technique Using Chinese Remainder Theorem

Kimio MISEKI, Hideo KITAJIMA, Tetsuo SHIMONO,
Yoshihiko OGAWA

(Received December 27, 1986)

Abstract

A new technique for converting the RNS (residue number system) to binary is proposed. Although the basic algorithm is a form of the CRT (Chinese remainder theorem), the technique is unique in that it can be used in finding the value of the integer function P without a base extension operation. In this paper, we restrict the moduli used as $m_i \leqq 32$ for high-speed computation of ROM table look-up method. Sign detection is readily achieved in 2's complement by adopting the symmetric residue representation and using mod 2^k adder in place of mod M adder. In spite of the CRT algorithm, this method can be applied to a large number of small moduli RNS ($n \leqq 10$). Therefore we can expand the dynamic range in the RNS even when high-speed processing is required. Applied to a scaler in RNS recursive filtering, its throughput is insensitive to the increase of the number of the moduli. With our method, RNS table look-up recursive digital filter with a high-speed and high-precision performance will be realized.

1. 序　　論

剰余数系 (Residue Number System : RNS) は理論的に完全に並列で高精度な算術演算能力を持つために，1960年代の初頭から数多くの論文で，高速計算機への応用と実現のための問題点について議論されてきた[1)-11)] etc.。この分野に於ていまだに中心となる問題点はスケーリングとRNSから2進数への高速変換である。この問題の解決なしにはRNSの持つ魅力も半減してしまうであろう。

現在，一般的にRNSの応用が考えられているのはディジタルフィルタリングと数論変換によるコンボリューションである。特に前者に関する論文の増加は外国論文誌に於て近年著しい。非回

*電子工学科　電子回路工学講座

帰形フィルタについては，一般にフィルタの出力精度は入力の精度と同程度でよいことを考慮に入れた場合，パイプライン化したROM (Read Only Memory) table-look-up法を用いて10～100 MHz程度の高いサンプリング・レイトの実現が報告されている[11]。一方RNS回帰形フィルタの高速化は非回帰形フィルタほど簡単にはいかない。何故なら回帰形フィルタにはその名の通り帰還部があるのでスケーリングは不可欠であり[3)4)]，scalerでの遅れが直接サンプリング・レイトの低下につながるからである。RNSは有限環であるからRNS内ではスケーリング（固定定数割り算）は不可能である。従って，スケーリングは一時的にでもRNSから普通の数に戻して行わなければならない。結局，スケーリングを高速に行うことはRNSから2進数への変換を高速に行うことに帰する。

RNSから普通の数への変換アルゴリズムには中国人の剰余定理(Chinese remainder theorem : CRT)[2)-7)] と mixed radix conversion (MRC)[5)8)-10)] の二つがよく知られている。どちらのアルゴリズムを使うかは，実際に使用する法 m_i の個数と大きさに依存する。例えば，法 m_i の大きさがROM table-look-upに適した大きさ（$m_i \leqq 32$）で，法の個数が4以内であればスループットやtableの個数の点でMRCはCRTに及ばないであろう。しかし上述の条件が満されない多くの場合は，CRTを諦めてMRCを使わざるを得ないのが実状である。

スケーリングについてはCRTタイプのJenkinsのスケーリング[3)4)]が簡単で注目に値するが，2個から4個の特別な法についてのみ有効な方法であり，さらにbase extension[1)]を必要とすること，スケール・ファクタを特定の法の積にとらなければならないなど制限が厳しい。一方，MRCタイプのものには大きな3個の法の組 $\{2^n+1, 2^n, 2^n-1\}$ 用のTaylorのauto scale[9)]や，table look-up法によるMillerとPolkyのスケーリング[10)]があるが，MRCの構造からスループットが低くなることは避けられず，文献[10)]の場合には法の個数が多くなるとROM tableが急激に増えるため経済的ではない。

本論文はこれらの現状を踏まえた上で，table-look-up法を用いたRNS-to-binary converterとRNS回帰形フィルタのscalerに対する一つの解答を与える。また，これまでMRCのみで可能であった2進数出力の符号検出 (sign detection) がCRTタイプである本手法で簡単に行えることを示す。

2. 剰 余 数 系

RNSは整数値を扱うシステムなので，以下の議論で現れる文字変数は特にことわらない限りすべて整数を表すことにする。

剰余数系（以後RNSと略す）はn個の互いに素な数 $m_1, m_2, \cdots, m_n$（RNSの法）により構成される。あるダイナミックレンジ内の任意の数Xはn個の法 m_i（$i=1, \cdots, n$）のそれぞれの剰余（residue）によって一意に表現され，これをXのRNS表現という。

$$X=(x_1, x_2, \cdots, x_n) \tag{1}$$

$$x_i=\langle X\rangle_{m_i}=X \bmod m_i \tag{2}$$

$$\langle X\rangle_{m_i}\in\begin{cases}[-(m_i-1)/2,\ (m_i-1)/2] & (m_i\text{: 奇数})\\ [-m_i/2,\ m_i/2-1] & (m_i\text{: 偶数})\end{cases} \tag{3}$$

記号 $\langle X\rangle_{m_i}$ はXの法 m_i に関するsymmetric residueと呼ぶ。ダイナミックレンジは普通(5)のようにとることが多い。

$$M=\prod_{i=1}^{n} m_i \tag{4}$$

$$X\in\begin{cases}[-(M-1)/2,\ (M-1)/2] & (M：奇数)\\ [-M/2,\ M/2-1] & (M：偶数)\end{cases} \tag{5}$$

Xは一たびRNS表現されると非常に扱いやすくなる。何故なら一般に$x_i \ll X$であり，しかも割り算を除く演算が法ごとに独立に行えるからである。つまり，

$$X\circ Y=(<x_1\circ y_1>_{m_1},\ <x_2\circ y_2>_{m_2},\ \cdots,\ <x_n\circ y_n>_{m_n}) \tag{6}$$

記号○は加算，減算および乗算を表している。ここで注意しなければならないのはRNS内のすべての演算はMを法とする剰余環内で定義されていることである。

3. S−CRTによるデコーディング

3.1 原　　理

いまn個のRNSの法$m_1, \cdots, m_n$に対しYが(7)で与えられているとする。

$$Y=(y_1,\ y_2,\ \cdots,\ y_n) \tag{7}$$

Yを普通の数に戻すためにCRTを用いる。CRTはsymmetric residue表現を使っても非負値の剰余を用いる場合と同じ形式を有する：

$$Y=<\sum_{i=1}^{n} M_i<M_i^{-1}\cdot y_i>_{m_i}>_M \tag{8}$$

ここで$M_i=M/m_i$，$<M_i\cdot M_i^{-1}>_{m_i}=1$である。(5)と同様に正しいYが得られる範囲は(9)となる。

$$Y\in\begin{cases}[-(M-1)/2,\ (M-1)/2] & (M：奇数)\\ [-M/2,\ M/2-1] & (M：偶数)\end{cases} \tag{9}$$

(8)は(10)の形に書き換えることができる。

$$Y=\sum_{i=1}^{n} M_i<M_i^{-1}\cdot y_i>_{m_i}-P(Y)\cdot M \tag{10}$$

P(Y)はRNSの法が決まっていればYの値で決まる整数関数である。ここで(8)と(10)の違いについて述べておこう。(8)から得られるYは明らかに(9)の範囲内の値である。つまりYは剰余環R(M)の上から出ることはできない。一方(10)はまだmod Mの概念を式の中に残してはいるが，P(Y)の値の制限がなければYは自由に(9)の範囲を逸脱することができる。この意味で(8)と(10)の関係は

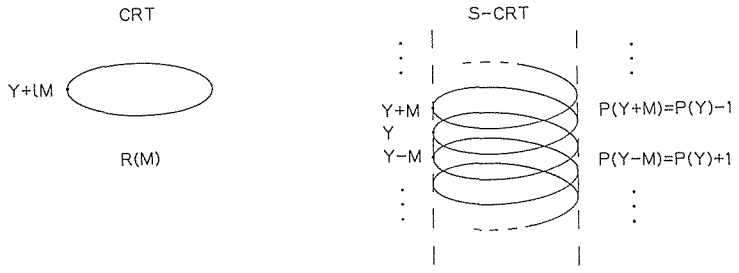

図1(a)　概　念　図

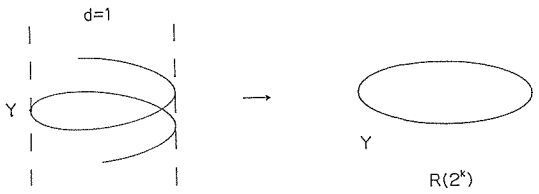

図1(b)　S−CRTによる逆変換

概念上，環 (ring) とそれと同じ半径（と呼べるものがあるなら）の無限に続くらせん (spiral) の関係に似ている（図1(a)）。よって以後(10)のような表現形式を spiral Chinese remainder theorem (S-CRT) と呼ぶ。

いま(9)を満たすYに対して(10)からP(Y)の範囲を求めると(11)になる。

$$\begin{cases} -(n-1)/2 \leqq P(Y) \leqq (n-1)/2 & (n：奇数) \\ -n/2 \leqq P(Y) \leqq n/2 & (n：偶数) \end{cases} \quad (11)$$

nはRNSの法の個数である。(11)からS-CRTのP(Y)の範囲は法の大きさに無関係で，法の個数にのみ依存することがわかる。ここで(11)の範囲のP(Y)の値を求めるために，条件(12)を満たすような新なる法m_pを導入する。

$$(M,m_p)=1, \begin{cases} m_p \geqq n & (n：奇数) \\ m_p \geqq n+1 & (n：偶数) \end{cases} \quad (12)$$

このm_pに対し(11)から$P(Y)=<P(Y)>_{m_p}$となることは明らかである。よってS-CRTからP(Y)は

$$P(Y)=<\sum_{i=1}^{n} <<m_i^{-1}>_{m_p} \cdot <M_i^{-1} \cdot y_i>_{m_i}>_{m_p} + <<-M^{-1}>_{m_p} \cdot <Y>_{m_p}>_{m_p}>_{m_p} \quad (13)$$

と表すことができる。$<Y>_{m_p}=y_p$はm_pを初めからRNSの法の他に加えておいて(13)で使うときだけ他の法と異なる役割をするように決めておけばbase extension[1]の必要なく簡単に得られる。従ってYのRNS表現(7)は(14)のように書き換えられる。

$$Y=(y_1, y_2, \cdots, y_n, y_p) \quad (14)$$

m_pはRNSの法として数えないことにする。いま$2 \leqq n \leqq 14$とすると，(12)から$3 \leqq m_p \leqq 15$と選ぶことは多くの場合やさしい。m_pが4ビット以下であるので(13)のP(Y)はROM table-look-upで高速に求めることができる。

実用上(12)によるm_pの選択の自由度はかなり大きいことが予想される。ここで，選択したm_pとダイナミックレンジの関係として重要である次の基本事項を記しておく。

[基本事項1]

(12)を満たすm_pに対するダイナミックレンジの倍率をdとすると，

$$d=\begin{cases} 2\left[\frac{m_p-n}{2}\right]+1 & (n：奇数) \\ 2\left[\frac{m_p-n-1}{2}\right]+1 & (n：偶数) \end{cases} \quad (15.a)$$

ここで式の［ ］はガウスの記号を表す。dによってダイナミックレンジは，

$$Y \in \begin{cases} [-(Md-1)/2, (Md-1)/2] & (M：奇数) \\ [-Md/2, Md/2-1] & (M：偶数) \end{cases} \quad (15.b)$$

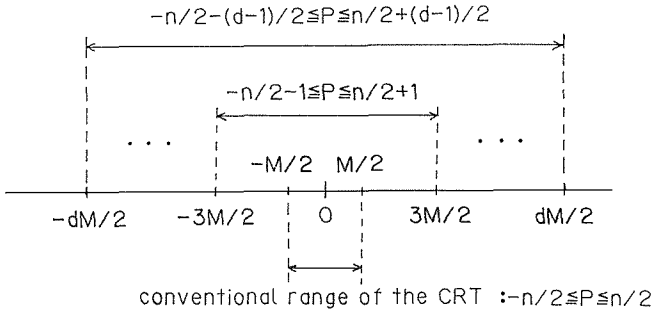

図2 ダイナミックレンジとPの関係

となる。このことはS-CRTのP(Y)の性質$P(Y\pm\ell M)=P(Y)\pm\ell$と図2から明らかである。

現在多くのディジタル回路は2進数に対応しているため，例えばn=5のときm_pとして5を選んでも7を選んでも$<\ >_{m_p}$の表現には3ビット必要なことには変りない。しかし，(15. b)から$m_p=7$と選ぶとd=3となり，大きい方の数を選んだ分の見返りとして$m_p=5$とした場合の3倍のダイナミックレンジが具体的な量として得られることがわかる。

(13)よりP(Y)が得られればあとはmod 2^k adderで(17)からYが簡単に得られる。ここでkは，

$$2^{k-1}<Md<2^k \tag{16}$$

を満たす数である。(15. b)と(16)より　$Y=<Y>_{Md}=<Y>_{2^k}$であるから

$$Y=<\sum_{i=1}^{n}<M_i<M_i^{-1}\cdot y_i>_{m_i}>_{2^k}+<-P(Y)\cdot M>_{2^k}>_{2^k} \tag{17}$$

ただし(17)の$<M_i<M_i^{-1}\cdot y_i>_{m_i}>_{2^k}$および$<-P(Y)\cdot M>_{2^k}$はtableによって与えられる。Yの負数は2の補数で自動的に表されるので符号検出のために特別な注意は必要ない。

以上のRNSから2進数への変換の概念は図1(a)の無限長らせんから条件(12)によりレンジ(15. b)を十分満たす分のらせんを切りとり，(16)を満たす2^kの剰余環$R(2^k)$により（15. b）の範囲の数Yを表すことに対応する（図1(b)）。

図3に本手法によるRNS-to-binary converterの基本構成を示す。ここまではconverterの処理速度については何も考えていない。4章で述べるスケーリングを行って出力の精度を入力の精度と同程度に落すことによりk>k′なるmod $2^{k'}$ adderでconverterは高速化されることになる。

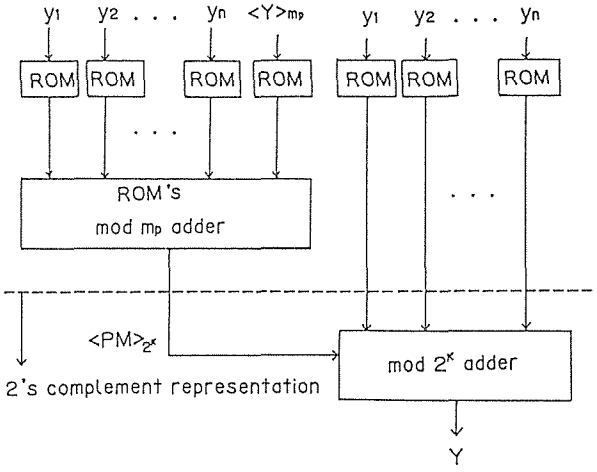

図3　RNS-to-binary converterの基本構成

3.2　table-look-up用のS-CRT

3.1に於て基本原理を示した。CRTアルゴリズムを使って高速にRNSから2進数に変換することが必要なときは必ずROM tableが使用されるであろう。何故ならCRTの性質から一つの法m_iに関する入力y_iの重みは複雑であるが他の入力に無関係にy_iのみの値で決まるからである。この事実は3.1の手法にさらに好ましい結果を与えることになる。この節ではtable-look-up用に改良したS-CRTについて考察する。

剰余環R(M)はMの因数である法m_i (i=1, ..., n)の組み合わせにより様々な同形関係（≅）を持つ。

$$
\begin{aligned}
R(M) = \; & R(m_1\, m_2 \cdots\cdots m_n) \\
\cong \; & R(m_1) \oplus R(m_2) \oplus \cdots\cdots \oplus R(m_n) \qquad (18.\,a) \\
\cong \; & \begin{cases} R(m_1\, m_2) \oplus R(m_3\, m_4) \oplus \cdots\cdots \oplus R(m_{n-1}\, m_n) & (n:\text{偶数}) \\ R(m_1\, m_2) \oplus R(m_3\, m_4) \oplus \cdots\cdots \oplus R(m_{n-2}\, m_{n-1}) \oplus R(m_n) & (n:\text{奇数}) \end{cases} \qquad (18.\,b) \\
\vdots & \\
\cong \; & R(m_1\, m_2 \cdots\cdots m_{n-1}) \oplus R(m_n) \quad \text{etc.}
\end{aligned}
$$

これらはそれぞれがRNSを作ることができ，その法の個数は環の個数に一致する。もし(18.b)のRNSをS-CRTに利用できれば法の個数nは明らかに約半分にできる。その手順は，

ⅰ） CRTにより（18. a）から例えば（18. b）のRNSを得る。

ⅱ） （18. b）のRNSに対しS-CRTを用いる。

ⅰ）ⅱ）の操作は（19. a）（19. b）で表される。ただし，ここではnが偶数であるとして表記を簡単にした。

$$y_{2i-1,\,2i} \triangleq \langle m_{2i} \langle m_{2i}^{-1} \cdot y_{2i-1} \rangle_{m_{2i-1}} + m_{2i-1} \langle m_{2i-1}^{-1}\, y_{2i} \rangle_{m_{2i}} \rangle_{m_{2i-1}\, m_{2i}} \qquad (19.\,a)$$

$$Y = \sum_{i=1}^{n/2} M_{2j-1,\,2i} \langle M_{2i-1,\,2i}^{-1} \cdot y_{2i-1,2i} \rangle_{m_{2i-1}\, m_{2i}} - \hat{P}(Y) \cdot M \qquad (19.\,b)$$

$$M_{i,j} \triangleq M/(m_i\, m_j) \qquad (19.\,c)$$

(19. b）の$\hat{P}(Y)$は⑽の$P(Y)$と違う整数関数なのでハットをつけて区別する。$\hat{P}(Y)$を求めるための⑿に対応する$m_{\hat{p}}$の条件は⑳となり，⒀⒂はそれぞれ㉑㉒となる。

$$(M,\, m_{\hat{p}}) = 1, \quad \begin{cases} m_{\hat{p}} \geqq \left[\dfrac{n+1}{2} \right] & (n=4t-2,\ 4t+1) \\ m_{\hat{p}} \geqq \left[\dfrac{n+1}{2} \right] + 1 & (n=4t-1,\ 4t) \end{cases} \qquad ⑳$$

$$\hat{P}(Y) = \left\langle \sum_{i=1}^{n/2} \langle\langle (m_{2i-1}\, m_{2i})^{-1} \rangle_{m_{\hat{p}}} \cdot \langle M_{2i-1,\,2i}^{-1} \cdot Y_{2i-1,\,2i} \rangle_{m_{2i-1}\, m_{2i}} \rangle_{m_{\hat{p}}} \right.$$

$$\left. + \langle\langle (-M)^{-1} \rangle_{m_{\hat{p}}} \cdot \langle Y \rangle_{m_{\hat{p}}} \rangle_{m_{\hat{p}}} \right\rangle_{m_{\hat{p}}} \qquad ㉑$$

［基本事項２］

$$\hat{d} \triangleq \begin{cases} 2\left[\dfrac{1}{2} \left(m_{\hat{p}} - \left[\dfrac{n+1}{2} \right] \right) \right] + 1 & (n=4t-2,\ 4t+1) \\ 2\left[\dfrac{1}{2} \left(m_{\hat{p}} - \left[\dfrac{n+1}{2} \right] - 1 \right) \right] + 1 & (n=4t-1,\ 4t) \end{cases} \qquad (22.\,a)$$

$$Y \in \begin{cases} \left[-\dfrac{M\hat{d}-1}{2},\ \dfrac{M\hat{d}-1}{2} \right] & (M:\text{奇数}) \\ \left[-\dfrac{M}{2}\hat{d},\ \dfrac{M}{2}\hat{d}-1 \right] & (M:\text{偶数}) \end{cases} \qquad (22.\,b)$$

幸運なことにⅰ）ⅱ）の操作は一回のROM table look-upで行うことができる（図4）。さらにこの方法はスケーリングによるエラーも減少させることになる。

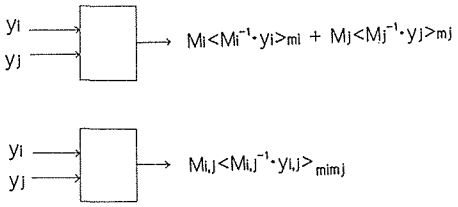

図4　table-look-up 法における二つの手法の違い（上：従来の手法）

4. スケーリング

4.1 RNSから2進数への変換のためのスケーリング

CRTタイプのスケーリングとして知られているJenkinsによるスケーリング[3)4)]はS-CRTに非常に適している。何故ならこのスケーリングはS-CRTのP(Y)および$\hat{P}(Y)$に影響を与えないからである。つまり，(10)(19)はそれぞれ（23. a）（24. a）とできる。

$$Y/S \simeq Y_s \triangleq \sum_{i=1}^{n} \left[\frac{M_i}{S} <M_i^{-1} \cdot y_i>_{m_i} \right]_r + \left[-P(Y) \frac{M}{S} \right]_r \tag{23. a}$$

$$\left| Y/S - Y_s \right| \leqq \frac{1}{2}(n+1) \tag{23. b}$$

$$Y/S \simeq \hat{Y}_s \triangleq \begin{cases} \sum_{i=1}^{n/2} \left[\frac{M_{2i-1,2i}}{S} <M_{2i-1,2i}^{-1} \cdot y_{2i-1,2i}>_{m_{2i-1}m_{2i}} \right]_r \\ \qquad + \left[-\hat{P}(Y) \frac{M}{S} \right]_r \qquad (n：偶数) \\ \sum_{i=1}^{(n-1)/2} \left[\frac{M_{2i-1,2i}}{S} <M_{2i-1,2i}^{-1} \cdot y_{2i-1,2i}>_{m_{2i-1}m_{2i}} \right]_r \\ \qquad + \left[\frac{M_n}{S} <M_n^{-1} \cdot y_n>_{m_n} \right]_r + \left[-\hat{P}(Y) \frac{M}{S} \right]_r \qquad (n：奇数) \end{cases} \tag{24. a}$$

$$\left| Y/S - \hat{Y}_s \right| \leqq \frac{1}{2} \left\{ \left[\frac{n+1}{2} \right] + 1 \right\} \tag{24. b}$$

$[\ ]_r$は内の数を整数値にまるめることを意味する。Sは任意のスケール・ファクタである。(23.b)と（24. b）からn≧2のときは(24)の方法の方がスケーリングエラーが小さいことがわかる。また，m_pや$m_{\hat{p}}$が条件(12)(20)を満していれば(13)および(21)によって正しいP(Y)または$\hat{P}(Y)$が得られるので，少なくとも(15)または(22)の範囲内のYに対してスケーリングを行っても符号の逆転という重大なスケーリングエラー(polarity error[3)4)])は生じない。

Y_sや$\hat{Y}_s$は必要な出力ビット数k′が与えられていれば，$2^{k'-1} < (Md/S) < 2^{k'}$または$2^{k'-1} < (M\hat{d}/S) < 2^{k'}$を満たすスケール・ファクタSを定めると，前の(17)と同様にしてmod $2^{k'}$ adderで求めることができる。図5はn≦10, $m_{\hat{p}}=7$としたときのRNS-to-binary converterの構成を示したものである。（24. b）のスケーリングエラーは文献10）のエラー補償を利用すれば，図5の$\hat{Y}_s$に於て1/2+5/16以下にできる。いま簡単のためnを偶数とすると，まるめによる各tableのエラーは，

$$\delta_{2i-1,2i} \triangleq \frac{M_{2i-1,2i}}{S} <M_{2i-1,2i}^{-1} \cdot y_{2i-1,2i}>_{m_{2i-1}m_{2i}} - \left[\frac{M_{2i-1,2i}}{S} <M_{2i-1,2i}^{-1} \cdot y_{2i-1,2i}>_{m_{2i-1}m_{2i}} \right]_r, \quad i=1,\cdots,\frac{n}{2} \tag{25}$$

よって $\delta_{2i-1,\,2i} \in [-1/2,\ 1/2]$ である。いま $\hat{P}$ generator の第一段目の table の使用されていない3ビットの出力で値 $\{\pm 1/16,\ \pm 3/16,\ \pm 5/16,\ \pm 7/16\}$ を表すことにする。$\delta_{2i-1,\,2i}$ に最も近いものを $\delta_{2i-1,\,2i}$ として割り当てれば，3ビットの $\delta_{2i-1,\,2i}$ に含まれるエラーは 1/16 を超えない。あとは table look-up で $\Sigma\delta$ のうち必要なビット数だけを $\hat{P}$ generator へ渡すことによりエラーが補償される。しかしエラーの補償は RNS フィルタではそんなに重要なことではないように思われる。何故なら変換前の実際にフィルタリングを行う部分で RNS に於て非常に精度の高い（非回帰形なら誤差は0）演算が行われるので，$\hat{Y}_s$ を k′ ビットに制限することは converter の入力（フィルタの出力）Y に少し大きめの量子化誤差を加える程度の意味しかないからである。もちろん k′ の値はこの量子化誤差（24. b）が気にならない程度に大きくとってある場合の話である。

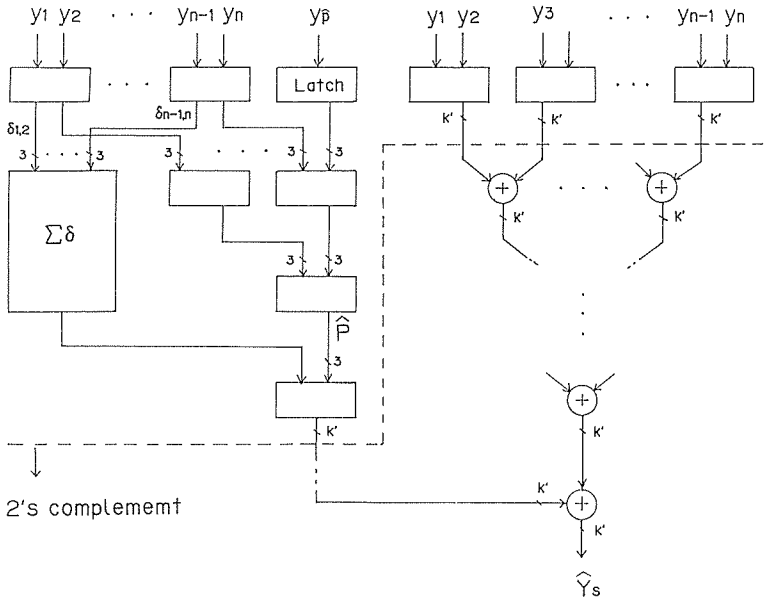

図5　$n \leqq 10$, $m_{\hat{p}} = 7$ のときの RNS-to-binary converter

4.2　回帰形フィルタのためのスケーリング

回帰形のフィルタリングを高速に行うためには，scaler に於て Y_s や $\hat{Y}_s$ よりむしろ $<Y_s>_{m_j}$ や $<\hat{Y}_s>_{m_j}$ が先に求められることが望ましい。いま $m_{\hat{p}}$ を使うことにする。n が偶数とすると (24.a) から直接 $<\hat{Y}_s>_{m_j}$ は，

$$<\hat{Y}_s>_{m_j} = <\sum_{i=1}^{n/2} <\left[\frac{M_{2i-1,\,2i}}{S} < M_{2i-1,\,2i}^{-1} \cdot y_{2i-1,\,2i} >_{m_{2i-1}\,m_{2i}}\right]_r >_{m_j}$$

$$+ <\left[-\hat{P}(Y)\frac{M}{S}\right]_r >_{m_j} >_{m_j},\ j=1,\ \cdots\cdots,\ n,\ \hat{p} \qquad (26)$$

(21)と(26)から table look-up で求められる。(26)からわかるように scaler は各法に対して一つずつ必要であることに注意してもらいたい。このためのハードウエアの増大が RNS の欠点の一つであり，RNS 回帰形フィルタの実現を難しくしている。しかし本手法(26)は scaler に必要な table 数が可能な限り少なくなっていることが図6から見てとれる。ここで使用される table は 1K×8 ビットの ROM とする。また，$m_{\hat{p}}$ は3ビットしか必要ないのでどれか一つの法の scaler の一部と $\hat{P}$

generator を組み合わせることにより $\hat{P}$ を求めるための table 数を節約できる。$\hat{P}$ generator は法の個数に関係なくただ一つでよいことに注意してほしい。

表 1 に $m_i \leqq 32$, $2 \leqq n \leqq 10$ の法に対する本手法による scaler の性能を示す。条件(20)から $n \leqq 14$ について $m_{\hat{p}} \leqq 7$ と選べるが，ここでは $m_i \leqq 32$ と制限したため n=10 で法の候補をすべて使い尽すことがわかる。n=7～10 については $m_{\hat{p}}$ を 5 から 7 に変えて 3 ビットを有効に使うことによる効果と 25 が法として使えるようになったことで約 2.1～3.4 ビットダイナミックレンジの増加が見られる。scaler の性能の重要な指標である table-look-up cycle 数（throughput に反比例すると考えてよい）は n=7～10 で MRC の約半分に減っている。一方，scaler の一部と組み合わせることによって $\hat{P}$ generater で必要な table 数はせいぜい 3 個になる。またスケーリングエラーの値が適当か判断するための指標として SNR を $20 \log_{10} \{M\hat{d}/([(n+1)/2]+1)\}$ で定義した。

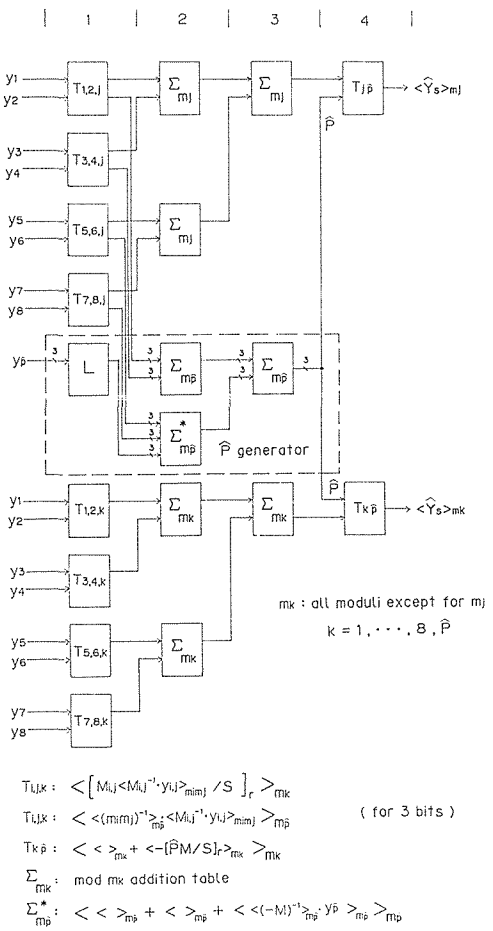

図 6　n=8，$m_{\hat{p}}=7$ のときの scaler

前に述べたことだが，法 $m_{\hat{p}}$ は scaler やデコーダ以外の処理では他の RNS の法と全く同様に機能しなければならない。従って，他の法と $m_{\hat{p}}$ を役割上交換をしてもハードウエアは $\hat{P}$ generator しか変らない。$m_{\hat{p}}$ を他の大きな法と交換して table の増加があるとしても，それは $\hat{P}$ generator 中のわずかなものである。表 2 には表 1 と比較するために，表 1 で用いた法と同じものを用いて $m_{\hat{p}}=31$ としたときの各項目への影響を調べたものを示した。ダイナミックレンジ拡大という点から見れば明らかに $m_{\hat{p}}$ は大きな数のほうが望ましいことがわかる。予想された $\hat{P}$ generator の table の増加は 1～2 個であるのに対し，ダイナミックレンジの増加は n=3～6 で約 1.5 ビット，n=7～10 で約 1 ビットある。しかし n=8 の場合のように table-look-up cycle 数が増えてしまっては何もならないので，一概に $m_{\hat{p}}$ が大きければよいとはいえない。

表 3 は table-look-up 法でスケーリングをする方法のうち，広いダイナミックレンジを扱うことのできる従来の MRC と * 印で表した Miller と Polky の MRC[10]，提案した S-CRT と * * 印の table-look-up 用の S-CRT を比較したものである。S-CRT のスケーリングエラーは MRC のそれよりも大きいが，それ以外の項目では圧倒的に S-CRT のほうが優れていることがわかる。scaler に於て特に多く使用される ROM table の個数で経済性を比較すると，

n	RNSの法の例	$\hat{d}$	$m_{\hat{p}}$	ﾀﾞｲﾅﾐｯｸﾚﾝｼﾞ (bit)	table lookup cycle 数	table数/n+1	$\hat{p}$ 発生器 table 数	SNR (dB)
2	32,31		1	9.95	1	1	0	
3	32,31,29	1	3	14.81	3	4	1	79.6
4	32,31,29,25	1	3	19.46	3	4	1	107.6
5	32,31,29,25,23	1	3	23.98	4	6	1	132.3
6	32,31,29,25,23,19	1	3	28.23	4	6	1	157.9
7	32,31,29,27,23,19,17	1	5	32.43	4	8	3	181.3
	32,31,29,27,25,23,19	3	7	34.58	4	8	3	194.2
8	32,31,29,27,23,19,17,13	1	5	36.13	4	8	3	203.5
	32,31,29,27,25,23,19,17	3	7	38.65	4	8	3	218.7
9	32,31,29,27,23,19,17,13,11	1	5	39.59	5	10	3	222.8
	32,31,29,27,25,23,19,17,13	3	7	42.36	5	10	3	239.5
10	32,31,29,27,23,19,17,13,11,7	1	5	42.39	5	10	3	239.7
	32,31,29,27,25,23,19,17,13,11	3	7	45.81	5	10	3	260.2
11 ・ ・ ・ 14	候補無し	1 ・ ・ ・ 1	7 ・ ・ ・ 7					

表1 scaler performance

$$\frac{\text{S-CRT(table数)}}{\text{MRC (table数)}} \simeq \begin{cases} \dfrac{2(n+1)}{n^2} & (n：奇数) \\ \dfrac{2}{n} & (n：偶数) \end{cases} \tag{27}$$

となり，例えばn=8のときtable数はMRCで288個であるのに対し，S-CRTでは$m_{\hat{p}}$も加えた法の個数が9であるにもかかわらず72個で済む。

しかしS-CRTによる方法はscaler以外の部分でmod $m_{\hat{p}}$の分のtableが必要なことを忘れてはならない。ただ$m_{\hat{p}}$が3ビット程度しかないことや回帰形フィルタでは非回帰形フィルタほど高次のものが必要ないことを考慮に入れると，法$m_{\hat{p}}$によるscaler以外の部分でのコストはあまり重大なものにはならない。

n	RNSの法の例	$\hat{d}$	$m_{\hat{p}}$	ﾀﾞｲﾅﾐｯｸﾚﾝｼﾞ (bit)	table lookup cycle数	table数/n+1	$\hat{p}$発生器table数	SNR (dB)
3	32,29,3	29	31	16.30	3	4	1	88.6
4	32,29,25,3	29	31	20.94	3	4	2	116.5
5	32,29,25,23,3	29	31	25.47	4	6	3	141.3
6	32,29,25,23,19,3	29	31	29.72	4	6	3	166.9
7	32,29,27,25,23,19,7	27	31	35.59	4	8	3	200.3
8	32,29,27,25,23,19,17,7	27	31	39.68	5	8	4	224.9
9	32,29,27,25,23,19,17,13,7	27	31	43.38	5	10	4	245.6
10	32,29,27,25,23,19,17,13,11,7	27	31	46.84	5	10	5	266.4

表2　scaler performance ($m_{\hat{p}}$=31)

method	table lookup cycle数	max scaling error	法あたりのtable数	Sの制限	total table数
MRC	n	1/2	n(n+1)/2	あり	$n^2(n+1)/2$
MRC'	n	[(n+1)/2]/2	n(n+1)/2	なし	$n^2(n+1)/2$
S-CRT	$[\log_2(n+1)]_r+1$	(n+1)/2	2[(n+1)/2]	なし	2(n+1)・[(n+1)/2]
S-CRT''	$[\log_2(n+1)]_r+1$	$\frac{1}{2}\{[\frac{n+1}{2}]+1\}$	2[(n+1)/2]	なし	2(n+1)・[(n+1)/2]

表3　法の個数nに対する各手法のscalerの比較

5. 数　値　例

この章ではS-CRTによる方法で実際にRNSから2進数に変換できることを具体的な数値例で示すことにする。

$n=4$, $m_1=16$, $m_2=7$, $m_3=13$, $m_4=11$とすると(20)から$m_{\hat{p}}=3$と選べる。(22)から$\hat{d}=1$, ダイナミックレンジは, $-8008\leqq Y\leqq 8007$

table look-up用のS-CRTとしていまm_1とm_2, m_3とm_4を組み合わせる。(19. a), (19. b)より,

$$Y=13\times 11<\frac{1}{13\times 11}\ y_{1,2}>_{m_1 m_2}+16\times 7<\frac{1}{16\times 7}\ y_{3,4}>_{m_2 m_4}-\hat{P}(Y)\cdot M \tag{28. a}$$

$$\begin{cases} y_{1,2}=<7<7\ y_1>_{m_1}+16<-3\ y_2>_{m_2}>_{m_1 m_2} \\ y_{3,4}=<11<6\ y_3>_{m_3}+13<-5\ y_4>_{m_4}>_{m_3 m_4} \end{cases} \tag{28. b}$$

ここで　$<(13\times 11)^{-1}>_{m_1 m_2}=47$, $<(16\times 7)^{-1}>_{m_3 m_4}=-60$, $<7^{-1}>_{m_1}=7$, $<16^{-1}>_{m_2}=-3$, $<11^{-1}>_{m_3}=6$, $<13^{-1}>_{m_4}=-5$である。

従って

$$Y=143<47\ y_{1,2}>_{112}+112<-60\ y_{3,4}>_{143}-\hat{P}(Y)\cdot M \tag{29. a}$$

又は,

$$Y=143<-7<7\ y_1>_{16}-32<-3\ y_2>_7>_{112}+112<55<6\ y_3>_{13} -65<-5\ y_4>_{11}>_{143}-\hat{P}(Y)\cdot M \tag{29. b}$$

一方, もし普通のS-CRTに従うと,

$$Y=1001<-7\ y_1>_{16}+2288<-y_2>_7+1232<4\ y_3>_{13}+1456<3\ y_4>_{11}-P(Y)\cdot M$$

となり$m_p\geqq 5$でなければならない。

$\hat{P}(Y)$は(21)から

$$\hat{P}(Y)=<<<47y_{1,2}>_{112}>_3+<-<-60y_{3,4}>_{143}>_3+y_{\hat{p}}>_3 \tag{30}$$

少なくとも$-8008\leqq Y\leqq 8007$の範囲のYの値は正確に2進数に変換できる。

いま　$Y=(y_1, y_2, y_3, y_4, y_{\hat{p}})$として, $-7992=(8, 2, 3, 5, 0)$が与えられたとする（もちろんY=−7992であることは今はわからないとする)。

(28. b) より

$$y_{1,2}=-40,\quad y_{3,4}=16$$

(30)より

$$\hat{P}(Y)=<<<47\times(-40)>_{112}>_3+<-<(-60)\times 16>_{143}>_3+0>_3$$
$$=1$$

(29. a) より

$$Y=143\ (+24)+112\ (+41)-(+1)\cdot M$$
$$=-7992$$

を得る。

次に$2^{k-1}<M\hat{d}<2^k$なるmod 2^k adderによりYが得られることを示す。$M\hat{d}\fallingdotseq 2^{13.96}$より$k=14$,

$143\times24\Rightarrow0$	0 1 1 0 1 0 1 1 0 1 0 0 0	
$112\times41\Rightarrow0$	1 0 0 0 1 1 1 1 1 0 0 0 0	
+) $-M\Rightarrow0$	0 0 0 0 1 0 1 1 1 0 0 0 0	
1	0 0 0 0 0 1 1 0 0 1 0 0 0	$\Rightarrow-7992$ （2の補数）
0	1 1 1 1 1 0 0 1 1 1 0 0 0	$\Rightarrow$ 7992

6. 結　　論

CRTタイプの新しいRNSデコーディングの手法を提案した。この手法はRNS回帰形フィルタのscalerに応用した場合，MRCや従来のCRTのtable-look-up法を用いた手法のいくつかの欠点を克服し，CRTの持つ高いスループット，MRCの持つ広いダイナミックレンジを同時に実現できるものである。

RNSについて論ずるときにしばしば欠点として指摘されるハードウェアのコストの面でも，scalerのtable数はMRCによるscalerの約2/nでよいので比較的経済的である。

また，従来の手法では使われることのなかった小さな数（3や5や7）を法m_pとして有効に利用できる点でこの手法はユニークである。

今回の研究は話をtable-look-up法に限定して行なったが，table-look-up法にだけ固執する必要はなく，他にも様々なアプローチの仕方があるので，今後はもっと大きな数のRNSにも目を向けてゆきたい。

参考文献

1) K.H.O'keefe: IEEE Trans. Comput., vol.C-22, pp.833-835, Sept. 1973
2) W.K.Jenkins and B.J.Leon: IEEE Trans. Circuits Syst., vol. CAS-24, pp.191-201, Apr. 1977
3) M.H. Etzel and W.K. Jenkins: IEEE Trans. Acoust., Speech, Signal Processing, vol. ASSP-30, pp.370-380, June 1982
4) W.K. Jenkins: IEEE Trans. Acoust., Speech, Signal Processing, vol. ASSP-27, pp.19-30, Feb.1979
5) G.A. Jullien: IEEE Trans. Comput., vol. C-27, pp.325-336, Apr. 1978
6) Thu Van Vu: IEEE Trans. Comput., vol. C-34, pp.646-651, July 1985
7) M.A. Soderstrand, et al.: IEEE Trans. Circuits Syst., vol. CAS-30, pp.903-907, Dec.1983
8) F.J. Taylor and A.S. Ramnarayanan: IEEE Trans. Circuits Syst., vol. CAS-28, pp.1164-1169, Dec. 1981
9) R.Ramnarayan and F.J.Taylor: IEEE Trans. Circuits Syst., vol. CAS-32, pp.349-359, Apr. 1985
10) D.D. Miller and J.N. Polky: IEEE Trans. Circuits Syst., vol. CAS-31, pp.452-461, May 1984
11) M.A. Soderstrand and B.Sinha: IEEE Trans. Circuits Syst., vol. CAS-31, pp.415-417, Apr. 1984