PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H03M 13/27, 13/29

A1

(11) International Publication Number: **WO 00/62426**

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/IB00/00375

(22) International Filing Date: 29 March 2000 (29.03.00)

(30) Priority Data:
09/291,353 14 April 1999 (14.04.99) US

(71) Applicant: NORTEL NETWORKS LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors: LI, Bin; 1908–1316 Carling Avenue, Ottawa, Ontario K1Z 7L1 (CA). TONG, Wen; #903–1000 Castle Hill Crest, Ottawa, Ontario K2C 3L7 (CA).

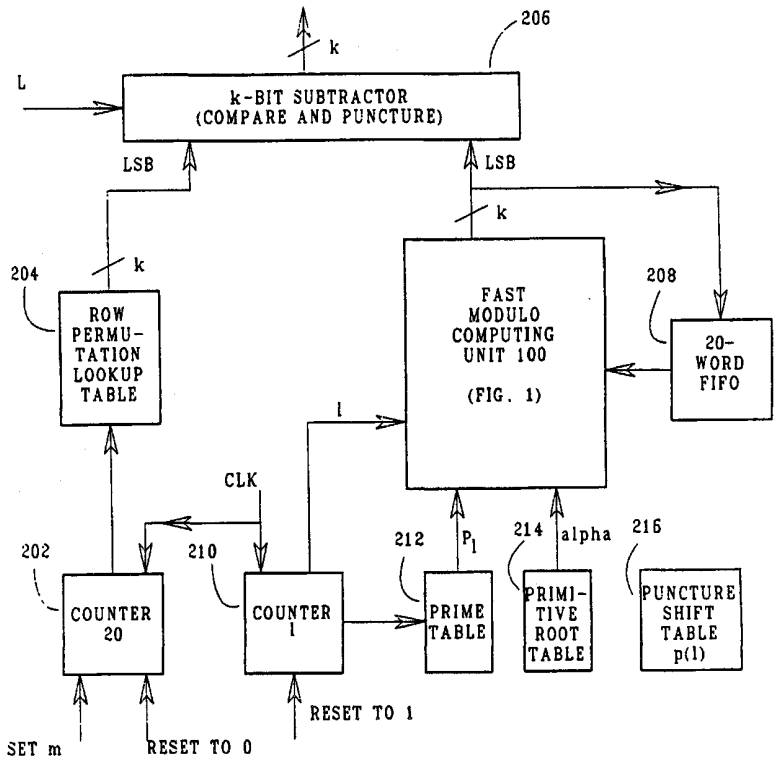
(81) Designated States: BR, CA, CN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: INTRA–ROW PERMUTATION FOR TURBOCODE

(57) Abstract

An interleaver in which a frame of data to be interleaved is stored in at least a portion of an array having R rows and C columns, the portion having $N_r^{(1)}$ rows and $N_c^{(1)}$ columns that satisfy the inequality $N_r^{(1)} \times N_c^{(1-1)} < L < N_r^{(1)} \times N_c^{(1)}$ where $N_c^{(1)}$ is a prime number and $N_c^{(1-1)}$ is the highest prime number less than $N_c^{(1)}$. The elements of each row are permuted according to a predetermined mathematical relationship, and the rows are permuted according to predetermined mapping.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTRA-ROW PERMUTATION FOR TURBOCODE

FIELD OF THE INVENTION

This invention relates generally to communication systems and, more particularly to interleavers for performing code modulation.

BACKGROUND OF THE INVENTION

Techniques for encoding communication channels, known as coded modulation, have been found to improve the bit error rate (BER) of electronic communication systems such as modem and wireless communication systems. Turbo coded modulation has proven to be a practical, power-efficient, and bandwidth-efficient modulation method for "random-error" channels characterized by additive white Gaussian noise (AWGN) or fading. These random-error channels can be found, for example, in the code division multiple access (CDMA) environment. Since the capacity of a CDMA environment is dependent upon the operating signal to noise ratio, improved performance translates into higher capacity.

An aspect of turbo coders which makes them so effective is an interleaver which permutes the original received or transmitted data frame before it is input to a second encoder. The permuting is accomplished by randomizing portions of the signal based upon one or more randomizing algorithms. Combining the permuted data frames with the original data frames has been shown to achieve low BERs in AWGN and fading channels. The interleaving process increases the diversity in the data such that if the modulated symbol is distorted in transmission the error may be recoverable with the use of error correcting algorithms in the decoder.

A conventional interleaver collects, or frames, the signal points to be transmitted into an array, where the array is sequentially filled up row by row. After a predefined number of signal points have been framed, the interleaver is emptied by sequentially reading out the array column by column for transmission. As a result, signal points in the same row of the array that were near each other in the original signal point flow are separated by a number of signal points equal to

the number of rows in the array. Ideally, the number of columns and rows would be picked such that interdependent signal points, after transmission, would be separated by more than the expected length of an error burst for the channel.

Non-uniform interleaving achieves "maximum scattering" of data and "maximum disorder" of the output sequence. Thus the redundancy introduced by the two convolutional encoders is more equally spread in the output sequence of the turbo encoder. The minimum distance is increased to much higher values than for uniform interleaving. A persistent problem for non-uniform interleaving is how to practically implement the interleaving while achieving sufficient "non-uniformity," and minimizing delay compensations which limit the use for applications with real-time requirements.

Finding an effective interleaver is a current topic in the third generation CDMA standard activities. It has been determined and generally agreed that, as the frame size approaches infinity, the most effective interleaver is the random interleaver. However, for finite frame sizes, the decision as to the most effective interleaver is still open for discussion. Decreasing the amount of memory space (RAM or ROM) needed to store the information required to carry out an interleaving scheme is also a subject of current discussion.

Accordingly there exists a need for systems and methods of interleaving codes that improve non-uniformity for finite frame sizes.

There also exists a need for such systems and methods of interleaving codes which are relatively simple to implement, including having relatively low memory space requirements.

It is thus an object of the present invention to provide systems and methods of interleaving codes that improve non-uniformity for finite frame sizes.

It is also an object of the present invention to provide systems and methods of interleaving codes which are relatively simple to implement and which have relatively low memory space requirements.

These and other objects of the invention will become apparent to those skilled in the art from the following description thereof.

SUMMARY OF THE INVENTION

The foregoing objects, and others, may be accomplished by the present invention, which includes an interleaver for interleaving these data frames. The interleaver includes a storage area containing an array large enough to store the largest expected data frame. A frame of size L elements to be interleaved is stored in $N_r^{(1)}$ rows and $N_c^{(1)}$ columns of the array, where $N_r^{(1)}$ is a predetermined integer and $N_c^{(1)}$ is a prime number which satisfy the inequality

$$N_r^{(1)} \times N_c^{(1-1)} < L < N_r^{(1)} \times N_c^{(1)}$$

where $N_c^{(1-1)}$ is the highest prime number less than $N_c^{(1)}$. The elements of each row are permuted according to a predetermined mathematical relationship, and the rows are permuted according to predetermined mapping.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be more clearly understood by reference to the following detailed description of an exemplary embodiment in conjunction with the accompanying drawings, in
which:

Fig. 1 depicts a fast modulo computing embodiment according to the present invention; and

Fig. 2 depicts the structure of an interleaver according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention finds embodiment as a turbo encoder in a CDMA radio communication system. A stream of bits to be transmitted is divided into a series of frames, each frame including a number L of elements, each element being at least one bit.

Each frame is to be interleaved prior to transmission. If there are a large number of possible frame sizes L, specifying an interleaver for each possible frame size results in a necessity for storing a large number of parameters.

The invention reduces the number of parameters that must be stored by providing a reduced number of prototype interleavers (or mother interleavers), each for a one of a subset of frame sizes, selecting one of the mother interleavers at least large enough to interleave a current frame of size L, and puncturing the interleaved frame to a size of L bits.

The maximum size of an array for storing a frame to be interleaved is N_r rows x N_c columns. For a given frame size L, a mother interleaver is chosen having an array of size of

$N_r^{(1)}$ rows x $N_c^{(1)}$ columns, such that:

$N_r^{(1)} \times N_c^{(1-1)} < L < N_r^{(1)} \times N_c^{(1)}$

and after interleaving the array is punctured to size L.

While it is possible to design a good mother interleaver with exact dimensions $N_r^{(1)}$ x $N_c^{(1)}$, the performance of an interleaver for a frame size punctured from the mother interleaver's size cannot, under any conventional systems, be guaranteed.

The invention provides an interleaver which can adapt to arbitrary frame size by providing a scheme for proper selection (optimization) of parameters

$N_r^{(1)}$ $1 = 1, 2, \ldots R$ (max. no. of rows)

$N_c^{(1)}$ $1 = 1, 2, \ldots C$ (max. no. of columns)

In one embodiment of the invention, a fixed value is selected for the number of rows N_r, and the number of columns $N_c^{(1)}$ is selected from a set of prime numbers (non-uniform grid), i.;

e. $N_c^{(1)} = P_1$. (In an alternative embodiment of the invention a uniform grid is employed, such as $P_1 = 1 \times \text{delta}$.)

The core of the interleaving procedure employing the present invention generally comprises:

i) Writing the frame elements into the $N_r^{(1)} \times N_c^{(1)}$ working array row by row;

ii) Permuting the columns i of each row j according to

$$c_j(i) = [\alpha_j \times c_j(i-1)] \bmod P_1 \quad j = 1,2,\ldots R \quad i = 1,2,\ldots C$$

iii) Permuting the rows according to a predetermined mapping; and

iv) Reading out the frame elements column by column.

The intra-row permutation (item ii) is based on a complete residual system of modulo P_1. That is, α_j is selected from all possible exponential congruent roots of P_1:

$$\alpha_j = \{\alpha_1, \alpha_2, \ldots \alpha_\Phi\}$$

The intra-row permutation uses a special root called the primitive root α_p of prime P_1 to construct the set of roots α_j by using a reduced residual system as:

$$\overline{\alpha}_j = \{\alpha_p^{p(1)}, \alpha_p^{p(2)}, \ldots \alpha_\Phi^{p(R)}\}$$

It should be noted that $\overline{\alpha}_j$ is a subset of α_j. The advantage of using this special reduced system is to add additional constraints on the intra-row permutation roots to simplify the search computing for the parameter optimization.

For an embodiment of the invention, a set of prime numbers is chosen:

$$\{p(1), p(2), \ldots p(R)\}$$

under the condition that

$$\gcd\{p(i), P_1-1\} = 1$$

(gcd connotes "greatest common denominator").

In such a case:

$$c_1(i) = [\alpha_p^{p(1)} \times c_1(i-1)] \bmod P_1$$

is equivalent to a decimated sampling (with rate sampling ratio p(1)) of the complete residual system generated by the primitive root. Therefore, the intra-row permutation may be accomplished as:

a) permuting the first row using the primitive root α_p of P_1:

$$c_1(i) = [\alpha_p^{p(1)} \times c_1(i-1)] \bmod P_1$$

and

b) permuting the rest of the rows using the cyclic shift by p(j) of the first-row permutation:

$$c_j(i) = c_1([i \times p(j))] \bmod P_1).$$

This is equivalent to the cyclic group

$$c_j(i) = [\alpha_j^{p(j)} c_j(i-1)] \bmod P_1)$$

where $j = 2,3,\ldots R$

$i = 1,2,\ldots C.$

In this case, the intra-row permutation rule is a deterministic one. The interleaver optimization is performed by searching a set of primes for cyclic shift of the primitive complete residual system. For example, if R=20 (i.e., a matrix with 20 rows and P_i columns) a prime set might be chosen as

p(1)={7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83}

[Example 1]

For each prime (column number) such a set is chosen. To cover a range of frame sizes from 320 bits to 8192 bits, at least 75 mother interleavers are provided. The column dimensions used for each are listed in Table 1 together with associated primitive roots. Seventy-six primes are listen in Table 1 in order to provide a value for the lowest $N_c^{(1-1)}$.

A	B	C	A	B	C	A	B	C	A	B	C
13	2	21	97	5	21	193	5	21	307	5	21
17	3	21	101	2	21	197	2	21	311	17	4
19	2	21	103	5	21	199	3	21	313	10	21
23	5	21	107	2	9	211	2	21	317	2	15
29	2	21	109	6	21	223	3	5	331	3	21
31	3	21	113	3	21	227	2	21	337	10	21
37	2	21	127	3	21	229	6	1	347	2	21
41	6	21	131	2	21	233	3	3	349	2	3
43	3	21	137	3	21	239	7	21	353	3	21
47	5	2	139	2	2	241	7	21	359	7	21
53	2	21	149	2	5	251	6	21	367	6	11
59	2	3	151	6	21	257	3	21	373	2	4
61	2	21	157	5	21	263	5	21	379	2	21
67	2	21	163	2	21	269	2	12	383	5	21
71	7	21	167	5	16	271	6	21	389	2	18
73	5	21	173	2	7	277	5	2	397	5	21
79	3	21	179	2	17	281	3	21	401	3	21
83	2	6	181	2	21	283	3	8	409	21	21
89	3	21	191	19	1	293	2	14	419	2	1

(A = prime number $N_c^{(1)}$; B = primitive root α_p; C = puncture)

Table 1

In a practice of the present invention, the storage requirement for the set of primitive roots is reduced by using a set of twenty-one consecutive primes (in the present example (Example 1), adding the prime 89 to the exemplary twenty primes p(l) given above).

There is then at most one number that does not satisfy

$$\gcd\{p(i), P_i - 1\} = 1.$$

In a case where such a number occurs, it is punctured from p(l) set. In a case where all primes in p(l) satisfy such a condition, the last (twenty-first) prime (89 in the current example (Example 1)) is punctured. Thus, for each prime given in Table 1 (column A), there is also given the primitive root (column B) and the position which should be punctured (column C). The memory requirement for the data given in Table 1 is:

Prime Numbers: 589 bits
Primitive Roots: 159 bits
Puncture Pattern: 322 bits
Prime Set p(l): 120 bits
Total: 1190 bits or 149 bytes.

A practice of the invention based on fast modulo computing will now be described:

Any prime number P can be described by the condition:

$$P = 2^k - 1.$$

Given any number $x < P$, the following decomposition applies:

$$x = m \times 2^k + c$$
$$= m \times (2^k - 1) + lm + c$$
$$= m \times p + lm + c$$

Therefore:

$$[x] \bmod P = [lm + c] \bmod P \quad [Eq. 1]$$

and the modulo value can be computed in such a recursive fashion. (In the special case that $l = 1$, only a single iteration is required.)

Since $\alpha < P$, and thus $\alpha \times (k) < P^2$, a multiplier may be employed that is 2k bits in width. Also:

$$\log_2[m] < k \text{ and } \log_2[c] < k.$$

The modulo P value can be computed according to Eq. 1 by multiplying a k-bit LSB with l and then adding a k-bit MSB. If the sum is more than k bits wide, Eq. 1 must be reinvoked, i.e.:

$$[lm + c] \bmod P = [m' + c'] \bmod P$$
$$= m' + c'.$$

In the extreme case:

$$m = \{111\ldots1\}_{k \text{ bits}}$$

and

$$c = \{111\ldots1\}_{k \text{ bits}},$$

and thus

$$m' = \{1\}_{1 \text{ bit}}$$

and

$$c' = \{111\ldots10\}_{k \text{ bits}}.$$

Hence,

$$\log_2[c' = m'] < k.$$

An embodiment of the modulo P calculation presented here is depicted in Fig. 1. An overall embodiment of the interleaver presented here is depicted in Fig. 2.

The interleaver parameters are to be selected according to the given intra-row congruential rule. It is known that once the recursive convolutional code (RCC) constituent code is determined, error performance is characterized by the input

and output weight of error events of the constituent decoders. (The input weight is the number of bit errors.) It is known that the performance of Turbo codes at high SNR is dictated by output error events with input weight 2. The effective free distance is the minimum output weight of all error events of input weight 2. A key to optimizing the interleaver parameters is to identify parameter sets which minimize low-weight error events, with the patterns shown in Table 3 as criteria.

Weight-2 $1+D^i$		Weight-3 $1+D^i+D^j$		Weight-4 $1+D^i+D^j+D^k$	
len.	i	len.	i,j	len.	i,j,k
8	7	4	2,3	7	1,3,6
15	14	6	1,5	10	1,4,9
22	21	7	4,6	5	1,2,4
29	28	9	5,8	11	1,6,10
		10	3,9	9	1,7,8
		11	2,10	12	1,2,11
		11	9,10	9	2,4,8
		12	6,11	7	2,5,6
		13	1,12	10	2,7,9
		13	8,12	6	3,4,5
		14	4,13	11	3,7,10
		14	11,13	10	4,8,9
		16	5,15	12	4,7,11
		16	12,15	12	5,10,11
				12	8,9,11

Table 2

For example, if an input pattern has weight-2 (e.g., two 1 bits with six 0's between them, then according to the Weight-2 column of Table 3 a set of interleaver parameters is sought that produce an output with 1 bits in the zero'th (initial) and seventh, fourteenth, twenty-first, or twenty-eight positions (according to length) with six, thirteen, twenty, or twenty-seven 0 bits, respectively, between the two one bits. This may be expressed as verifying 1 bits in zero'th and i'th positions.

In similar application of this "low-weight filtering technique", weight-3 streams are checked for 1 bits in the zero'th, i'th, and j'th positions. Weight-4 streams are

checked for 1 bits in the zero'th i'th, j'th, and k'th positions.

Although the embodiment described above is a turbo encoder such as is found in a CDMA system, those skilled in the art realize that the practice of the invention is not limited thereto and that the invention may be practiced for any type of interleaving and de-interleaving in any communication system.

It will thus be seen that the invention efficiently attains the objects set forth above, among those made apparent from the preceding description. In particular, the invention provides improved apparatus and methods of interleaving codes of finite length while minimizing the complexity of the implementation and the amount of storage space required for parameter storage.

It will be understood that changes may be made in the above construction and in the foregoing sequences of operation without departing from the scope of the invention. It is accordingly intended that all matter contained in the above description or shown in the accompanying drawings be interpreted as illustrative rather than in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention as described herein, and all statements of the scope of the invention which, as a matter of language, might be said to fall therebetween. Having described the invention, what is claimed as new and secured by Letters Patent is:

1. A method of interleaving elements of frames of data, the method comprising:

providing a storage array c of R rows and C columns, where R and C are positive integers;

storing a frame of data comprising a plurality L of elements in a working array within the storage array c, the working array having $N_r^{(1)}$ rows and $N_c^{(1)}$ columns, where:

$N_r^{(1)}$ is a positive integer no greater than R;

$N_c^{(1)}$ is a prime number no greater than C; and

$N_r^{(1)} \times N_c^{(1-1)} < L < N_r^{(1)} \times N_c^{(1)}$;

where $N_c^{(1-1)}$ is the highest prime number less than $N_c^{(1)}$, and

permuting the elements of each row of the storage array c according to a predetermined mathematical relationship.

2. The method according to claim 1 wherein the predetermined mathematical relationship for permuting the elements of each row of the storage array c is:

$c_j = [\alpha_j \times c_j(i-1)] \bmod P_l$

where:

$j = 1, 2, \ldots R$;

$i = 1, 2, \ldots C$;

P is a set of contiguous prime numbers;

P_l is equal to $N_c^{(1)}$; and

α_j is selected from exponential congruent roots of P_l.

3. The method according to claim 2 further comprising permuting the rows of the storage array c according to predetermined mapping.

4. The method according to claim 3 further comprising storing said frame of data in row-by-row order, and reading out said frame of data after permutation in column-by-column order.

5. The method according to claim 2 wherein the values of α_j are selected from exponential congruent roots of P_1 according to

$$\alpha_j = \{\alpha_p^{p(1)}, \alpha_p^{p(2)}, \ldots \alpha_\Phi^{p(R)}\}$$

where:

α_p is the primitive root of P_1; and

gcd $\{p(i), P_1-1\} = 1$.

6. The method according to claim 2 wherein the values of α_j are selected from among j+1 values by eliminating a value for which gcd $\{p(i), P_1-1\}$ is not equal to 1.

7. The method according to claim 2 wherein:
the values of α_j are selected from among values found to produce minimum bit errors with low-weight input data.

8. The method according to claim 2, wherein the values of α_j associated with each value of $N_c^{(1)}$ are precomputed and stored.

9. An interleaver for interleaving elements of frames of data, the interleaver comprising:
a memory containing at least a storage array c of R rows and C columns, where R and C are positive integers;
a memory read-write circuit storing a frame of data comprising a plurality L of elements in a working array within the storage array c, the working array having $N_r^{(1)}$ rows and $N_c^{(1)}$ columns, where:

$N_r^{(1)}$ is a positive integer no greater than R;

$N_c^{(1)}$ is a prime number no greater than C; and

$N_r^{(1)} \times N_c^{(1-1)} < L < N_r^{(1)} \times N_c^{(1)}$;

where $N_c^{(1-1)}$ is the highest prime number less than $N_c^{(1)}$, and
an ALU adapted to permute the elements of each row of the storage array c according to a predetermined mathematical relationship.

10. The interleaver according to claim 9 wherein the ALU is adapted to permute the elements of each row of the storage array c according to:

$c_j = [\alpha_j \times c_j(i-1)] \bmod P_1$

where:

$j = 1, 2, \ldots R;$

$i = 1, 2, \ldots C;$

P is a set of contiguous prime numbers;

P_1 is equal to $N_c^{(1)}$; and

α_j is selected from exponential congruent roots of P_1.

11. The interleaver according to claim 10 wherein the ALU permutes the rows of the storage array c according to predetermined mapping.

12. The interleaver according to claim 11 wherein the memory read-write circuit stores said frame of data in row-by-row order, and reads out said frame of data after permutation in column-by-column order.

13. The interleaver according to claim 10 wherein the ALU selects the values of α_j from exponential congruent roots of P_1 according to

$$\alpha_j = \{\alpha_p^{p(1)}, \alpha_p^{p(2)}, \ldots \alpha_\phi^{p(R)}\}$$

where:

α_p is the primitive root of P_1; and

$\gcd\{p(i), P_1-1\} = 1.$

14. The interleaver according to claim 10 wherein the ALU selects the values of α_j from among j+1 values by eliminating a value for which $\gcd\{p(i), P_1-1\}$ is not equal to 1.

15. An interleaver for interleaving elements of frames of data, the interleaver comprising:

memory means containing at least a storage array c of R rows and C columns, where R and C are positive integers;

memory read-write means for storing a frame of data comprising a plurality L of elements in a working array within the storage array c, the working array having $N_r^{(1)}$ rows and $N_c^{(1)}$ columns, where:

$N_r^{(1)}$ is a positive integer no greater than R;

$N_c^{(1)}$ is a prime number no greater than C; and

$N_r^{(1)} \times N_c^{(1-1)} < L < N_r^{(1)} \times N_c^{(1)}$;

where $N_c^{(1-1)}$ is the highest prime number less than $N_c^{(1)}$, and

logic means for permuting the elements of each row of the storage array c according to a predetermined mathematical relationship.

16. The interleaver according to claim 15 wherein the logic means is permutes the elements of each row of the storage array c according to:

$c_j = [\alpha_j \times c_j(i-1)] \bmod P_1$

where:

$j = 1, 2, \ldots R$;

$i = 1, 2, \ldots C$;

P is a set of contiguous prime numbers;

P_1 is equal to $N_c^{(1)}$; and

α_j is selected from exponential congruent roots of P_i.

17. The interleaver according to claim 16 wherein the logic means permutes the rows of the storage array c according to predetermined mapping.

18. The interleaver according to claim 17 wherein the memory read-write means stores said frame of data in row-by-row order, and reads out said frame of data after permutation in column-by-column order.

19. The interleaver according to claim 16 wherein the logic means selects the values of α_j from exponential congruent roots of P_1 according to

$$\alpha_j = \{\alpha_p^{p(1)}, \alpha_p^{p(2)}, \ldots \alpha_\Phi^{p(R)}\}$$

where:

α_p is the primitive root of P_1; and

gcd $\{p(i), P_1-1\} = 1$.

20. The interleaver according to claim 16 wherein the logic means selects the values of α_j from among j+1 values by eliminating a value for which gcd $\{p(i), P_1-1\}$ is not equal to 1.

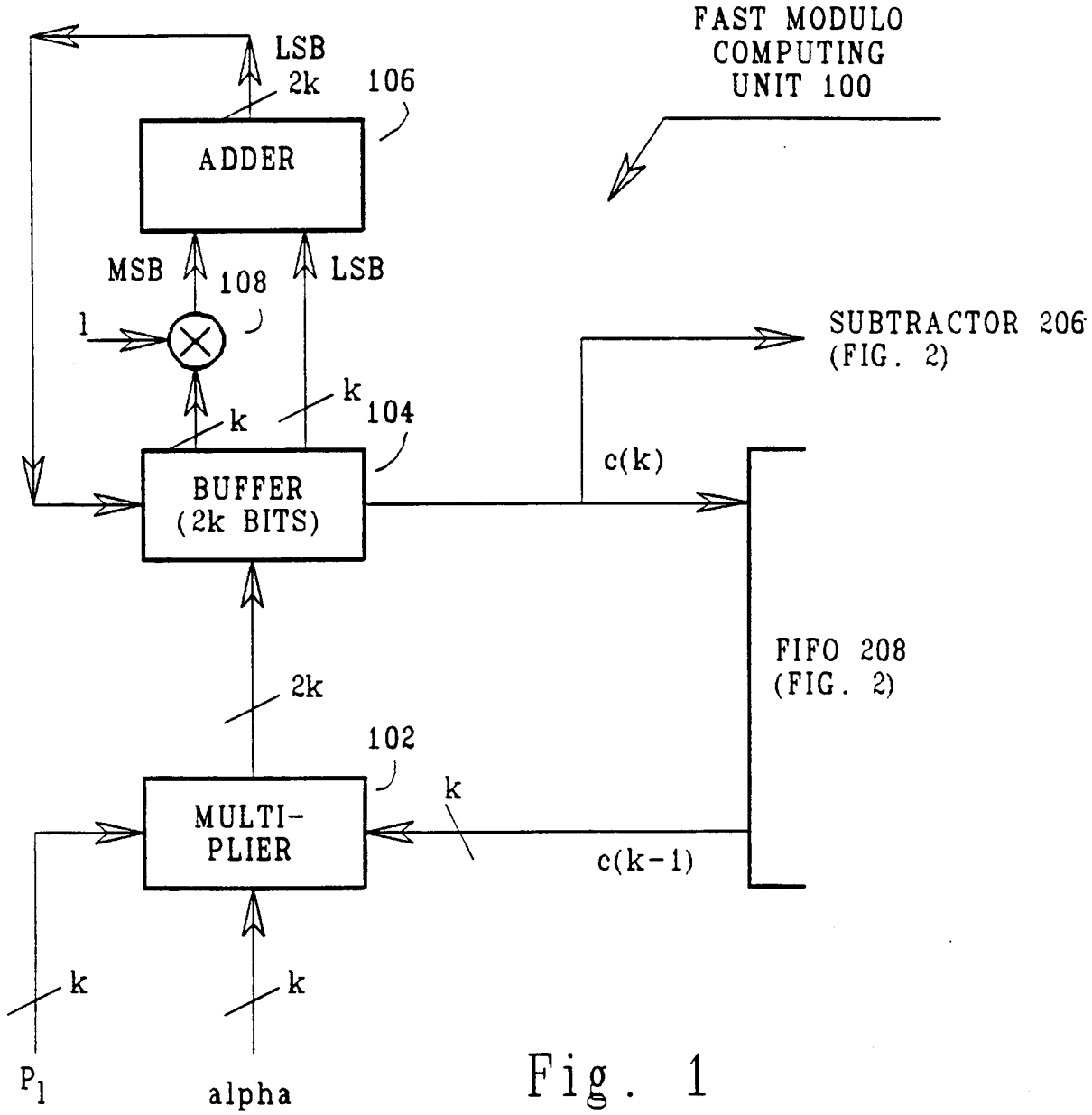

FAST MODULO
COMPUTING
UNIT 100
LSB
2k
106
ADDER
MSB
108
LSB
1
SUBTRACTOR 206
(FIG. 2)
k
k
104
BUFFER
(2k BITS)
c(k)
FIFO 208
(FIG. 2)
2k
102
MULTI-
PLIER
k
c(k-1)
k
k
P1
alpha

Fig. 1

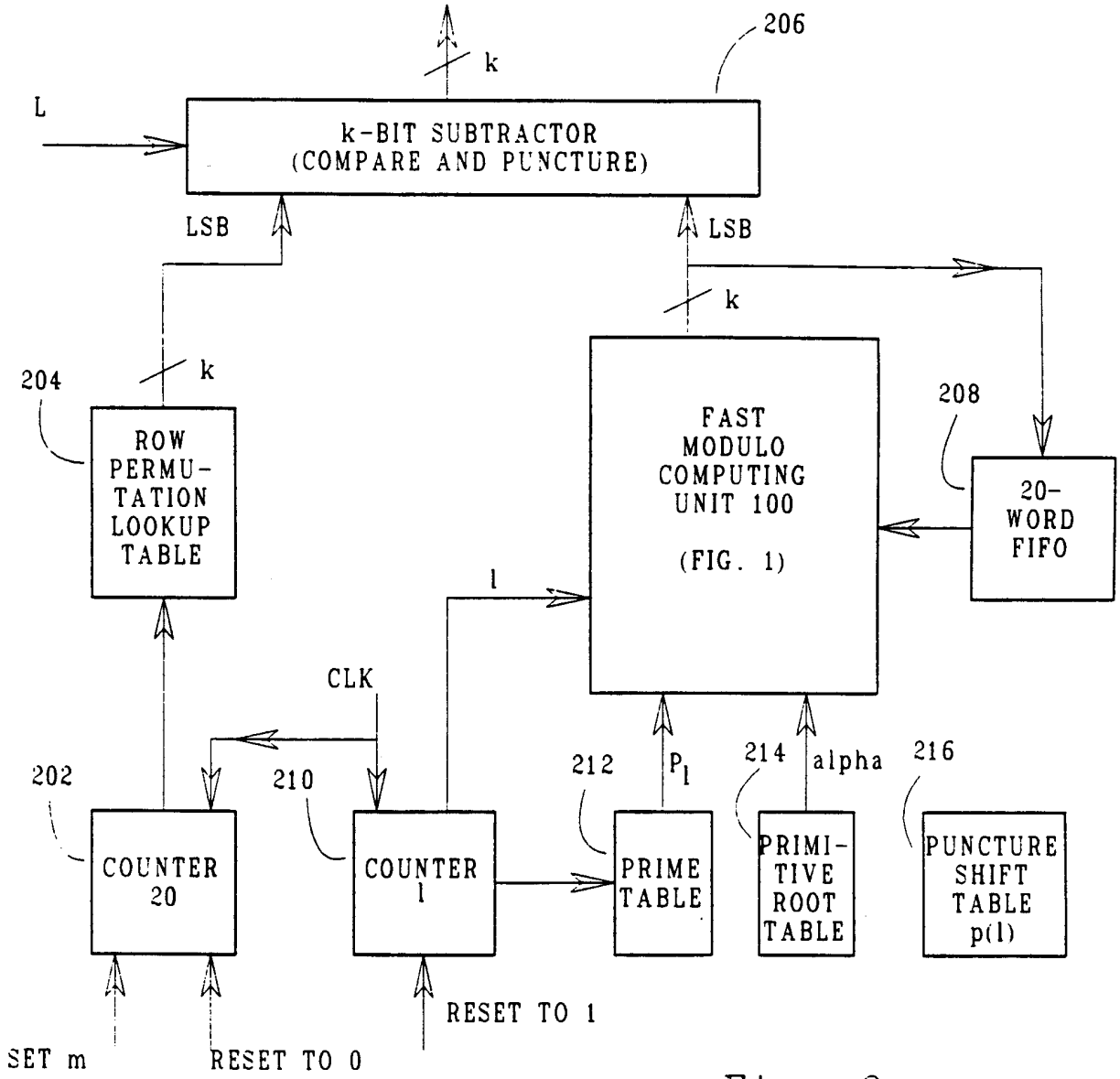

k
206
L
k-BIT SUBTRACTOR
(COMPARE AND PUNCTURE)
LSB
LSB
k
k
204
ROW
PERMU-
TATION
LOOKUP
TABLE
FAST
MODULO
COMPUTING
UNIT 100
(FIG. 1)
208
20-
WORD
FIFO
l
CLK
202
210
212
P_l
214
alpha
216
COUNTER
20
COUNTER
l
PRIME
TABLE
PRIMI-
TIVE
ROOT
TABLE
PUNCTURE
SHIFT
TABLE
p(l)
RESET TO 1
SET m
RESET TO 0

Fig. 2

INTERNATIONAL SEARCH REPORT

Intern. al Application No
PCT/IB 00/00375

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H03M13/27 H03M13/29

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H03M H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	SHIBUTANI A ET AL: "Complexity reduction of turbo decoding " IEEE VTS 50TH VEHICULAR TECHNOLOGY CONFERENCE, vol. 3, 19 - 22 September 1999, pages 1570-1574, XP002142762 Amsterdam, Netherlands the whole document ---	1-5, 7-13, 15-19
P,A	WO 00 08770 A (NORTEL NETWORKS CORP) 17 February 2000 (2000-02-17) the whole document --- -/--	1,2,5, 7-10,13, 15,16,19

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2000	28/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna ıl Application No
PCT/IB 00/00375

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 00 10257 A (HUGHES ELECTRONICS CORP) 24 February 2000 (2000-02-24) the whole document	1-3, 5-11, 13-17, 19,20
A	US 5 742 612 A (DE SEZE FABRICE ET AL) 21 April 1998 (1998-04-21) column 1, line 39 - line 59 column 2, line 19 - line 25 column 2, line 40 -column 3, line 3	1,2,4,7, 9,10,12, 15,16,18
A	US 4 394 642 A (RATTLINGOURD GLEN D ET AL) 19 July 1983 (1983-07-19) column 1, line 34 - line 40	1,3,4,9, 11,12, 15,17,18
A	EP 0 300 139 A (IBM) 25 January 1989 (1989-01-25)	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/IB 00/00375

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0008770 A	17-02-2000	NONE	
WO 0010257 A	24-02-2000	AU 5675499 A	06-03-2000
US 5742612 A	21-04-1998	FR 2706054 A	09-12-1994
		EP 0627821 A	07-12-1994
		EP 0996232 A	26-04-2000
		FI 942512 A	03-12-1994
US 4394642 A	19-07-1983	NONE	
EP 0300139 A	25-01-1989	DE 3882175 A	12-08-1993
		DE 3882175 T	27-01-1994
		JP 1036337 A	07-02-1989
		JP 2506936 B	12-06-1996
		US 4862463 A	29-08-1989