		ア デ グ ベ ン ロ　　オ ル ウ オ レ	
氏　　　　　名	Adegbenro Oluwole	
授 与 学 位	工　　学　　博　　士	
学 位 授 与 年 月 日	昭和61 年 3 月 25 日	
学位授与の根拠法規	学位規則第 5 条第 1 項	
研究科，専攻の名称	東北大学大学院工学研究科	
	（博士課程）電子工学専攻	
学 位 論 文 題 目	LSI-Oriented Residue Arithmetic Circuits and their	
	Application in the Implementation of a Digital Signal	
	Processor （LSI 向き剰余数演算回路とそのディジタル信	
	号処理プロセッサへの応用に関する研究）	
指 導 教 官	東北大学教授　　樋口　龍雄	
論 文 審 査 委 員	東北大学教授　　樋口　龍雄　東北大学教授　　松尾　正之	
	東北大学教授　　高木　相　東北大学助教授　亀山　充隆	

論　文　内　容　要　旨

CHAPTER 1　INTRODUCTION

　　The demand for increased functional throughput rate(FTR) of VLSI chips requires that circuits be implemented more compactly and be capable of high-speed operation. This in turn means that for a given chip area, the number of devices becomes quite large and gives rise to the VLSI design problem of layout. A recognised solution is to employ parallelism /modularity whereby circuits can be partitioned and thus a 'divide and conquer'strategy can be used in tackling the layout problem. A number coding scheme which embodies parallelism is the residue number system (RNS) which also has the capability of supporting high-speed processing because unlike the usual weighted binary number system, there is no carry when arithmetic operations are carried out. This thesis explores the wherewithal of obtaining an increased FTR by exploiting these properties of the RNS. A new residue multiplier circuit using shift registers connected in a ring form is proposed. The outstanding feature of this multiplier circuit is that it is completely flexible, has a computation time which is the same

as that of a residue number adder and also shares a structural similarity with the adder; a feature which will greatly simplify the layout problem. In addition the multiplier circuit can be used in a pipelining mode because the shift registers have both computing and memory functions.

The feasibility of this proposal is proved firstly be constructing a real-time digital signal processor for linear convolution. In this processor, the residue arithmetic circuits support pipelined processing without the need for any additional hardware and are used in a structure which allows 100% pipelining efficiency in the arithmetic unit such that an optimum through-put rate is obtained for a filter of any order. Secondly a comparison of the complexity figure of merit based on the Area Time product of the proposed residue arithmetic circuits with the more conventional approches shows that the new scheme performs better and when a moderate processing speed is acceptable it offers a much more compact structure.

CHAPTER 2 BASIC CONSIDERATIONS OF RESIDUE ARITHMETIC AND THE RESIDUE NUMBER SYSTEM

In the residue number system, an integer X is represented by an L-tuple as:

$$X = (x_0, x_1, \ldots x_{L-1}) \tag{1}$$

were x_i is the remainder of X when divided by the i-th modulus, m_i and denoted as in Eq. (2).

$$x_i = |X|_{m_i} \tag{2}$$

If all the m_i are mutually prime integers, the dynamic range of X is $0 \leqslant X \leqslant M-1$ where M is the product of all the moduli. Addition and multiplication are performed on each digit separately as in Eq. (3).

$$X \bigcirc Y = (x_0 \bigcirc y_0, x_1 \bigcirc y_1, \ldots x_{L-1} \bigcirc y_{L-1}) \tag{3}$$

where the symbol $\bigcirc$ denotes multipication or addition. The reverse operation of obtaining the value of X given the residue digits $(x_0, x_1, \ldots x_{L-1})$ is performed by invoking the Chinese remainder theorem given in Eq. (4).

$$|X|_M = \left| \sum_{i=1}^{L} \stackrel{\wedge}{m_i} \cdot \left| \frac{x_i}{\stackrel{\wedge}{m_i}} \right|_{m_i} \right|_M \tag{4}$$

where $\hat{m}_i = M/m_i$ and $M = \prod_{i=1}^{L} m_i$

When the modulus, m is a prime number, it can be shown that all the elements in the set {1,2,3,......m-1} can be written as powers of the primitive root of m and that the set forms a field with multiplication and addition. These are the basic properties which are used in the implementation of any RNS based system and in the implementation of the new residue arithmetic circuit proposed in this thesis.

CHAPTER 3 FLEXIBLE LSI-ORIENTED SHIFT REGISTER BASED RESIDUE ARITHMETIC CIRCUITS

An m-stage shift register connected in a ring form can be used for implementing modulo-m addition or subtraction. The circuit model and the form of the input/output signal are shown in Fig.1. The operation of a subtracter circuit is illustrated in Fig.2. If the multiplier coefficient K is a constant, multiplication can be performed by the interconnection between the multiplicand and the product registers. For example, the multiplication table for m = 7 and the interconnection for $|A \cdot K|_7$, where A is any value of the multiplicand and K equals 3, are shown in Table I and Fig.3 respectively. Since the interconnection is fixed for a specified coefficient, this circuit is not flexible enough for many applications.

For the general case when K is not fixed, we can use the cyclic properties of a Galois field, as expressed in Eqs.(5) and (6), as the basis of a new flexible residue number multiplier circuit. Let the modulus, m be a prime number.
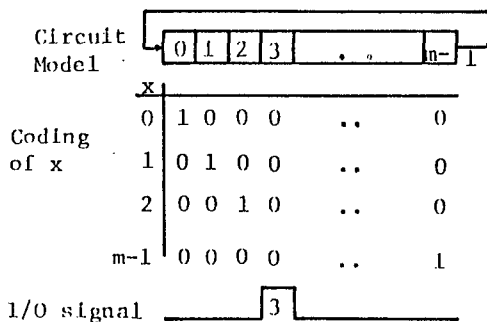
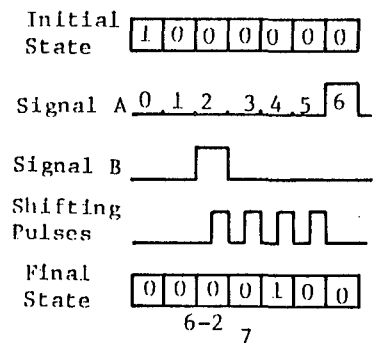$$i\ (k) = |\ g^k|_m \tag{5}$$

Fig. 1 Circuit model and signal form

Fig. 2 Operation of the subtracter

Multiplier i(k)

Multiplicand	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$P_1 \, P_2 \, P_6 P_4 \, P_5 \, P_3$
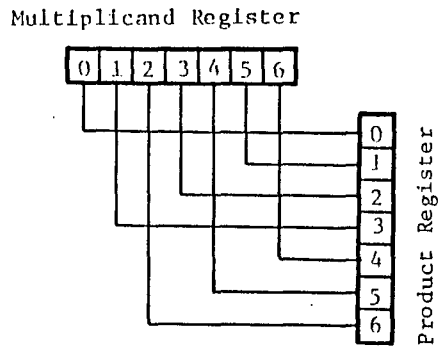
Multiplicand Register

Product Register

Table I Modulo-7 multiplication table

Fig. 3 Connections for k=3 in Modulo-7 multiplication

where i (k) is an element in the set $Z_m = \{1, 2, \ldots m-1\}$, g is the primitive root of m and k is an integer such that $0 \leqslant K \leqslant m-1$. Let $P_{i\,(k)}$ be a column vector in the modulo-m multiplication truth-table.

$$P_{i\,(k+1)} = | \ g \cdot P_{i\,(k)} \ |_m \tag{6}$$

Eq. (6) is recursive in k and hence also in some manner in i through Eq. (5), and since the primitive root is fixed for a given value of m, the same mechanization can be used to realize Eq. (6) for any set of values of k which have serially related members. The case of m = 7 is used as an example to see how any flexible modulo-m multiplier circuit can be configured. The primitive root of 7 is 3 and Eq. (6) for k = 0, gives

$$P_{i(1)} = P_3 = | \ 3 \ P_1 \ |_7 \tag{7}$$

Eq. (7) is mechanizable, using the model shown in Fig. 1, as shown in the right part of Fig. 4. This mechanization enables Eq. (6) to be realized for values of k = 0,1,2,......m-2 which in effect means that all columns except the zero column in the truth-table can be obtained. It is noted that the value of the primitive root enables the interconnections between the stages in the register to be defined. This would be different for different m and g combinations, hence the circuit shown in Fig. 4 is unique for modulo-7 multiplication. Thus using the circuit connection of the form shown in Fig. 4 and since the P_1 column and the multiplicand column of the truth-table are identical, the multiplication operation for any two modulo-m residues A and B can be performed by using the multiplier, B to change the state of an
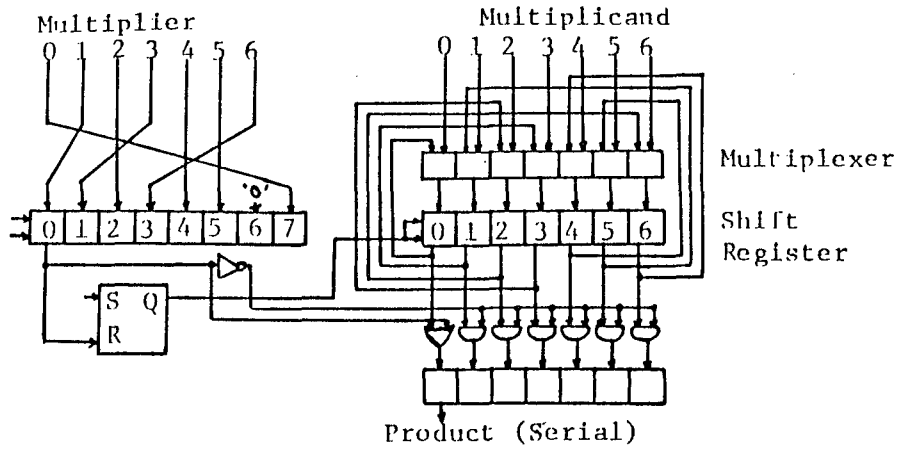
Fig. 4　Circuit configuration of the residue number multiplier

m-stage register whose initial state is the multiplicand, A. This is accomplished by the using the value of B through Eq. (5) to control the duration of the common clock which in turn determines the number of changes in the state of the register. Since k is undefined when B= 0, this principle cannot be used to effect the desired multiplication. A solution is to simply set the register to the zero value when B = 0 . The multiplier circuit has the same structure and computation time as an existing adder circuit. These features mean that there is a uniform processing rate throghout a system employing both the adder and the multiplier and the fabrication problem is reduced to that of only a single type of building block.

CHAPTER 4　APPLICATION IN A PROGRAMMABLE RNS BASED DIGITAL SIGNAL PROCESSOR

　　High-speed computation is possible in the residue number system because of the parallel nature of the processing. If in addition, the processing in each parallel path can be pipelined, then an increased throughput can also be achieved. The RNS has found application mostly in areas where a large amount of simple arithmetic operations is to be perfomed. This calls for flexibility on the part of the arithmetic circuits if the hardware requirement is to be economically feasible. The residue number arithmetic circuits described earlier can thus be used advantageously here. The application of the residue number multiplier in FIR digital filtering by using it in a structure which is amenable to pipelined processing is considered. In addition,

by exploiting the flexible nature of the multiplier, it is used for an increased processing capability using a limited amount of hardware.

A finite impulse response (FIR) digital filter is a number processing algorithm in the form of Eq. (8).

$$y(k) = \sum_{j=0}^{N-1} h(j) \cdot u(k-j) \tag{8}$$

where $y(k)$, $u(k)$ and $h(j)$ are respectively the output of the filter, the input data and the coefficient. The direct form realization of Eq. (8) requires N number of multipliers which means a high hardware overhead and circuit complexity when N is large. This may be reduced by using a fixed low-order filter section with changeable coefficients. The low-order section is used for higher-order filtering by changing the coefficients and the input data applied to the multipliers in a predetermined manner. Consider that an n-th. order filter section is to be used to implement a higher N-th. order filter. The direct form realization of the n-th. order section requires (n+1) number of multipliers and the N-th. order filter output is obtained every $\lceil (N+1)/(n+1) \rceil = \ell$ cycles, where the notation $\lceil x \rceil$ denotes the integer such that $x \leqslant \lceil x \rceil \leqslant x+1$. Using the arithmetic circuits described earlier, the computations proceed in a pipelining manner with no idle state, resulting in an optimum sampling frequency, f_s, expressed as:

$$f_s = f/\ell(m+1) \tag{9}$$

and the latency, τ, as:

$$\tau = (q+1)(m+1)/f \tag{10}$$

where the number of adder stages, $q = (\lceil \log_2 n \rceil + 1)$, f is the clock frequency of the arithmetic circuit and m is the modulus.

A breadboard implementation using off-the-shelf components is built and tested. In the implementation a set of moduli {23, 19, 17, 13} - which gives a dynamic range of approximately 16 bits- and a basic structure consisting of two multipliers and two adders for each of the four moduli is used. Residue code to analog conversion is done through the use of the Chinese remainder theorem using table-look-up techniques. The control circuit of the filter is cascade of two counters respectively modulo-24 and modulo-ℓ; with ℓ as defined earlier. In the implementation pipelining latches are not used because the shift registers composing the arithmetic circuits combine both computation and pipelining functions.

CHAPER 5 EVALUTION AND COMPARISONS FROM THE VIEW POINT OF VLSI IMPLEMENTATION

The ultimate goal of the implementation of the flexible digital signal processor, based on the pulse train arithmetic circuit, is in VLSI. It is therefore worthwhile to have some estimate of the magnitude of the chip area needed for fabrication. This will also facilitate the comparison of hardware complexity of alternative implementation approaches. A figure of merit useful in the comparison is the Area-Time product where the Area is the chip area required for fabrication in a given technology and the Time is that for processing one word. For the comparison the nMOS technology based on the 5 μm design rule is used and the alternative implementations under consideration are:

(a) the RNS pulse-train technique described earlier,

(b) the RNS table-look up approach using ROM and

(c) the conventional binary weighted number system using the Baugh-Wooley multiplication and ripple-carry adder. (The algorithm has LSI fabrication appeal because of the use of only one type of full adder)

By performing a computer simulation of the basic building blocks of these alternatives, the performance of a sum of product module consisting of two multipliers and two adders, in terms of the fabrication area and the computation time can be estimated. The result is the complexity measure shown in Fig.5. This shows that the table-look-up approach is the most complex because of the large number of memory cells which are required while the approach proposed in this thesis is the least complex if the dynamic type of shift registers are used in the fabrication.
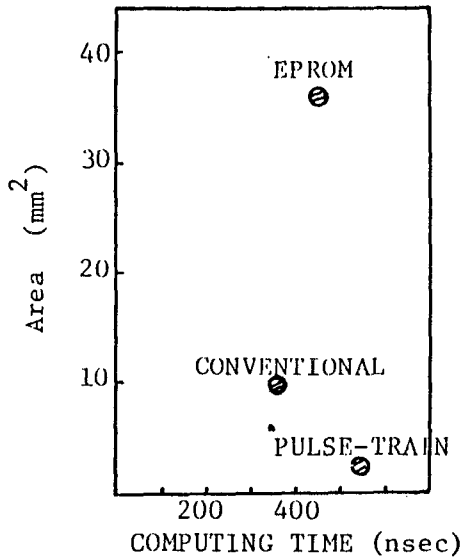
Fig.5　Fabrication area versus computing time for a dynamic
range of 18 bits

CHAPTER 6　CONCLUSIONS AND SUGGESTIONS FOR FURTHER RESEARCH

Parallel processing through the use of the RNS is an effective way of tackling the LSI design problem. A new residue number multiplier circuit is proposed and is used in the breaboard implementation of a programmable FIR filter where the type and the order of the filter can easily be changed as desired. Comparison of the complexity of the implementation approach proposed in the thesis shows that it is quite suitable for VLSI because of reduced fabrication area due to the use of a single building block composed of the dynamic type of shift register.

The proposed technique can be extended for application in other areas of digital signal processing such as the FFT and number theoretic transforms. The multiplier circuit can also be used in the implementation of the general division algorithm in the RNS which hitherto, because of the complexity of existing residue number multiplier circuits, is prohibitively complex to implement.

審 査 結 果 の 要 旨

　最近ディジタル信号処理システムは，集積回路技術の著しい発展を背景としてその実現が容易となり，種々の分野で盛んに用いられるようになってきた。それに伴い，システム構成上最も重要となる演算回路の小形化と高速化両者を考慮した，ＬＳＩ向き回路構成法の研究が望まれている。

　著者は，剰余数系が演算上の優れた性質を有することに着目し，ディジタル信号処理プロセッサの実現に適する剰余数演算回路を提案して，その構成法を確立すると共に，新しいアーキテクチャに基づく信号処理プロセッサを考案しその有用性を実証した。本論文はその成果をまとめたもので，全文6章よりなる。

　第1章は緒言である。第2章では，加算器および乗算器などの演算回路を構成する上で基礎となる剰余数系の数学的性質を考察し，その巡回的性質がパルス列演算回路の構成に極めて適していることを明らかにしている。

　第3章では，パルス列剰余演算回路，特に信号処理プロセッサの性能を支配する乗算器の新しい構成法を提案している。すなわち，剰余数演算のモジュラスが素数のとき，零以外の任意の元はガロア体上の原始元のべき乗で表せることに着目し，シフトレジスタを基本構成要素とする乗算器の構成法を与えている。得られた乗算器のハードウェア量と演算時間は，加算器の場合と同程度であることから，本構成法が小形化と高速化の点で優れていることを明らかにしている。これは有用な成果である。

　第4章では，前章で確立されたパルス列剰余数演算回路の応用として信号処理プロセッサの構成法を検討している。特に，並列処理とパイプライン処理に基づき加算器および乗算器の稼動率が100％のアーキテクチャを考案し，汎用ＩＣを用いて信号処理プロセッサを試作しその動作を確認している。

　第5章では，ＬＳＩ化に適した信号処理プロセッサの構成法を明らかにすると共に，計算機シミュレーションにより，その性能を詳細に検討している。その結果，本プロセッサは，演算回路が極めて簡単かつ規則的であり，また本質的にメモリ機能のあるシフトレジスタを主体とした回路構成であるため，パイプライン動作が容易であるなどＬＳＩ化に適した構造を有していることを実証している。これらは本研究の重要な成果である。

　第6章は結言である。

　以上要するに本論文は，剰余数系の演算上の優れた性質を巧みに利用したＬＳＩ向きの新しい演算回路を提案し，その構成法を確立すると共に，信号処理プロセッサの構成上多くの有用な知見を与えたもので，電子工学および情報工学の発展に寄与するところが少なくない。

　よって，本論文は工学博士の学位論文として合格と認める。