

NOVEL IMPLEMENTATION METHOD OF MODULO 2^N MULTIPLICATION FOR DIGITAL SIGNAL PROCESSING

MOHAMED ARIF BIN NUN

Fakulti Kejuruteraan Elektrik
Universiti Teknologi Malaysia

RINGKASAN

Kertaskerja ini membentangkan satu cara baharu dalam mana satu pendaraf modulo 2^N dijemakan secara isomorfik menjadi sepasang penyampur modulo 2 dan modulo 2^{N-2} . Bilangan penyampur-penyampur penuh yang diperlukan untuk pelaksanaan bertambah secara linear dengan bertambahnya panjang perkataan N , dan tidak dengan secara eksponen, dan kelewatan pengantaran sistem tetap pada asasnya tidak berubah dengan bertambahnya N .

ABSTRACT

This paper presents a novel method in which a modulo 2^N multiplier is transformed isomorphically into a pair of modulo 2 and modulo 2^{N-2} adders. The number of full-adders required for implementation increases linearly with increasing wordlength N , rather than exponentially, and the system propagation delay remains basically constant with increasing N .

1. Introduction

In the past few years there has been an increasing application of number-theoretic concepts to digital signal processing¹. In most signal processing algorithms the multiplier invariably forms one of the main computing elements, especially in hardware implementations in which component cost and processing speed are essential for efficient and economic hardware structures. In this paper, we present the main concepts and results of a novel technique with which a modulo 2^N multiplier can be isomorphically transformed into a pair of modulo 2 and modulo 2^{N-2} adders. It is shown that the number of full-adders required for their implementation increases linearly with increasing wordlengths N of the multiplier operands,

rather than exponentially as in most conventional implementations. Furthermore the system propagation delay is shown to remain basically constant with increasing N . The application of these results will lead to efficient and cost-effective hardware structures for modulo 2^N multiplications.

2. Modulo 2^N Multiplication Using “Forced” Operands and Product Correction

The approach proposed is based on a *reduced* multiplier, which is the original modulo 2^N multiplier whose operands and product are constrained to take on only the odd values from the set

$$Z_N = (0, 1, 2, \dots, 2^N - 1)$$

Hence, if A, B and A', B' are the operands to the original and reduced multipliers respectively, then $A', B' \in Z_D$, where

$$Z_D = (x : x \text{ odd integer}, 1 \leq x \leq 2^N - 1).$$

These modified operands may be derived from the originals by the mapping g_A and g_B , where

$$g_A : A \longrightarrow A' = A + c$$

$$\text{and } g_B : B \longrightarrow B' = B + d$$

such that

$$c = \begin{cases} 0 & \text{for } A \text{ odd} \\ 1 & \text{for } A \text{ even} \end{cases} \quad d = \begin{cases} 0 & \text{for } B \text{ odd} \\ 1 & \text{for } B \text{ even} \end{cases}$$

Multiplying these ‘forced’ operands, we obtain,

$$\begin{aligned} P'_0 &\equiv A' \times B' \equiv (A + c) (B + d) \text{ modulo } 2^N \\ &\equiv AB + dA + cB + cd \text{ modulo } 2^N \end{aligned}$$

Hence the required product $P_0 \equiv A \times B \text{ modulo } 2^N$ is given by $AB = (A' \times B') - (dA + cB + cd) \text{ mod. } 2^N$

This congruence relationship expresses our proposed multiplication scheme, in which $(A' \times B')$ describes the reduced multiplication and $C = (dA + cB + cd)$ the correction required to obtain the actual product. The block diagram of the overall configuration is shown in Fig. 1.

The various values of C corresponding to all possible combinations of a and b , the L.S.B's of A and B respectively, are given below.

a	b	c	d	C
0	0	1	1	$A + B + 1$
0	1	1	0	B
1	0	0	1	A
1	1	0	0	0

This leads to a very simple correction circuit consisting of a modulo 2^N adder which is just the conventional 2^N adder with the carry digit excluded, and two gating circuits, each consisting of $(N-1)$ 2-input AND gates and one inverter. The output C from this correction unit is then subtracted from P' to obtain the actual product P_0 .

3. Internal Algebraic Structure of Reduced Modulo 2^N Multipliers

In the following, we present only the main concepts and results of our study of the algebraic structure of a general reduced modulo 2^N multiplier. The corresponding detailed arguments and proofs are in Ref. 2.

3.0 The group under modulo 2^N reduced multiplication

Let (Z_D, \otimes_{2^N}) be the multiplier modulo 2^N whose operands are constrained to odd values, i.e. from the set Z_D .

Theorem 1:— The set of odd integers, i.e. $Z_D = (x : x \text{ odd integer, } 1 \leq x \leq 2^N - 1)$, forms an Abelian group under multiplication modulo 2^N . This group, which we denote by $G(2^N)$, has order

$$G(2^N) = 2^{N-1}$$

For the specific cases of our reduced multipliers moduli 2^0 , 2^1 and 2^2 , we can prove, using elementary concepts in number theory (pages 123 to 125 in Ref. 2), that for each of these multipliers, its algebraic structure can be directly described and the complete multiplication table can be generated by a single element $x \in Z_D$, if x is a primitive root of 2^N , where $N = 0, 1$ or 2 .

3.1 Detailed algebraic structure of reduced modulo 2^N multipliers

In our following two lemmas and one theorem we extend the analysis to cases where $N \geq 3$ and will show that the table of a general reduced modulo 2^N multiplier, $N \geq 3$, can still be described completely but this time two elements $Z_i, Z_j \in Z_D$ are required to generate it.

Lemma 1:— $3^{2^N} = (2^{n+2}) (x(n)) + 1$ for $n \geq 1$ where $x(n)$ is an odd number for all n .

Corollary. The element 3 in Z_{2^N} has order 2^{N-2} in $G(2^N)$.

Lemma 2:— There are four elements, ± 1 and $(2^{N-1} \pm 1)$, in $G(2^N)$ having order 2

Corollary. (a) The values $x_h \equiv 1$ and $x_i \equiv 2^{N-1}$

$+ 1$ (modulo 2^N) may be expressed as powers of 3 (modulo 2^N).
 (b) The values $x_j \equiv -1$ and $x_k \equiv 2^{N-1} - 1$ (modulo 2^N) cannot be powers of 3.

As a result of the above-mentioned Lemmas, the algebraic structure of our modified or reduced modulo 2^N multiplier, for $N \geq 3$, can be described in detail via the following theorem.

Theorem 2:— The group $G(2^N)$, as described by Theorem 1, for $N \geq 3$, is isomorphic to the direct product group $K \times H$, where K and H are cyclic groups of orders 2^{N-2} and 2 respectively.

The subgroup K is given by

$$K = (k_0, k_1, \dots, k_i, \dots, k_m), 0 \leq i < 2^{N-2},$$

$$m = 2^{N-2} - 1, k_i \in G(2^N) \text{ and } k_i = 3^i \text{ modulo } 2^N.$$

Thus subgroup L is given by $L = (1_0, 1_i)$ where $1_0, 1_i \in G(2^N)$ and

$$1_i \equiv x^i \text{ modulo } 2^N, \text{ for } i = 0, 1.$$

1. The value of x is either $x \equiv -1$ modulo 2^N or $x \equiv 2^{N-1} - 1$ (see Corollary (b) of Lemma 2).

4. Application of Theoretical Results

The subgroups K and L may be used to organise $G(2^N)$ by forming the relevant cosets in the usual way.

Let the cosets w.r.t. K be V_0 and V_1 and those w.r.t. L be $W_0, W_1, \dots, W_i, \dots, W_n$,
 $n = (2^N - 2 - 1)$, given by

$$V_0 = (V_{0,0}, V_{0,1}, V_{0,2}, \dots, V_{0,i}, \dots, V_{0,n}) =$$

$$V_1 = (V_{1,0}, V_{1,1}, \dots, V_{1,i}, \dots, V_{1,n})$$

$$\text{and } W_0 = (W_{0,0}, W_{0,1}) = L, W_1 = (W_{1,0}, W_{1,1})$$

$$\dots, W_i = (W_{i,0}, W_{i,1}).$$

Where $v_{d,i} = x^d 3^i$ modulo 2^N , $d = 0$ or 1 , $0 \leq i \leq n$

and $W_{i,d} = 3^i x^d$ modulo 2^N , in which the value x is either x_j or x_k as described by Corollary (b) of Lemma 2.

In general, each element $g_{l,m}$ of $G(2^N)$ can be presented by the modulo 2^N product of powers of x and 3 via the following congruence, i.e.

$$x^l 3^m = g_{l,m} \text{ modulo } 2^N, 1 \leq g_{l,m} \leq 2^N - 1,$$

where $l = 0$ or 1 and $0 \leq m < n$.

From the corollary to Lemma 1, and the results in Lemma 2, the components 3^m and x^l , will go through 2^{N-2} and 2 values respectively before repeating themselves. Therefore this will generate $(2^{N-2}) \times 2 = 2^{N-1}$ different elements of $G(2^N)$, the above congruence describes $g_{l,m}$ uniquely.

Let us now express $G(2^N)$ in terms of its cosets,
 i.e. $G(2^N) = \{V_0 ; V_1\}$ using subgroup K, and $G(2^N)$

$$= \{W_0 ; W_1 ; \dots ; W_i ; \dots ; W_n\} \text{ using the subgroup L.}$$

If we consider any two elements of $G(2^N)$, say $g_{l',m'}$ and $g_{l'',m''}$, then, it can be shown (Ref. 2)

that, their product P is given by $P = g_{i, j}$ modulo 2^N , where $(1' + 1'') \equiv i$ modulo 2 and $(m' + m'') \equiv j$ modulo 2^{N-2} .

Since the subscripts I and m denote the cosets w.r.t. the subgroups K and L respectively, then we know that $g_{1', m'} \in V_{1'}$, and also $W_{m'}$; and $g_{1'', m''} \in V_{1''}$, and also $\in W_{m''}$

Furthermore, their modulo 2^N product $g_{i,j}$ belongs to both cosets V_i and W_j where i and j are the modulo 2, and modulo 2^{N-2} sums of $1', 1''$, and m', m'' respectively.

Consequently, if we denote the operation (i.e. multiplication) between any two cosets (w.r.t. K) by \square_1 and that between any two (w.r.t.) by \square_m then it is not difficult to see that

$$V_{1'} \square_1 V_{1''} = V_{(1' + 1'')} \text{ modulo } 2, \text{ and } W_{m'} \square_m$$

$$W_{m''} = W_{(m' + m'')} \text{ modulo } 2^{N-2}$$

In other words, if each coset is mapped onto its corresponding index, i.e. $V_{1'} \rightarrow 1'$, $V_{1''} \rightarrow 1''$ and

$W_{m'} \rightarrow m'$, $W_{m''} \rightarrow m''$, Then operations between cosets may be mapped onto modulo addition operations between indices as shown by the two commutative diagrams below.

$$(a) \begin{array}{ccc} V_{1'} & , & V_{1''} \\ \swarrow & & \searrow \\ 1' & ; & 1'' \end{array} \xrightarrow{\square_1} \begin{array}{c} V_{1'} \square_1 V_{1''} \\ = V_i \end{array}$$

$$\xrightarrow{\oplus 2} \begin{array}{c} i = (1' + 1'') \\ \text{modulo } 2 \end{array}$$

$$(b) \begin{array}{ccc} W_{m'} & , & W_{m''} \\ \downarrow & & \downarrow \\ m' & , & m'' \end{array} \xrightarrow{\square_m} \begin{array}{c} W_{m'} \square_m W_{m''} \\ = W_j \end{array}$$

$$\xrightarrow{\oplus 2^{N-2}} \begin{array}{c} j = (m' + m'') \\ \text{modulo } 2^{N-2} \end{array}$$

Finally, the complete reduced modulo 2^N multiplication may be described in a compact way as follows.

Let f_g and f_p be the mappings given by $f_g : g_{l,m} \rightarrow$

(l,m) and $f_p : \otimes_{2^N} \rightarrow (\oplus_2, \oplus_{2^{N-2}})$ where

$g_{l,m} \in G(2^N)$, $l \in (0,1)$, $m \in (0,1,2, \dots, 2^{N-2} - 1)$

and \square is the parallel component-wise operation between any two ordered-pairs (l', m') and

(l'', m'') , i.e.

$$(l', m') \square (l'', m'') = \{ [l' \oplus_2 l'']$$

$$[m' \oplus_{2^{N-2}} m''] \} = (i,j).$$

Thus, for any two elements of $G(2^N)$, say $g_{l', m'}$,

and $g_{l'', m''}$, we have the following useful commutative diagram shown in Fig. 3:

It is now easily seen that the mapping-pair f_g, f_p transforms the original reduced multiplier into two adders, modulo 2 and modulo 2^{N-2} respectively, operating in parallel.

To illustrate this isomorphism between the multiplier and the adder-pair, let $N = 4$. Two possible organisations of $G(2^4)$ into sets of cosets are (a) $G(2^4) = \{ (1,3,9,11) ; (7, 5, 15,13) \}$ and (b) $G(2^4) = \{ (1,7) ; (3,5) ; (9,15) ; (11, 13) \}$.

Consider multiplying, modulo 16, the number 9 by 11. Using the mappings shown in Tables 1 and 2, and the commutative diagram (3), we may substitute additions modulo 2 and modulo 4 for our original modulo 16 multiplication as shown below.

$$\begin{array}{ccc}
 9 & ; & 11 & \xrightarrow{\otimes_{16}} & (9 \times 11) \text{ modulo } 16 \\
 | & & | & & = 3 \\
 f_g & & f_g & & \downarrow \\
 \downarrow & & \downarrow & & f_g \\
 (0,2) & ; & (0,3) & & \\
 & \downarrow \square & & & \\
 (0,2) \square (0,3) & = & [0 \oplus_2 0] , [2 \oplus_4 3] & = & (0,1)
 \end{array}$$

In practice, the results that we have derived are easily applied to the implementation of the general modulo 2^N reduced multiplier. The subgroup K is first generated by simply forming, modulo 2^N , the

successive powers, up to the $(2^{N-2} - 1)$ th, of 3 or 5, e.g. $K = 3^0 = 1, 3^1, 3^2, \dots$

$3^{2^{N-2}-1}, 3^{2^{N-2}} = 1$, either manually or by means of a straight forward computer program for large values of N. The resulting modulo 2^{N-2} adder may be further structurally simplified using loop-free finite-state machine technique for adders developed by the author (Ref. 3).

5. General Comparison With The Direct Implementation of Modulo 2^N Multipliers

In making a detailed comparison of our proposed method of implementing a modulo 2^N multiplier with that of the direct approach in which the first N bits of the partial products are summed using rows of full-adders, the following observations are made.

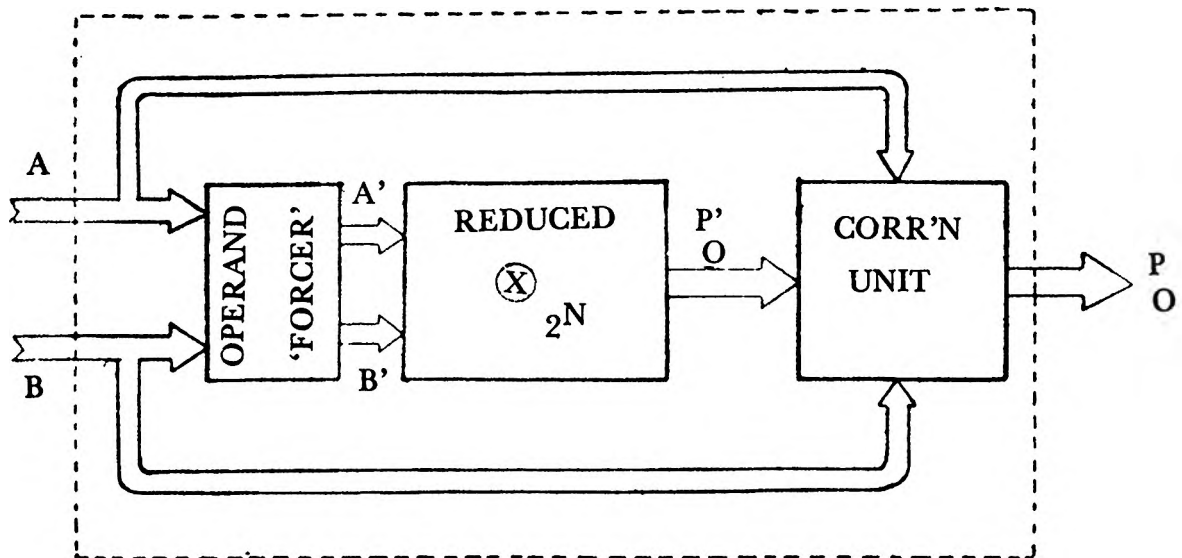


Fig. 1 Block diagram of modulo 2^N multiplication using 'forced' operands and product correction.

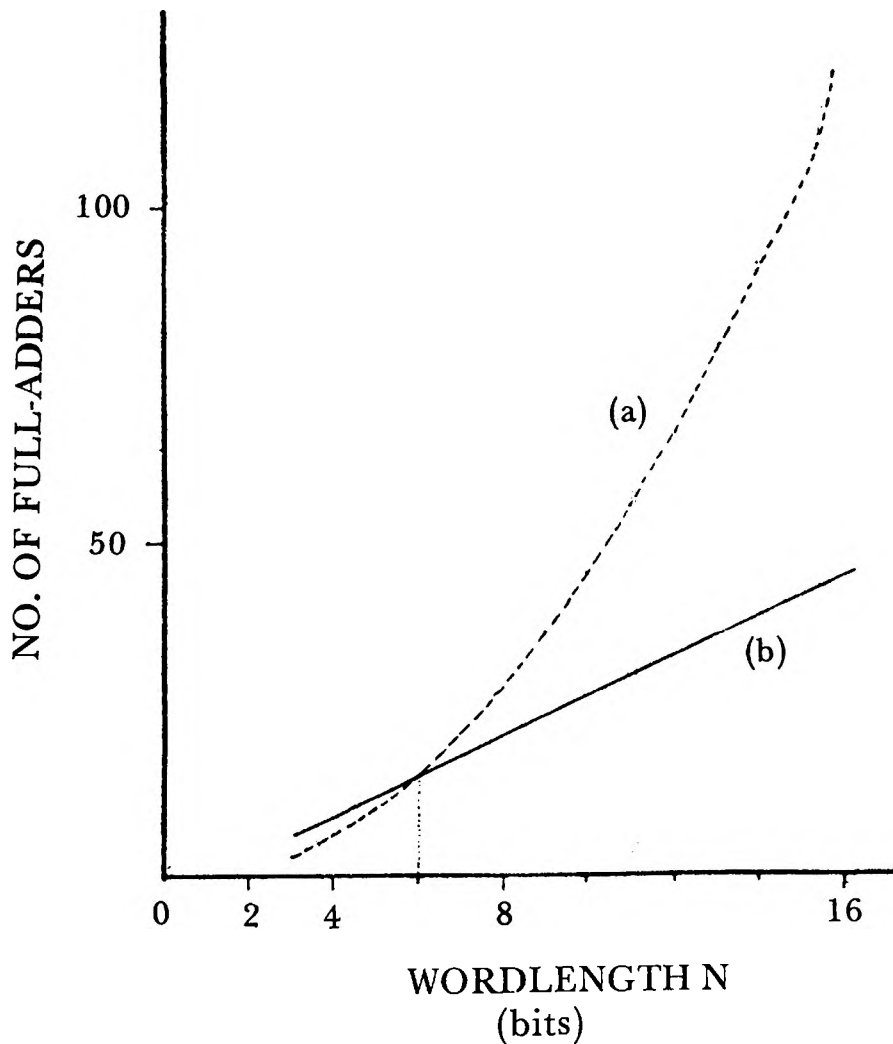


Fig. 2 Complexity in full-adder requirement for (a) direct implementation and (b) proposed implementation of modulo 2^N multiplier.

Novel implementation method of modulo 2^N multiplication

In both approaches, the number of full-adders (F.A's) required can give some indication of the overall hardware complexity. With the direct method we can easily work out that the number of F.A's needed is $(1 + 2 + 3 + \dots + N-1)$. With the proposed approach, we would need $(N-2) + 1$ F.A's for the modulo 2^{N-2} and modulo 2 adder-pair, along with $(N-1)$ F.A's for each of the two $(N-1)$ -bit adders used in the correction circuit, giving a total of $3(N-1)$ F.A's. The effect on the full-adder requirement with increasing word-length N is shown in the graph in Fig. 2. We see that with the method proposed, the full-adder count increases linearly with N , while that of the direct approach is proportional to N^2 . For $N > 6$, the proposed implementation technique required considerably fewer full-adders.

Furthermore, with the direct approach the propagation delay through the circuit, apart from the ripple delays through each row of F.A's is dependent on N . With our method, however, the system delay is basically constant, and is the sum of the delays through the first correction adder, a circuit for encoding into partition blocks, the adder-pair, a circuit for decoding from the partition blocks, and the final correction adder.

6. Conclusions

A novel method of implementing a general modulo 2^N multiplier has been presented, and consists of constraining the operands to odd values for a modified or reduced multiplier and correcting the output to obtain the actual modulo 2^N product. Analysis of the algebraic structure of the reduced multiplier shows that a reduced modulo 2^N multiplier is isomorphic to two adders, modulo 2^{N-2} and 2 respectively, operating in parallel. Finally, it was observed that when compared with the direct way of implementing modulo 2^N multipliers, the proposed approach leads to a circuit which required considerably less full-adder units and possesses a basically constant system propagation delay.

References

1. McClellan, J.H., "Number theory in digital signal processing", (Prentice-Hall, 1979).
2. Bin Nun, M.A., "Modular decomposition techniques for stored-logic digital filters", Ph.D. Thesis, Dept. of Electronic and Electrical Engineering, Loughborough University of Technology, Leics., England, 1977.
3. Bin Nun, M.A., and Woodward, M.E., "Halfadders modulo 2^N using read-only memories", Electronics Letters, 30th. May 1974, Vol. 10 No. 11.

\otimes_{16}	0				A'	1			
	1	3	9	11		7	5	15	13
1	1	3	9	11		7	5	15	13
3	3	9	11	1		5	15	13	7
0 9	9	11	1	3		15	13	7	5
B' 11	11	1	3	9		13	7	5	15
7	7	5	15	13		1	3	9	11
5	5	15	13	7		3	9	11	1
1 15	15	13	7	5		9	11	1	3
13	13	7	5	15		11	1	3	9

Table 1(a). Reduced multiplication table organised by subgroup (1,3,9,11)

\otimes_{16}	A'							
	00		01		10		11	
1	1	7	3	5	9	15	11	13
00 1	1	7	3	5	9	15	11	13
7	7	1	5	3	15	9	13	11
01 3	3	5	9	15	11	13	1	7
5	5	3	15	9	13	11	7	1
B' 9	9	15	11	13	1	7	3	5
10 15	15	9	13	11	7	1	5	3
11 11	11	13	1	7	3	5	9	15
13	13	11	7	1	5	3	15	9

Table 2(a). Reduced multiplier table organised by subgroup (1,7).

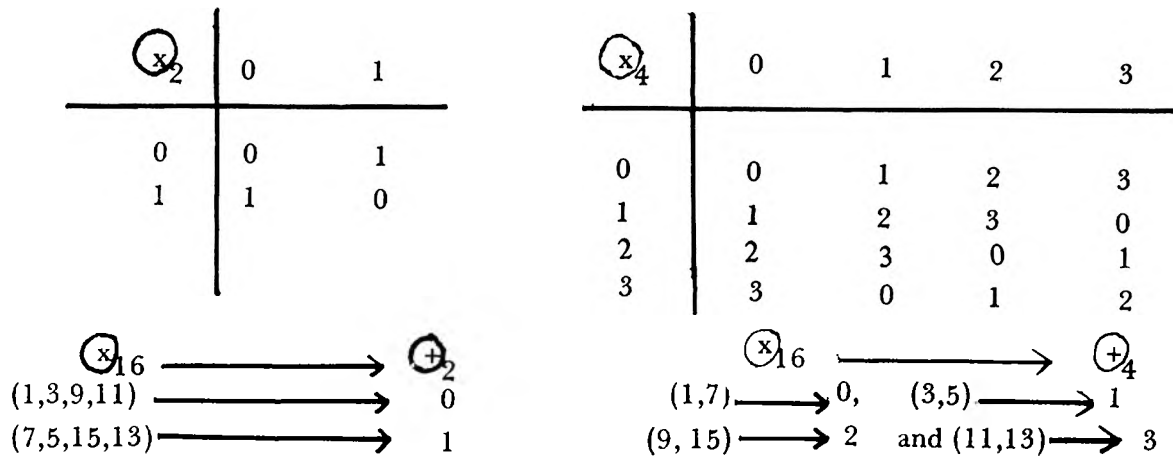


Table 1(b). Operation between blocks

Table 2 (b). Operation between blocks.

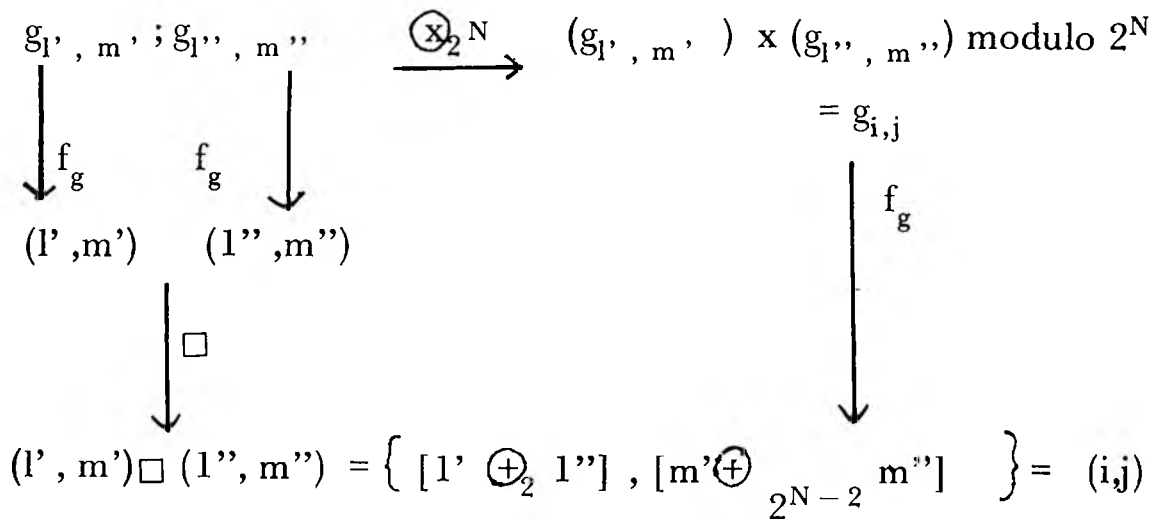


Fig. 3. Commutative diagram for transforming a reduced multiplier modulo 2^N into two adders, modulo 2 and modulo 2^{N-2} respectively, operating in parallel.

KURIKULUM VITAE PENULIS

MOHD. AZMI BIN ARIFFIN

- Tarikh lahir : 31hb. Januari, 1940
- Kelulusan : i) Peperiksaan iktisas the Royal Institution of Chartered Surveyors, United Kingdom – 1965
ii) Diploma Pentadbiran Awam, Universiti Malaya – 1970
- Jawatan : Professor Madya,
Ketua Jabatan Pengurusan Hartabenda dan Penilaian, Fakulti Ukur, Universiti Teknologi Malaysia.
- Keahlian iktisas : i) Fellow of the Royal Institution of Chartered Surveyors.
ii) Fellow of the Institution of Surveyors, Malaysia.
iii) Jurukur Berdaftar, Lembaga Jurukur Malaysia.
- Pengalaman : i) Pegawai Penilaian di Bahagian Penilaian, Perbendaharaan Malaysia.
(Julai 1965 – Oktober 1973)
ii) Pengarah Penilaian Kawasan di Negeri Sembilan/Melaka (1970 – 1973) dan Selangor (April – Oktober 1973).
iii) Pensyarah Kanan (sekarang Professor Madya), Universiti Teknologi Malaysia, (November 1973 hingga sekarang).

R. W. COUCHMAN

- Tarikh lahir : 19hb. November, 1948
- Kelulusan : i) B.Sc. (Estate Management) Southbank Polytechnic London (1968 – 1972).
ii) A.R.I.C.S. (November 1973)

- Jawatan : Professor Madya,
Fakulti Ukur, Universiti Teknologi Malaysia.
- Pengalaman : i) Pensyarah/Pensyarah Kanan,
Portsmouth Polytechnic (1972 – 1977)
ii) Pensyarah/Pensyarah Kanan,
Hong Kong Polytechnic (1977 – 1979)
iii) Pensyarah Kanan,
Royal Agricultural College (1979 –
1980)
iv) Professor Madya,
Universiti Teknologi Malaysia (1980)
v) Berkhidmat dengan The Ministry of
Defence Land Agent's Office, Aldershot.
vi) Berkhidmat dengan Collier and Collier,
Chartered Surveyors.
vii) Amalan perundingan secara persendirian.

KHALID RASHID UPPAL

- Tarikh lahir : 5hb. Mei, 1938
- Kelulusan : B.Sc. (Mech. Eng) (Pb) 1960
M.Sc. (Thermo) (Birm) 1966
Ph.D (Mech. Eng) (Birm) 1968
- Jawatan : Professor,
Fakulti Kejuruteraan Jentera,
Universiti Teknologi Malaysia.
- Keahlian iktisas : P.Eng., Mem.I.E. Malaysia,
C. Eng., F.I. Mech. E. (Lond),
C.B.S.T., Mem. C.I.B.S. (Lond),
Mem. A.S.M.E. (NY),
Mem. A.S.H.R.A.E. (NY).
- Pengalaman : i) Pensyarah,
Jabatan Kejuruteraan Jentera,
University of Engineering and Techno-
logy,
Lahore, Pakistan.
(September 1960 – Jun 1967)

- ii) Professor Madya,
Jabatan Kejuruteraan Jentera,
University of Engineering and Techno-
logy,
Lahore, Pakistan.
(Jun 1967 – Jun 1975)
- iii) Professor,
Fakulti Kejuruteraan Jentera,
Universiti Teknologi Malaysia,
Kuala Lumpur.
(Jun 1975 hingga sekarang)

.S. KANNAN

- tarikh lahir : 22hb. Julai, 1946
- kelulusan : Sarjanamuda Kejuruteraan (Jentera),
Universiti Malaya. (Jun 1968).

Sarjana Sains (Kejuruteraan Jentera),
U.M.I.S.T. (Disember 1974)
- jawatan : Professor Madya,
Fakulti Kejuruteraan Jentera,
Universiti Teknologi Malaysia.
- keahlian iktisas : i) Ahli Bersekutu, Institut Kejuruteraan
Jentera, U.K.
ii) Chartered Engineer – C.E.I.
iii) Ahli Bersekutu, Institut Jurutera Malaysia
iv) Jurutera Profesyenal, Lembaga Jurutera
Malaysia.
- pengalaman : i) Telah melibatkan diri dalam bidang aka-
demik sejak 27hb. September, 1968.

ii) Sebagai Ketua Jabatan (Jun 1975 –
Januari 1976) dan Timbalan Dekan
(Februari 1976 – April 1980),
Fakulti Kejuruteraan Jentera,
Universiti Teknologi Malaysia.

iii) Berkhidmat dengan Lembaga Peperiksa-
an Malaysia sebagai Ketua Pasukan

(bagi pemeriksaan kertas soalan dan penggubal kertas soalan).

- iv) Ahli Majlis,
Institut Jurutera Malaysia.
- v) Berkhidmat dengan Tentera Laut Di
Raja Malaysia sebagai Pegawai Teknik
dalam Pasukan Simpanan.

MOHD ZAIN BIN HAJI YUSUF

- Tarikh lahir : 10hb. April, 1949
- Kelulusan : i) Diploma Kejuruteraan Awam, Maktab
Teknik – Mei 1971.
ii) Sarjanamuda Kejuruteraan Awam,
University of Strathclyde – Mei 1974
iii) Sarjana Kejuruteraan Awam (Geoteknikal)
University of Mississippi,
U.S.A. – Mei 1978.
- Jawatan : Timbalan Dekan,
Fakulti Kejuruteraan Awam,
Universiti Teknologi Malaysia.
- Pengalaman : i) Ketua Jabatan Tanah dan Geologi,
Fakulti Kejuruteraan Awam,
Universiti Teknologi Malaysia.
(Mei 1978 – September 1980)
ii) Timbalan Dekan,
Fakulti Kejuruteraan Awam,
Universiti Teknologi Malaysia,
(Oktober 1980 hingga sekarang)

MOHAMED ARIF BIN NUN

- Tarikh lahir : 29hb. Julai, 1945
- Kelulusan : B.Sc. Hons. (University of London – 1971)
M.Sc. (Loughborough University – 1972)
Ph.D. (Loughborough University – 1977)

- Jawatan : Ketua Jabatan Kejuruteraan Perhubungan
dan
Ketua Makmal Sistem Komputer ini,
Fakulti Kejuruteraan Elektrik,
Universiti Teknologi Malaysia.
- Pengalaman : Penglibatan dalam prosesan isyarat, teori
automata, pengantaran data, Kejuruteraan
Komputer dan pemeroses mikro.