



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

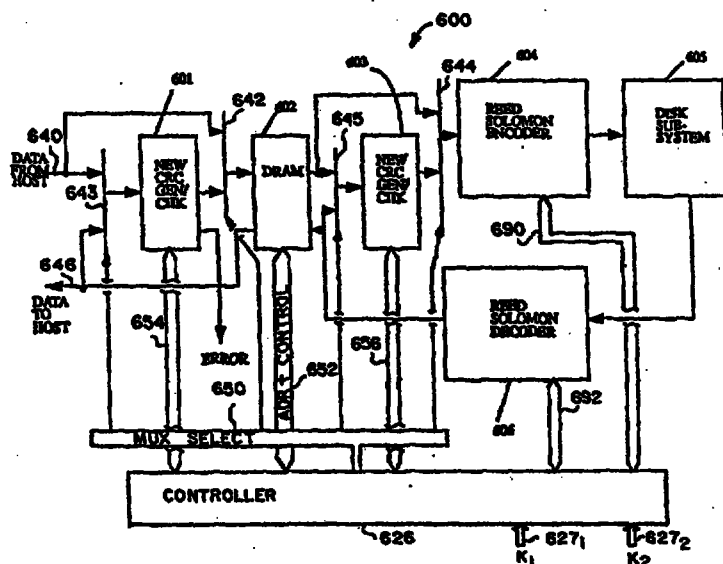
(51) International Patent Classification 6 : H03M 13/00, G06F 11/08	A1	(11) International Publication Number: WO 95/12921 (43) International Publication Date: 11 May 1995 (11.05.95)
(21) International Application Number: PCT/US94/12138 (22) International Filing Date: 18 October 1994 (18.10.94) (30) Priority Data: 147,865 4 November 1993 (04.11.93) US (71) Applicant: CIRRUS LOGIC, INC. [US/US]; 3100 West Warren Avenue, Fremont, CA 94538 (US). (72) Inventor: ZOOK, Christopher, P.; 8901 Sage Valley Road, Longmont, CO 80503 (US). (74) Agents: BURNAM, H., Warren, Jr.; Nixon & Vanderhye, P.C., 8th floor, 1100 North Glebe Road, Arlington, VA 22201-4714 (US) et al.		(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published With international search report.

THIS SHEET HAS BEEN
REPLACED

This Sheet Has Been Replaced



(54) Title: CYCLICAL REDUNDANCY CHECK METHOD AND APPARATUS

**(57) Abstract**

One-stage and two-stage CRC generation systems (400, 600) feature a CRC generator/checker (700) comprising a segmenter (710) of an input data stream into substreams, a circuit (712) forming a linear combination of the substreams and generating CRC bytes therefrom, and a checker (714) comparing the CRC bytes with previously generated CRC bytes. The two-stage system (600) includes a first CRC generator/checker (601) generating primary CRC bytes, a memory (602) receiving the input data and the primary CRC bytes, and a second CRC generator/checker (603) generating verification CRC bytes for comparison with the primary CRC bytes to check the input data after retrieval from the memory (602) and before input to an encoder (604). The second CRC generator/checker (603) can optionally apply some of the verification CRC bytes to the encoder (604) for use as secondary CRC bytes. The number of CRC bytes outputted by the CRC generator/checkers (601, 603) is programmable.

THIS SHEET HAS BEEN REPLACED

-1-

**CYCLICAL REDUNDANCY CHECK
METHOD AND APPARATUS**

BACKGROUND

Cross-References to Related Applications

This patent application is a continuation application of United States Patent Application Serial Number 08/147,865; filed November 4, 1993, entitled DUAL
5 PURPOSE CYCLICAL REDUNDANCY CHECK, which is incorporated herein by reference. Patent applications filed concurrently (inventor: Christopher P. Zook) with this patent application and incorporated herein by reference U.S. Patent Application Serial Number 08/____,____ (attorney docket: 1777-6) entitled
10 "FINITE FIELD INVERSION"; U.S. Patent Application Serial Number 08/____,____ (attorney docket: 1777-9) entitled "BURST ERROR CORRECTOR", U.S. Patent Application Serial Number 08/____,____ (attorney docket: 1777-7) entitled "REED SOLOMON DECODER", and U.S. Patent Application Serial Number
15 08/____,____ (attorney docket 1777-10) entitled "ERROR CORRECTION METHOD AND APPARATUS". Patent applications filed concurrently with United States Patent Application Serial Number 08/147,865 filed November 4, 1993 (and all hereby incorporated herein by reference) include U.S. Patent
20 Application Serial Number 08/147,758 entitled "FINITE FIELD INVERSION", U.S. Patent Application Serial Number 08/148,068 entitled "BURST ERROR CORRECTOR", and U.S. Patent Application Serial Number 08/147,650, entitled "REED SOLOMON DETECTOR".

1. Field of Invention

This invention relates generally to digital data communication systems, particularly to the detection of transmission errors by the use of codes.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-2-

2. Related Art and Other Considerations

In a digital data communication system (including storage and retrieval from electronic memory, optical media or magnetic media) errors may occur as a result of noise, media defects or circuit failure. For reliable communications it is necessary to be reasonably sure of detecting all transmission errors. One way of doing this is by the use of cyclic redundancy check symbols or CRCs. In general CRCs are calculated by treating the data as the coefficients of a polynomial, dividing the data by another polynomial, and keeping the remainder. The data and CRC together make up a codeword which is then transmitted into the communication channel. At a receiving end of the channel a CRC is again calculated and compared to the original. A discrepancy between the two CRCs indicates a transmission error.

In some applications the data and CRC together are coded into an error-correcting code by adding error-correcting characters (ECC). After a correction procedure has been used the CRC can be used to detect errors that are either not detected or are miscorrected by the corrector.

The data can be viewed as a sequence of binary bits or a sequence of multi-bit symbols. In general a bit-oriented CRC is desired if the expected errors are random bit errors and a symbol-oriented CRC is desired if the expected errors are burst errors or random symbol errors.

Fig. 1 shows a typical bit-oriented 8-bit CRC generator where the serial input is on the DATA line. The generator in Fig. 1 will generate an 8-bit CRC character which can be used to detect any error which affects at most two bits in the serial data stream.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-3-

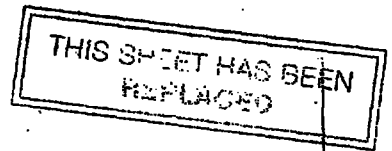
Fig. 2 shows a typical byte-oriented 8-bit CRC generator where D_0 to D_7 make up the input data byte. The generator in Fig. 2 will generate an 8-bit CRC character which can be used to detect any single-byte error. It cannot, however, detect every two-bit error since the two errors could be in two different bytes.

Fig. 3 shows a data transmission system which includes a dynamic RAM (DRAM) for temporary storage and a communication channel which could be, for example, magnetic storage. The system uses an ECC system to correct errors occurring in the communication channel. It also employs a two-byte CRC to check for errors in data retrieved from the DRAM and to check the results of the corrector. For ECC purposes the data is partitioned into three interleaves. Each interleave makes up one ECC codeword containing two ECC bytes which can correct one byte in each interleave. This is a common technique for making a system capable of correcting a burst error of three bytes but using an ECC capable of correcting only one byte. Conceptually, during ECC generation using the system of Fig. 3, the first data byte goes into ECC generator 1, the second byte goes into ECC generator 2, the third byte goes into ECC generator 3, the fourth byte goes into ECC generator 1, etc. After the data has been input to the generators the first ECC byte comes from the generator which follows the generator which received the last data byte and the remaining ECC bytes are taken from the generators in the same sequence as previously described. All signal lines are 8 bits wide.

The CRC system of Fig. 3 will detect all two-byte errors (and consequently all two-bit errors) in a block of data read from the DRAM. However, regardless of which CRC and ECC polynomials are used, it is possible to have three errors in one interleave which are not detected by the ECC or CRC.

This Sheet Has Been Replaced





-4-

SUMMARY

The invention features both one stage and two stage CRC generation systems which include a programmable CRC generator/checker. The CRC generation/checker comprises a segmenting circuit (for segmenting an input stream of user data into a plurality m of sub-streams); a circuit which forms a linear combination of the plurality m of sub-streams and operates upon the linear combination in order to generate CRC bytes; and, a checker circuit for comparing the generated CRC bytes with previously generated CRC bytes.

In connection with preparation of CRC bytes prior to an encoding operation of a two stage system, input user data is first applied to a first CRC generator/checker for the generation of K_1 number of primary CRC bytes. The input user data and associated resultant CRC bytes are then stored in a memory. Prior to encoding, a data block obtained from the memory (including both the user data and the primary CRC bytes) is applied to a second CRC generator/checker. User data from the memory is utilized by the second CRC generator/checker to generate verification CRC bytes. Following generation of the verification CRC information units, during K_1 number of verification clock cycles, the first K_1^{th} verification CRC bytes are compared with the K_1 number of primary CRC bytes for the purpose of detecting any errors occurring with respect to the memory. After the verification, a number $K_2 - K_1$ of verification CRC bytes generated by the second CRC generator/checker is optionally applied to the encoder as secondary CRC bytes, thereby adding additional CRC information prior to encoding and storage of a block on a storage medium.

In connection with processing of CRC information after a decoding operation of a two stage system, decoded user data (including CRC bytes) is applied both to the second CRC generator/checker and to the memory. The second CRC generator/checker receives the user data and CRC bytes

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-5-

in much the same manner as it does prior to an encoding operation, generating K_2 number of verification CRC bytes for comparison with a like number of corresponding CRC bytes obtained from the decoded data. When the decoded data is
5 retrieved from the memory for sending to a host, the decoded data is sent to the first CRC generator/checker to check for memory errors.

The first CRC generator/checker and the second CRC generator/checker are configured to generate as many as k
10 number of CRC bytes. However, the number of CRC bytes K_1 and K_2 actually outputted by the respective first and second CRC generator/checkers is programmable, so that K_1 and K_2 may be unequal (e.g., $K_2 > K_1$) for a specified encoding/decoding operation and changeable from one
15 encoding/decoding operation to another.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features, and advantages of the invention will be apparent from the
20 following more particular description of preferred embodiments as illustrated in the accompanying drawings in which reference characters refer to the same parts throughout the various views. The drawings are not necessarily to scale, emphasis instead being placed upon
25 illustrating the principles of the invention.

Fig. 1 is a schematic block diagrammatic view of a typical bit-oriented 8-bit CRC generator.

Fig. 2 is a schematic block diagrammatic view of a typical byte-oriented 8-bit CRC generator.

30 Fig. 3 is a schematic block diagrammatic view of a data path which includes a CRC generator and checker, a DRAM, and a communication channel with ECC protection.

Fig. 4 is a schematic block diagrammatic view of a one stage CRC generation system according to an embodiment
35 of the invention and provided with memory error checking.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-6-

Fig. 4A a schematic block diagrammatic view of a one stage CRC generation system of Fig. 4 which uses an adder and a conventional CRC generator.

5 Fig. 5 a schematic block diagrammatic view of the adder of Fig. 4A.

Fig. 6 is a schematic block diagrammatic view of a two stage CRC generation system according to an embodiment of the invention.

10 Fig. 7 is a schematic block diagrammatic view of a CRC generator/checker of the CRC generation system of Fig. 6.

Fig. 7A is a detailed schematic block diagrammatic view of an embodiment of the CRC generator/checker of Fig. 7.

15 Fig. 8 is a flowchart depicting basic steps executed by the CRC generation system of Fig. 6 in connection with two stage CRC generation prior to encoding.

DETAILED DESCRIPTION OF THE DRAWINGS

20 The invention includes both one stage and two stage CRC generation systems. Fig. 4 shows a generalized one stage CRC generation system 400 collaterally provided with memory error checking; Fig. 6 shows a generalized two stage CRC generation system 600 with in-line memory
25 checking. As discussed subsequently, both one stage CRC system 400 and two stage CRC system 600 employ a CRC generator/checker which can be a novel CRC generator/checker of the type basically illustrated in Fig. 7. In the embodiments illustrated in Fig. 4 and Fig. 6 the CRC systems
30 400 and 600 are used in conjunction with an ECC system which, in the preferred embodiment, is a three-way interleaved Reed-Solomon code.

The invention includes a method and apparatus that is capable of generating and checking CRC information units
35 (e.g., bytes) and which is order-programmable. The CRC bytes

This Sheet Has Been Replaced





THIS SHEET HAS BEEN REPLACED

-7-

are used to detect random errors occurring in DRAM and also to detect uncorrectable errors occurring in the communication channel.

5

SINGLE STAGE SYSTEM

The one stage CRC generation system 400 of Fig. 4 includes an encoding side and a decoding side. The encoding side of system 400 comprises CRC generator 401; memory (e.g., DRAM) 402; a set of ECC generators 420₁, 420₂, 420₃; and a CRC checker circuit 422, all under control of encoding controller 426. The encoding side of system 400 applies encoded data (including both CRC and ECC bytes) to a communication channel 430. Communication channel 430 in turn outputs received data to the decoding side. The decoding side of system 400 includes a error correction unit 432 and a CRC checker circuit 434, both under the control of decoding controller 436.

The encoding side of system 400 receives input electrical signals at a port 440 (e.g., a port from a host device). As used herein, a port such as port 440 receives a sequence of electrical signals representing a user data stream, the user data stream comprising bytes where each byte is an element of the finite field $GF(2^p)$ and where a byte can be of any p-bit arbitrary length. The user data stream is organized into blocks of electrical signals representing digital data, each block containing n data symbols, wherein each block is mathematically represented by the polynomial $D(x)$.

The electrical signals from port 440 are applied both to an input port CRC generator 401 and a first input port of a multiplexer 442. An output port of CRC generator 401 is connected to a second input port of multiplexer 442. An output port of multiplexer 442 is connected to a data input port of DRAM 402. A data output port of DRAM 402 is connected to: a first input port of channel multiplexer

THIS SHEET HAS BEEN REPLACED

-8-

444; an input port of CRC checker 422; and (via ECC input multiplexer 446) to a selected one of the ECC generators 420₁, 420₂, 420₃. Output ports of the ECC generators 420 are connected to respective input ports of ECC output multiplexer 448.

Encoding controller 426 controls the sequencing (e.g., timing) and operating of the constituent elements of the encoding side of system 400, including the application of signals (e.g., multiplexing) to and from such elements. Controller 426 is connected to DRAM 402 by an address and control bus 450; to MUXes 442, 444, 446, and 448 by a MUX SELECT bus 452; to CRC generator 401 by CRC generator control bus 454; and, to CRC checker 422 by CRC checker control bus 456. These and other unillustrated connections of controller 426 are understood by the man skilled in the art, such as unillustrated connections for controlling ECC generators 420, for example.

On the decoding side of system 400, error correction unit 432 receives and corrects data from channel 430. The corrected data is output on data bus 460, which data is also applied to CRC checker 434. Decoding controller 436 is connected by CRC checker control bus 462 to control the operation of CRC checker 434.

In one embodiment, the CRC generator 401, CRC checker 422, and CRC checker 434 take the form of a novel generator/checker subsequently illustrated with respect to Fig. 7. However, in another embodiment (system 400A) illustrated in Fig. 4A, CRC generator 401, CRC checker 422, and CRC checker 434 are conventional CRC units augmented by m-way adder circuits 471, 472, and 474, respectively. That is, m-way adder circuits 471, 472, and 474 are connected upstream of the respective CRC generator/checkers 401, 422, 434. In other respects, the elements of system 400A resemble like-numbered elements of system 400.

This Sheet Has Been Replaced



This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-9-

Fig. 5 illustrates the configuration of m-way adder circuits 471, 472, and 474. Each m-way adder circuit includes an adder 480 and a register 482. In the system 400B shown in Fig. 4A, each m-way adder circuit is a 3-way adder circuit.

The system 400A shown in Fig. 4A resembles that shown in Fig. 3 except, that the input user data from port 440 is segmented into groups of three bytes. The sum of the three bytes in each group is sent to the conventional CRC generator 410. The first byte in each group will ultimately be sent to ECC generator 420₁, the second byte in each group will ultimately be sent to ECC generator 420₂, and the third byte in each group will ultimately be sent to ECC generator 420₃. The CRC generator 401 is only clocked once for each three bytes. In Fig. 5 the register 482 is reset on the third clock of each three-byte group.

TWO STAGE SYSTEM

Fig. 6 shows a two stage CRC generation system 600 which generally comprises a first CRC generator/checker 601 for generating primary CRC information; a memory (e.g., DRAM) 602; a second CRC generator/checker 603 (for, e.g., generating secondary CRC information); an encoder (such as a Reed Solomon encoder) 604; a data utilization device (such as a disk sub-system) 605; a decoder (such as a Reed Solomon decoder) 606; and, a controller 626.

System 600 also includes a host port 640 connected to an unillustrated host device. Host port 640 is connected to apply an input user data stream to a first input port of DRAM input multiplexer 642 and to a first input port of first CRC generator multiplexer 643. An output port of multiplexer 643 is connected to an input port of first CRC generator/checker 601. An output port of generator/checker 601 is connected to a second input port of DRAM input multiplexer 642. An output port of DRAM multiplexer 642 is

This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-10-

connected to a first input port of DRAM 602. A first output port of DRAM 602 is connected both to a first input port of encoder input multiplexer 644 and to a first input port of second CRC generator/checker multiplexer 645. An output port of multiplexer 645 is connected to an input port of second CRC generator/checker 603. An output port of generator/checker 603 is connected to a second input port of encoder input multiplexer 644. An output port of multiplexer 644 is connected to an input port of encoder 604.

Disk sub-system 605 has both a data input port and a data output port. The data input port of disk sub-system 605 is connected to receive data from an output port of encoder 604. The data output port of disk sub-system 605 is connected to apply data to an input port of decoder 606.

An output port of decoder 606 is connected both to a second input port of second CRC generator multiplexer 645 and to a second data input port of DRAM 602. DRAM 602 has a second output port which is connected both to a host port 646 and to a second input port of first CRC generator multiplexer 643.

Controller 626 is connected to control the timing and sequencing of the operation of the constituent elements of system 600 as explained herein and as otherwise understood by the man skilled in the art. For example, controller 626 is connected to multiplexers 642, 643, 644, and 645 by a multiplexer select bus 650; to DRAM 602 by a DRAM address and control bus 652; to first CRC generator/checker 601 by a first CRC generator control bus 654; to the second CRC generator/checker 603 by a second CRC generator control bus 656; to encoder 604 by encoder control bus 690; and, to decoder 606 by decoder control bus 692. Controller 626 has a plurality of input ports 627, and 627₂ for obtaining input values for programming system 600. In particular, input port 627, receives a value K₁

This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-11-

determinative of the number of CRC bytes to be outputted by first CRC generator/checker 601; input port 627₂ receives a value K_2 determinative of the number of CRC bytes to be outputted by second CRC generator/checker 603.

5 In system 600, the first CRC generator/checker 601 is connected (via MUX 643) to host port (640) for generating primary CRC information based on input user data received from the host device. Memory 602 stores input user data received from the host device and the primary CRC
10 information generated with respect thereto by the first CRC generator/checker 601. Second CRC generator/checker 603, connected to memory 602 via MUX 645, serves to check data retrieved from memory 602 and (optionally) to generate secondary CRC information based on data obtained from memory
15 602 including the primary CRC information. Encoder 604 forms encoded information by utilizing the data obtained from memory 602 including the primary CRC information as well as optional secondary CRC information obtained from second CRC generator/checker 603.

20 Decoder 606 receives input data and decodes the input data into decoded input data including decoded CRC information. Decoder 606 applies the decoded input data including the decoded CRC information to second CRC generator/checker 603 and to memory 602. Second CRC
25 generator/checker 603 validates the decoded CRC information included in the decoded input data. First CRC generator/checker 601 is connected to receive decoded input data including the decoded CRC information stored in memory 602 for validating decoded CRC information received from
30 memory 602.

Thus, in an encoding operation, second CRC generator/checker 603 compares the primary CRC information and verification CRC information generated by second CRC generator/checker 603 to determine errors attributable to
35 memory 602. Encoder 604 is also connected to second CRC



-12-

generator/checker 603 and also utilizes the secondary CRC information to form the encoded information. Conversely, in a decoding operation, first CRC generator/checker 601 determines errors attributable to memory 602.

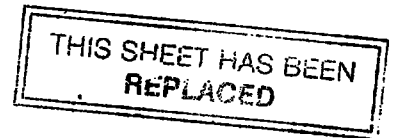
5

CRC GENERATOR/CHECKER STRUCTURE

Fig. 7 generally depicts a CRC generator/checker 700 suitable for use as the CRC generators and CRC checkers described herein. Generator/checker 700 basically includes a segmenting circuit 710; a switch or multiplexer 701; a circuit 712 for forming and using a linear combination of user data sub-streams to generate CRC information; and, an error checker circuit 714. Segmenting circuit 701 serves to segment an input stream of user data into a plurality m of sub-streams for application to switch 701. Switch 701 selects from the plurality of user data sub-streams in accordance with clock cycle and applies the selected user data sub-stream to circuit 712. The resultant CRC information, preferably in the form of CRC bytes, is outputted on parallel CRC bus 716. When generator/checker 700 is employed to check received CRC information previously generated on the basis of received data, the previously generated CRC information is compared by error checker 714 with verification CRC information currently generated (with respect to the same user data) by circuit 712. Should the previously generated and currently generated verification CRC information differ, an error signal is generated on CRC error line 718.

Fig. 7A shows structural details of one particular implementation of CRC generator/checker 700, and particular an implementation wherein $m=3$. Accordingly, segmenting circuit 710 of Fig. 7A is shown to include three sub-stream lines 707_0 , 707_1 , 707_2 . For reasons hereinafter discussed, sub-stream line 707_1 and 707_2 have multipliers M_1 and M_2 connected thereon. Switch 701 is a three-input multiplexer

35



-13-

having input selected by controller 626 (via a control bus). An output port of multiplexer 701 is connected to apply the sub-stream selected thereby to adder input bus 720.

As shown in Fig. 7A, circuit 712 comprises k number of sub-circuits 722₁ - 722_k for generating as many as k bytes of CRC information with respect to the linear combination of sub-streams. As explained below, each sub-circuit 722 is a divider having a divisor which is a power of α . Each sub-circuit 722 comprises an adder input multiplexer 702; an adder 703; a multiplier 704; a register 705 for storing CRC information; and, a register input multiplexer 708. Each adder 703 has a first input port, a second port, and an output port. The first port of each adder 703 is connected to adder input bus 720 so that the plurality of sub-streams can be multiplexed thereto. Each multiplier 704 has an output port thereof selectively connected (via a first input port of associated multiplexer 702) to the second input port of its associated adder 703. Each register 705 has an input port connected to the output port of associated adder 703 and its output port is selectively connected (via a first input port of associated multiplexer 702) to the second input port of the adder 703. Each register 705 stores CRC information in the form of a CRC byte which is related to an error correcting code. Each of the multiplexers 702 and 708 are controlled by controller 626 (for example, via control bus 654).

From the foregoing it is understood that sub-circuits 722 are numbered from a first sub-circuit 722₁ to a kth sub-circuit 722_k. Registers 705 of the sub-circuits 722 are connected so that CRC information stored therein can be rightwardly shifted. The rightward shift occurs after the n clock cycles executed to generate the CRC bytes in registers 705. After the n clock cycles are executed to generate the CRC bytes, the CRC bytes in registers 705 are shifted rightwardly a desired number of clocks (as input to

THIS SHEET HAS BEEN REPLACED

-14-

controller 626), one register (e.g., one sub-circuit) per clock. For example, considering the operation of first CRC , generator/checker 601, if an input value of 4 is inputted at input port 627, of controller 626, during a first shift
5 clock cycle the CRC byte in register 705₁ is shifted out on CRC bus 716; the CRC byte in register 705₂ is shifted into register 705₁; the CRC byte in register 705₃ is shifted into register 705₂; and so forth. Such shifting continues for four shift clock cycles, so that the CRC values initially in
10 registers 705₁ - 705₄ are ultimately shifted out to CRC bus 716.

The values of the multipliers 704 are chosen so that the multiplier multiplies by a power of a field element α , the power being $r+1$ for the multiplier of the first sub-circuit 722₁ and $r+k$ for the multiplier of the k^{th} sub-circuit 722_k.
15

The output port of adder 703, is connected to error checker circuit 714 and to MUX 708_k. As illustrated in Fig. 7A, error checker circuit 714 comprises an 8-input
20 OR gate 709 which is connected to the output port of adder 703₁. Error checker circuit 714 further includes an AND gate 730 and an R/S flip-flop or latch 732. An output pin of OR gate 709 is connected to a first input pin of AND gate 730, a second input pin of AND gate 730 being connected to
25 receive a signal CRC_TIME from controller 626. An output pin of AND gate 730 is connected to a set pin of flip-flop 732; a reset pin of flip-flop 732 receives a signal RST from controller 626. Since adder 703₁ is involved in verifying previously-generated CRC information with currently
30 generated CRC information in the manner hereinafter described, sub-circuit 722₁ is denominated the "comparison" sub-circuit.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-15-

TWO STAGE ENCODING OPERATION

Fig. 8 depicts basic steps executed by system 600 of Fig. 6 in connection with two stage CRC generation prior to encoding. Prior to actual CRC generation, as depicted by step 800 of Fig. 8, controller 626 is programmed with values K_1 and K_2 for determining the amount (e.g., number of bytes ranging from 1 to k) of CRC information to be shifted out of first CRC generator 601 and second CRC generator 602, respectively.

In connection with encoding aspects of the CRC generation of system 600 of Fig. 6, bytes of user data from the host are sent to first CRC generator/checker 601 and are written into DRAM 602. Step 802 of Fig. 8 shows first CRC generator/checker 601 obtaining n bytes of user data from the host and using the n bytes of user data to form CRC bytes C_j ($j=1,2,\dots,k$) during n clock cycles. After the n clock cycles for generating CRC bytes C_j ($j=1,2,\dots,k$), during the next K_1 clock cycles (step 804) first CRC generator/checker 601 shifts CRC bytes

$$C_1, \dots, C_k$$

also known as the primary CRC bytes, into DRAM 602.

In connection with the execution of step 802, and specifically with reference to generator/checker 700 illustrated in Fig. 7, during the first of the n clock cycles multiplexer 701 switches the first of the n user data bytes onto adder input bus 720. Concerning such first byte obtained on line 707₀ of segmenting circuit 710, M_0 for segmenting circuit 710 may always be selected as α^0 and hence no multiplier is needed for M_0 . During the second of the n clock cycles multiplexer 701 switches the second of the n user data bytes (multiplied by M_1) onto adder input bus 720; during the third of the n clock cycles multiplexer 701 switches the third of the n user data bytes (multiplied by M_2) onto adder input bus 720.

This Sheet Has Been Replaced



This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-16-

Thus, during a data portion of generation or checking depicted by step 802, MUX 701 supplies the dividers (e.g., sub-circuits 722) with the input user data multiplied by M_0 (from lead 707₀) on the first clock and on every third clock following the first, it supplies the dividers 722 with the input user data multiplied by M_1 (from lead 707₁) on the second clock and on every third clock following the second and it supplies the dividers 722 with the input user data multiplied by M_2 (from lead 707₂) on the third clock and on every third clock following the third. In execution of step 802, MUXes 702 supply adders 703 with the outputs of constant multipliers 704 on the first clock and on every third clock following the first. MUXes 702 supply the adders 703 with the outputs of registers 705 on the other clocks. MUXes 708 supply the adder outputs to the inputs of registers 705.

During execution of step 804, which is a CRC portion of CRC generation or checking, i.e. when CRC bytes are being output, MUXes 708 connect the registers 705 into one shift register. During generation this allows the programmed number (K_1) of CRC bytes which reside in the registers 705 to be shifted out onto CRC bus 716. K_1 clock cycles are required in step 804 to shift out the K_1 number of desired CRC bytes. After the K_1 clock cycles, all registers 705 are re-initialized at zero, so that CRC bytes $K_1 \dots k$ are discarded.

As mentioned before, step 804 shows the shifting of the primary CRC bytes C_j ($j=1, \dots K_1$) into DRAM 602. At some later time (depicted by step 806), the block of data in DRAM 602 and the primary CRC bytes C_j ($j=1, \dots K_1$) are read from DRAM 602 and sent both to Reed-Solomon encoder 604 (via MUX 644) and to second CRC generator/checker 603 (via MUX 645). The data from the block in DRAM 602 is applied to second CRC generator/checker 603 in a manner such that n number of user data bytes are applied followed by the K_1

This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-17-

number of primary CRC bytes C_j ($j=1, \dots K_1$) generated by generator 601 with respect to those n bytes.

In step 806, second CRC generator/checker 603 receives the user data from DRAM 602 in groups of n number of input bytes. Using the n number of input bytes, during n number of clock cycles the second CRC generator/checker 603 generates k number of verification CRC bytes C_j' in similar manner as first CRC generator/checker 601 generated the primary CRC bytes C_j . If the user data bytes obtained from DRAM 602 in step 806 are identical to the user data bytes shifted into DRAM 602 from the host as occurs when DRAM is operating properly, then the verification CRC bytes C_j' will equal the respective primary CRC bytes C_j .

After second CRC generator/checker 603 has generated the verification CRC bytes C_j' during the n clock cycles of step 806, at step 808 secondary CRC generator/checker 603 performs a checking operation to compare primary CRC bytes C_j ($j=1, \dots K_1$) with the verification CRC bytes C_j' ($j=1, \dots K_1$). In so doing, MUX 701 is operated to apply the primary CRC bytes C_j ($j=1, \dots K_1$) from line 707₀ of segmenting circuit 710 to the first input port of ADDER 703₁, the application being made one byte per clock cycle for each of K_1 number of verification clock cycles. During a first of the verification clock cycles, the first primary CRC byte C_1 is applied to the first input port of ADDER 703₁, and the first verification CRC byte C_1' stored in register 705₁ is applied to the second input port of ADDER 703₁, so that the result of the addition operation of ADDER 703₁ is applied to check circuit 714. With each verification clock cycle, the verification CRC bytes C_j' in registers 705₁ are shifted rightwardly by one sub-circuit 722 (e.g, to the next rightwardly adjacent register), as in the manner of CRC byte shift/readout described hereinbefore, so that after the first verification clock cycle register 705₁ will contain the verification CRC

This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-18-

byte C_2' . Similarly, during a second of the verification clock cycles, the second primary CRC byte C_2 is applied to the first input port of ADDER 703, and the second verification CRC byte C_2' now stored in register 705, is applied to the second input port of ADDER 703, again with the result of the addition operation of ADDER 703, is applied to check circuit 714. Such shifting and adding continues for each of the K_1 number of verification clock cycles, so that CRC bytes C_j are compared with corresponding bytes C_j' for $j=1, \dots, K_1$.

During execution of step 808, checker circuit 714 is effectively enabled by a signal CRC_TIME from controller 626. When checker circuit 714 is enabled, any inequality between a primary CRC byte C_j and its corresponding verification byte C_j' causes a non-zero output of OR gate 709 to be gated through AND gate 730 for application to flip-flop 732. The detected inequality causes flip-flop 732 to output a CRC ERROR signal to controller 626 on line 718.

If the value K_2 inputted to controller 626 with respect to second CRC generator/checker 603 is greater than the value K_1 , then at step 810 second CRC generator/checker 603 will shift out (on line 716) a number ($K_2 - K_1$) of secondary CRC bytes, specifically CRC bytes C_j' ($j=K_1+1, \dots, K_2$). In this regard, after execution of step 808, registers 705₁, 705₂, 705₃, etc. will contain

$$C_{K_1+1}, C_{K_1+2}, C_{K_1+3}, \text{etc.}$$

The shifting out of secondary CRC bytes C_j' ($j=K_1+1, \dots, K_2$) occurs in $K_2 - K_1$ clock cycles, and is accomplished in the hereinbefore described manner of controlling multiplexers 708 for the rightward shift operation.

After a block of data including both the primary CRC bytes C_j ($j=1, \dots, K_1$) and the secondary CRC bytes C_j' ($j=K_1+1, \dots, K_2$) is encoded by encoder 604, the encoded block

THIS SHEET HAS BEEN REPLACED

-19-

is written to disk subsystem 605. It will be appreciated by the man skilled in the art that encoder 604 generates ECC bytes for each interleave of data, preferably m number of interleaves using a ECC generator polynomial.

5 Thus, second CRC generator/checker 603 checks whether errors occurred in DRAM 602 and also may generate additional CRC bytes, known as secondary CRC bytes. These secondary CRC bytes may be written to the disk along with the primary CRC bytes. Inclusion of the secondary CRC bytes
10 can be important because the data read from disk may require more protection than the DRAM data owing to the fact that data from disk is more susceptible to error than data from DRAM 602.

 As described above, second CRC generator/checker
15 603 allows the incoming primary CRC bytes to be checked one at a time. It also shifts out as many of the $k-K_1$ remaining CRC bytes as are specified by the input value K_2 , these further shifted bytes being secondary CRC bytes). This facilitates a situation in which only the first K_1
20 number of primary CRC bytes are written into the DRAM 602 but K_2 are written to disk ($K_2 > K_1$). The checking of the primary CRC bytes is accomplished by adding the incoming primary CRC bytes to the newly generated verification CRC bytes by adder 703, and then detecting a non-zero byte with
25 OR gate 709. While CRC bytes are being input to the checker the CRC_TIME signal is ON and then any mismatches will set CRC_ERROR latch 732. The order of the generator is programmable since the CRC bytes are calculated independently of each other and hence only the desired
30 number of CRC bytes need be shifted out.

This Sheet Has Been Replaced



This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-20-

TWO STAGE DECODING OPERATION

In connection with an decoding operation executed by system 600 of Fig. 6, a data block is read from the disk by disk sub-system 605 and is sent to Reed-Solomon decoder 606. Corrected data obtained by decoder 606 (including CRC bytes) is sent both to second CRC generator/checker 603 (to check for uncorrectable errors) and to DRAM 602.

Second CRC generator/checker 603 receives data bytes and CRC bytes from the decoded block in much the same manner as it does prior to an encoding operation. Upon receiving each group of n data bytes, second CRC generator/checker 603 generates K_2 number of verification CRC bytes for comparison with a like number of corresponding CRC bytes obtained from the decoded data. Operation of the second CRC generator/checker 603 in connection with post-decode CRC processing is analogous to steps 806 and 808 above-discussed, and understand with reference thereto. Second CRC generator/checker 603 performs a verification with respect to CRC bytes obtained from the disk sub-system 605.

In connection with post-decode CRC processing, when the data block is retrieved from DRAM 602 for sending to the host, the data block is again sent to first CRC generator/checker 601 to check for DRAM errors. Operation of the first CRC generator/checker 601 in connection with post-decode CRC processing is also analogous to steps 806 and 808 above-discussed, and understand with reference thereto, with the proviso that K_1 number of CRC bytes are processed by the first CRC generator/checker 601.

OPERATION: MATHEMATICAL BASES

In the illustrated embodiments, the data stream which feeds the CRC generator/checker 700 is segmented into groups of three bytes. A linear combination of the three bytes is then sent to a collection of circuits (e.g., sub-

THIS SHEET HAS BEEN REPLACED

-21-

circuits 722) which divide by $X + \alpha^{n^j}$ for $j = 1, 2, \dots, k$ where α is a primitive element of the field representation of the data bytes. In the preferred embodiment the field is $GF(256=2^8)$. The linear combination may be a simple sum, leading to the embodiment shown in Fig. 4A.

While a simple linear combination may be simple to implement, it is possible to have two bytes each with a single bit error in a block of data read from the DRAM which are not detectable owing to the fact that if the same error is in two bytes of a three-byte group then the two errors will cancel when summed together before being sent to the CRC generator/checker 700. Alternately the linear combination can be chosen so that if the three bytes in the group each have no more than a single "1" in each byte, then the linear combination will be non-zero. In that case, if every byte in error in a block of data contains only a single bit in error, then k CRC bytes can be used to detect k bytes in error even if some of the bytes in error are in the same three-byte group.

Using a linear combination of every three input bytes allows the CRC bytes to be generated in such a way as to increase the minimum distance of the ECC code by one for each CRC byte. This can be done because the ECC consists of three interleaves.

The CRC bytes are generated according to the following rule: Let the input bytes be denoted as D_0 to D_{n-1} . These bytes make up the coefficients of three polynomials, $F^0(x)$, $F^1(x)$ and $F^2(x)$, thusly:

$$F^s(x) = \sum_{k=0}^{t_s} D_{(3 \cdot k) + s} \cdot x^{t_s - k}$$

for $s = 0, 1, 2$ where t_s is the largest integer that is less than $(n-s)/3$. These polynomials represent the division of

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

-22-

D(x) into three groups, e.g. D_0 is in F^0 , D_1 is in F^1 , D_2 is in F^2 , D_3 is in F^0 , etc. These polynomials are precisely the same polynomials that are processed by the Reed-Solomon encoder 604 to form the three Reed-Solomon code words. $G(x)$ is defined as a linear combination of $F^0(x)$, $F^1(x)$ and $F^2(x)$ thusly:

$$G(x) = \sum_{s=0}^2 M_s \cdot F^s(x)$$

The system 400A in Fig. 4A corresponds to the case where the multipliers, M_s , are all 1. The system 600 in Fig. 6 corresponds to the case where the M_s are chosen so that $aM_0 + bM_1 + cM_2$ is non-zero as long as a, b and c each contain a single "1". The coefficients of $G(x)$ are linear combinations of three consecutive input bytes, e.g. the first coefficient of $G(x)$ is $D_0M_0 + D_1M_1 + D_2M_2$, the second coefficient of $G(x)$ is $D_3M_0 + D_4M_1 + D_5M_2$, etc.

The j^{th} CRC byte, C_j , is defined as:

$$C_j = G(x) \bmod (x + \alpha^{r+j})$$

for $j = 1, 2, \dots, k$.

If only k or less of the input bytes D_i were non-zero, and the non-zero bytes each consisted of a single "1", then $G(x)$ would have at most k non-zero coefficients and $G(x)$ could not be zero. All of the CRC bytes are obtained by dividing $G(x)$ by consecutive powers of α , and therefore if there are k CRC bytes then at least one of the CRC bytes would be non-zero. This is equivalent to saying that any set of k or less single-bit errors would be detected.

The Reed-Solomon code to be used in conjunction with the new CRC generator has a generator polynomial which has, as roots, v consecutive powers of α , from α^{r-v+1} to α^r . Let $E(x)$ be an error polynomial which has been added to one of the ECC interleaves, i.e. one of the Reed-Solomon code

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

-23-

words. If the error is not detectable by the ECC, then $E(x)$ must have roots which include α^{r-v+1} to α^r . Since the factors, used in CRC generation have as roots the k consecutive powers of α , from α^{r+1} to α^{r+k} , for the error not to be
5 detected by the CRCs, $M_2 E(x)$ must have roots which include α^{r+1} to α^{r+k} . This implies that $E(x)$ must have roots which include α^{r-v+1} to α^{r+k} , which means that the error has more than $k+v$ bytes in error.

The set of M_1 and M_2 constants which cause $a + bM_1 + cM_2$ to be non-zero for all a , b and c which have a single
10 "1" is not unique. Therefore M_1 and M_2 are picked to satisfy that condition and to also cause linear combinations of other classes to be non-zero. For example, in the preferred embodiment the field generator polynomial is
15 $x^8 + x^4 + x^3 + x^2 + 1$. M_1 is chosen to be α^{25} and M_2 is chosen to be α^{112} . This choice causes $a + bM_1 + cM_2$ to be non-zero for the case where only two of the three bytes a , b and c are non-zero and the two bytes each have a single 3-bit or shorter non-zero bit sequence. After adding this condition the
20 choice of M_1 and M_2 is still not unique, therefore an additional condition is added which is to maximize the number of two-byte combinations where each byte can have a single 4-bit or shorter non-zero bit sequence. The M_1 and M_2 multipliers each consist of a set of XOR gates such that
25 the output bits are linear combinations, i.e. XOR sums, of certain subsets of the input bits and these subsets are listed in Table I and Table II.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-24-

Table I
M₁ multiplier

OUT0 = IN0 + IN7
OUT1 = IN0 + IN1
OUT2 = IN1 + IN2 + IN7
OUT3 = IN2 + IN3 + IN7
OUT4 = IN3 + IN4 + IN7
OUT5 = IN4 + IN5
OUT6 = IN5 + IN6
OUT7 = IN6 + IN7

Table II
M₂ multiplier

OUT0 = IN0 + IN1 + IN5 + IN6 + IN7
OUT1 = IN1 + IN2 + IN6 + IN7
OUT2 = IN1 + IN2 + IN3 + IN5 + IN6
OUT3 = IN1 + IN2 + IN3 + IN4 + IN5
OUT4 = IN1 + IN2 + IN3 + IN4 + IN7
OUT5 = IN2 + IN3 + IN4 + IN5
OUT6 = IN3 + IN4 + IN5 + IN6
OUT7 = IN0 + IN4 + IN5 + IN6 + IN7

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-25-

For example, the CRC generator/checker of this invention has been illustrated in conjunction with a three-way interleaved Reed-Solomon code. It may alternately be employed with, for example, a two-way or four-way interleaved code. The principles taught with the illustrated CRC can be applied to a CRC for use in conjunction with encoders not limited to the Reed-Solomon design. The method of this invention can be used for codeword generation, codeword checking or both. It can be used between a computer host and a DRAM, between a DRAM and a magnetic disk, or between two ends of any communication channel. The same CRC can be used in more than one communication channel of a system, for example both between the host and a DRAM and between the DRAM and storage disk.

The CRC of this invention can be programmed to generate k CRC bytes. In conjunction with a Reed-Solomon code the CRC allows detection of k more errors than the Reed-Solomon code is capable of detecting. The number k can be tailored to the propensity for errors of a given communication channel. When the same CRC is used for more than one communication channel, different values of k can be selected for each channel. The CRC of this invention can also be utilized in a non-programmable embodiment having a fixed number of CRC bytes.

A hardware implementation of this invention has been illustrated. The CRC can also be implemented with software. Specific circuitry to implement the block diagram of Fig. 7 of this invention can be readily designed by a routiner in the electronic arts. Variations on the block diagram will also be apparent to those skilled in the art. Specific examples of a field generator polynomial and of the constant multipliers M_i have been supplied. Other constants and polynomials can be chosen, as taught herein. For example, instead of dividing by two eight bit polynomials, division can instead occur with one sixteen bit polynomial.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-26-

U.S. Patent Application Serial Number 08/____,____
(attorney docket 1777-10) simultaneously filed by Zook et
al., entitled "ERROR CORRECTION METHOD AND APPARATUS", and
incorporated herein by reference, provides one non-limiting
example of a specific utilization of the present invention.

While the preferred embodiment has been disclosed
and described in detail herein, it will be obvious to those
skilled in the art that various changes in form and detail
may be made therein without departing from the spirit and
scope thereof.

This Sheet Has Been Replaced



This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-27-

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A cyclical redundancy check (CRC) generator which generates CRC information for error checking purposes, comprising:

5 a segmenting circuit for segmenting an input stream of data into a plurality of sub-streams;

a circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information.

2. The apparatus of claim 1, wherein the segmenting circuit segments the input stream into three sub-streams.

3. The apparatus of claim 1, wherein the segmenting circuit includes a multiplier for multiplying at least one of the sub-streams by a constant.

4. The apparatus of claim 3, wherein the multiplier is chosen so that a linear combination of certain bytes in the sub-stream is non-zero.

5. The apparatus of claim 4, wherein the constant is a power of a field element α .

6. The apparatus of claim 5, wherein there are three sub-streams, each sub-stream constituting a byte of data, and wherein one sub-stream is multiplied by a constant M_1 and another sub-stream is multiplied by a constant M_2 , and
5 wherein $M_1 = \alpha^{25}$ and $M_2 = \alpha^{112}$.



* C L H S *

This Sheet Has Been Replaced

THIS SHEET HAS BEEN
REPLACED

-28-

7. The apparatus of claim 1, wherein each sub-stream constitutes a byte of data, and wherein the circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information comprises k number of sub-circuits for generating k bytes of CRC information with respect to the linear combination of sub-streams.

8. The apparatus of claim 1, wherein each sub-stream forms at least part of a data polynomial, and wherein the circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information comprises k number of divider sub-circuits for generating k bytes of CRC information with respect to the linear combination of sub-streams.

9. The apparatus of claim 8, wherein each divider sub-circuit divides the data polynomial by a divisor which is related to a root of an ECC polynomial.

10. The apparatus of claim 1, wherein the circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information comprises a plurality of sub-circuits, each sub-circuit comprising:

an adder, the adder having a first input port, a second port, and an output port, the first port of the adder having the plurality of sub-streams multiplexed thereto;

a multiplier, the multiplier having an output port thereof selectively connected to the second input port of the adder;

a register for storing CRC information, the register having an input port connected to the output port of the adder and an output port selectively connected to the second input port of the adder.



* C L M S *

THIS SHEET HAS BEEN
REPLACED

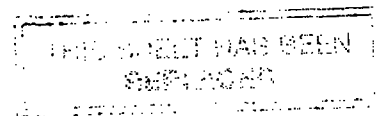
-29-

11. The apparatus of claim 10, wherein k number of sub-circuits are provided numbered from a first sub-circuit to a k^{th} sub-circuit, and wherein the registers of the sub-circuits are connected so that CRC information stored in the register of a K_1^{th} of the sub-circuits is shifted to the register of the first sub-circuit, K_1 being a constant less than or equal to k.
12. The apparatus of claim 11, wherein K_1 is programmable.
13. The apparatus of claim 10, wherein the multiplier multiplies by a factor related to a root of an ECC polynomial.
14. The apparatus of claim 10, wherein the output port of the adder of one of a comparison one of the sub-circuits is connected to a CRC comparator for comparing a value inputted to the input terminal of the adder of the comparison sub-circuit to CRC information stored in the register of the comparison sub-circuit.
15. The apparatus of claim 14, wherein the CRC comparator comprises an XOR gate.
16. A cyclical redundancy check (CRC) generator which generates CRC information for error checking purposes, comprising:
 means for segmenting an input stream of data into a plurality of sub-streams;
 means for forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information.
17. The apparatus of claim 16, wherein the segmenting means segments the input stream into three sub-streams.



This Sheet Has Been Replaced





-30-

18. The apparatus of claim 16, wherein the segmenting means multiplies at least one of the sub-streams by a constant.

19. The apparatus of claim 18, wherein the constant is chosen so that a linear combination of certain bytes in the sub-stream is non-zero.

20. The apparatus of claim 19, wherein the constant is a power of a field element α .

21. The apparatus of claim 20, wherein there are three sub-streams, each sub-stream constituting a byte of data, and wherein one sub-stream is multiplied by a constant M_1 and another sub-stream is multiplied by a constant M_2 , and
5 wherein $M_1 = \alpha^{25}$ and $M_2 = \alpha^{112}$.

22. The apparatus of claim 16, wherein each sub-stream forms at least part of a data polynomial, and means for forming a linear combination of the plurality of sub-streams and for operating upon the linear combination in order to
5 generate the CRC information comprises k number of dividers for generating k bytes of CRC information with respect to the linear combination of sub-streams.

23. The apparatus of claim 22, wherein the means for forming a linear combination of the plurality of sub-streams and for operating upon the linear combination in order to generate the CRC information actually outputs K_1 number of
5 bytes of CRC information, K_1 being a constant less than or equal to k.

24. The apparatus of claim 23, wherein K_1 is programmable.



* C L M S *

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-31-

25. The apparatus of claim 22, wherein each divider divides the data polynomial by a divisor which is related to a root of an ECC polynomial.

26. A cyclical redundancy check (CRC) method which generates CRC information for error checking purposes, the method comprising:

- 5 segmenting an input stream of data into a plurality of sub-streams; and,
 forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information.

27. The method of claim 26, wherein the input stream into three sub-streams.

28. The method of claim 26, further comprising multiplying at least one of the sub-streams by a constant.

29. The method of claim 28, wherein the constant is chosen so that all linear combinations of the sub-streams are non-zero.

30. The method of claim 29, wherein the constant is a power of a field element α .

31. The method of claim 30, wherein there are three sub-streams, each sub-stream constituting a byte of data, and wherein one sub-stream is multiplied by a constant M_1 and another sub-stream is multiplied by a constant M_2 , and
5 wherein $M_1 = \alpha^{25}$ and $M_2 = \alpha^{112}$.

This Sheet Has Been Replaced



* C L M S *

THIS SHEET HAS BEEN
REPLACED

-32-

32. The method of claim 26, wherein the steps of forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information comprises applying the plurality of sub-streams to k number of sub-circuits for generating k bytes of CRC information with respect to the linear combination of sub-streams, the sub-circuits being numbered from a first sub-circuit to a k^{th} sub-circuit
33. The method of claim 32, wherein for sub-circuit j, the linear combination applied thereto is divided by a factor related to a root of an ECC polynomial.
34. The method of claim 32, further comprising storing CRC information in a register of each sub-circuit and shifting CRC information stored in the register of the k^{th} sub-circuit to the register of the first sub-circuit.
35. The method of claim 32, further comprising comparing a CRC value inputted to a comparison one of the sub-circuits to CRC information stored in the register of the comparison sub-circuit.
36. A cyclical redundancy check (CRC) method which generates CRC information for error checking purposes, the method comprising:
- (a) segmenting an input stream of data into a plurality of sub-streams, the input stream being obtained from a communication channel;
 - (b) forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information;
 - (c) comparing the generated CRC information with decoded CRC information obtained from the communication channel; and

This Sheet Has Been Replac



THIS SHEET HAS BEEN
REPLACED

-33-

15 (d) producing an error signal when a discrepancy is detected between the generated CRC information and the decoded CRC information obtained from the communication channel.

37. The method of claim 36, wherein the CRC information generated in step (b) constitutes K_1 number of bytes stored in registers $j=1, \dots k$, wherein the decoded CRC information constitutes K_1 number of decoded CRC bytes $j=1, \dots k$ sequentially applied to a comparator, and wherein the comparison step comprises using the comparator to compare the contents of register j with decoded CRC byte j .

38. The method of claim 37, wherein K_1 is a programmable integer.

39. The method of claim 36, further comprising sequentially shifting K_1 number of values stored in registers $j=1, \dots k$ into a selected one of the registers for comparison with a corresponding decoded CRC byte.

40. The method of claim 39, wherein K_1 is a programmable integer.

41. A cyclical redundancy check (CRC) system comprising:
a host port connected to a host device;
a first CRC generator connected to the host port for generating primary CRC information based on input data
5 received from the host device;
a memory for storing therein input data received from the host device and the primary CRC information generated with respect thereto by the first CRC generator;
a second CRC generator connected to the memory for
10 generating verification CRC information for checking data retrieved from the memory;



This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

-34-

an encoder connected to form encoded information by utilizing the data obtained from the memory including the primary CRC information.

42. The apparatus of claim 41, wherein the second CRC generator compares the primary CRC information and the verification CRC information generated by the second CRC generator to determine errors attributable to the memory.

43. The apparatus of claim 41, wherein the second CRC generator also generates secondary CRC information based on data obtained from the memory; and wherein the encoder is also connected to the second CRC generator and also utilizes the secondary CRC information to form the encoded information.

44. The apparatus of claim 41, further comprising:
a utilization port connected to a utilization channel;
a decoder connected to receive input data at the utilization port and to decode the input data into decoded input data including decoded CRC information, the decoder being connected to apply the decoded input data including the decoded CRC information to the second CRC generator and to the memory, whereby the second CRC generator validates decoded CRC information included in the decoded input data, and

wherein the first CRC generator is connected to receive decoded input data including the decoded CRC information stored in the memory for validating decoded CRC information received from the memory.

45. The apparatus of claim 41, wherein the first CRC generator comprises the cyclical redundancy check (CRC) generator of claim 1.



* C L M S *

This Sheet Has Been Replac



-35-

THIS SHEET HAS BEEN REPLACED

46. The apparatus of claim 41, wherein the second CRC generator comprises the cyclical redundancy check (CRC) generator of claim 1.

47. A cyclical redundancy check (CRC) method comprising:
using a first CRC generator to generate primary CRC information based on input data received from a host device;

5 storing in a memory the input data received from the host device and the primary CRC information generated with respect thereto by the first CRC generator;

10 using a second CRC generator connected to the memory for generating verification CRC information with respect to data retrieved from the memory;

forming encoded information by utilizing the data obtained from the memory including the primary CRC information.

48. The method of claim 47, further comprising using the second CRC generator to compare the primary CRC information and verification CRC information generated by the second CRC generator to determine errors attributable to the memory.

49. The method of claim 47, wherein the second CRC generator generates secondary CRC information with respect to data retrieved from the memory.

50. The method of claim 49, further comprising forming the encoded information by also using the secondary CRC information.

This Sheet Has Been Replaced



* C L M S *

THIS SHEET HAS BEEN
REPLACED

-36-

51. The method of claim 47, further comprising:

decoding input data received from a utilization channel into decoded input data including decoded CRC information;

5 applying the decoded input data including the decoded CRC information to the second CRC generator and to the memory;

storing the decoded input data including the decoded CRC information in the memory;

10 using the second CRC generator to validate the decoded CRC information included in the decoded input data;

applying the decoded input data including the decoded CRC information from the memory to the first CRC generator; and

15 using the first CRC generator to validate the decoded CRC information received from the memory.

This Sheet Has Been Replaced



* C L M S *

THIS SHEET HAS BEEN
REPLACED

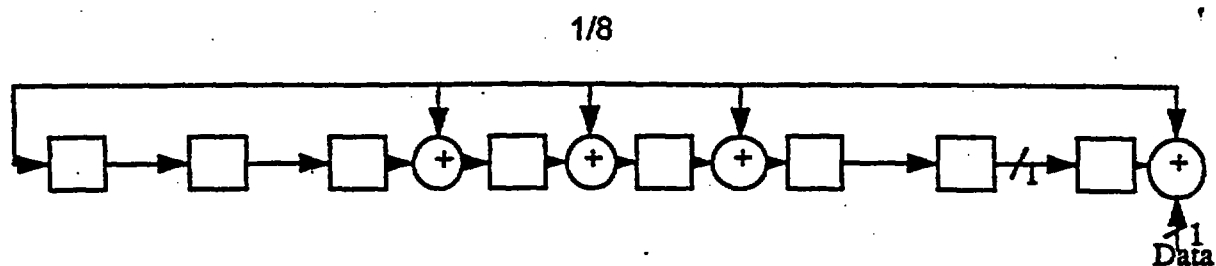


Fig. 1 (Prior Art)

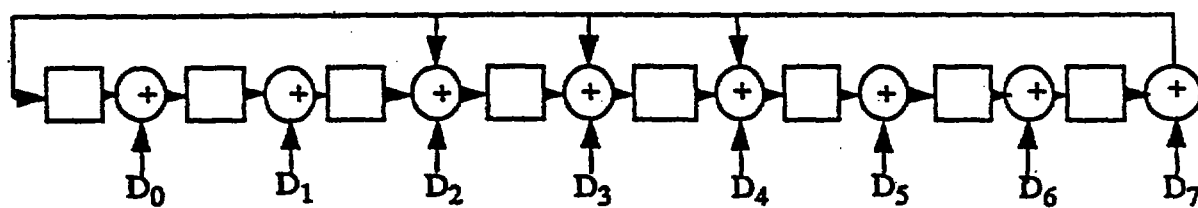


Fig. 2 (Prior Art)

This Sheet Has Been Replaced



THIS SHEET HAS BEEN
REPLACED

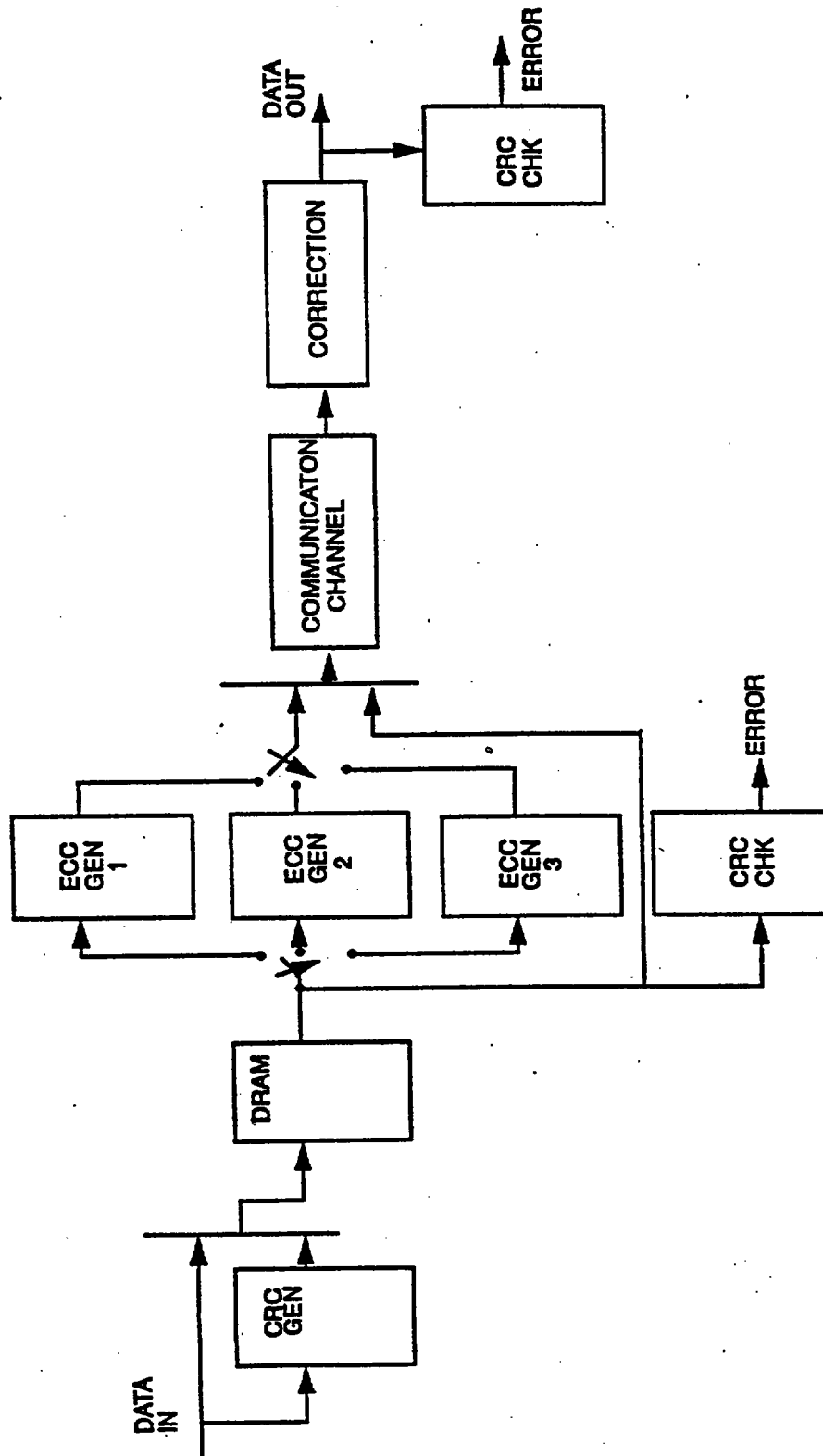
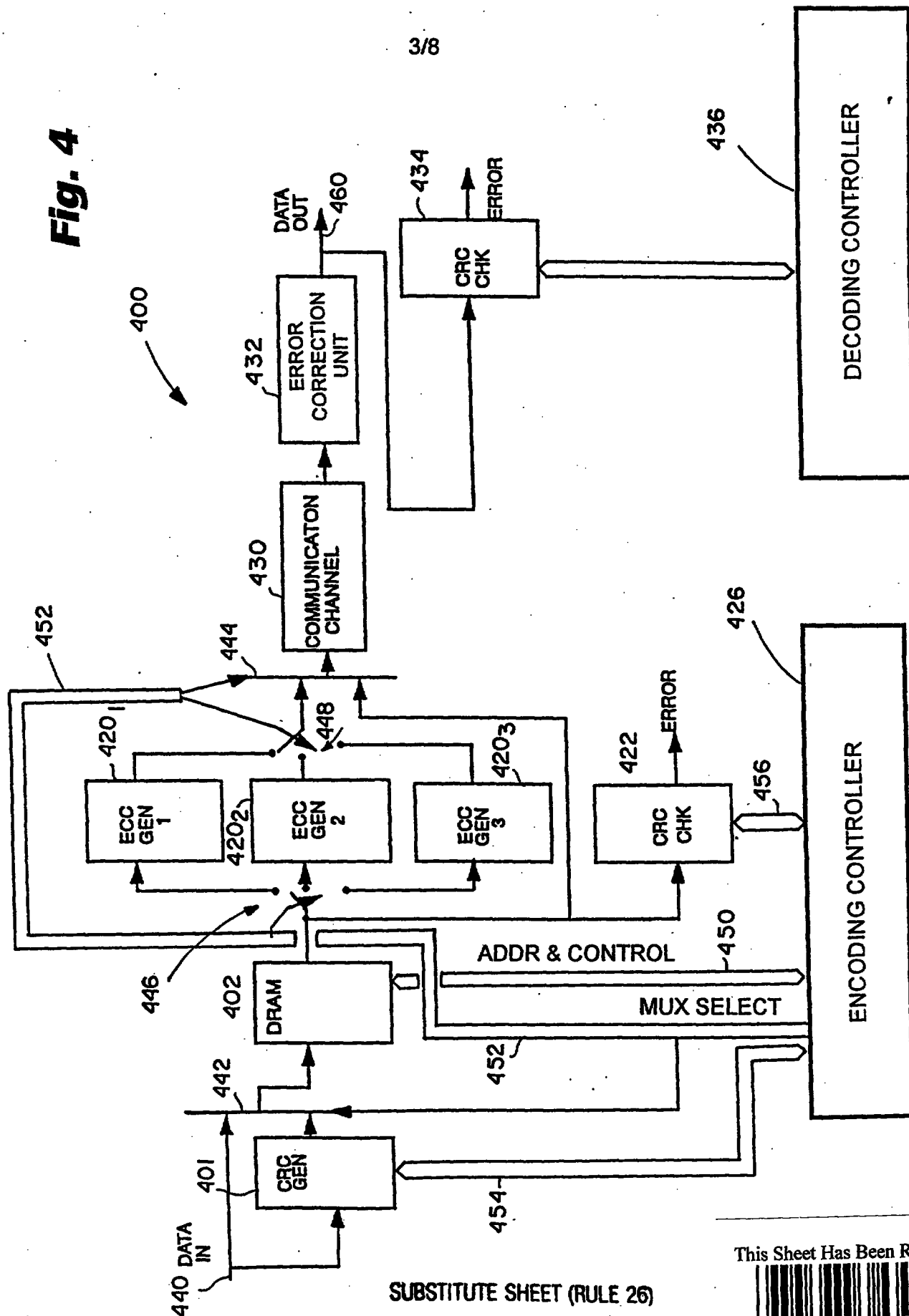


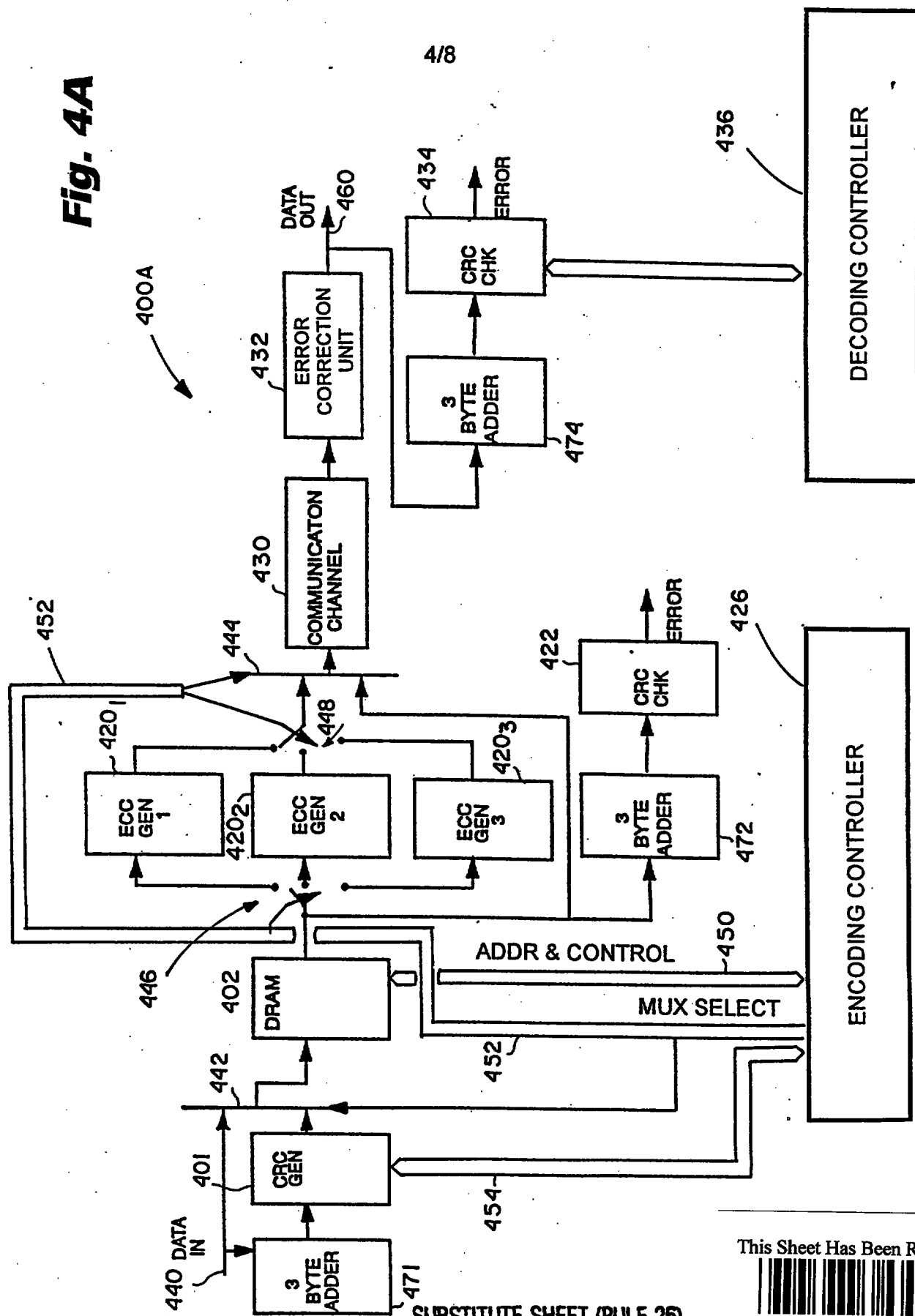
Fig. 3 (Prior Art)



THIS SHEET HAS BEEN
REPLACED**Fig. 4**

THIS SHEET HAS BEEN REPLACED

Fig. 4A



THIS SHEET HAS BEEN
REPLACED

This Sheet Has Been Replaced



5/8

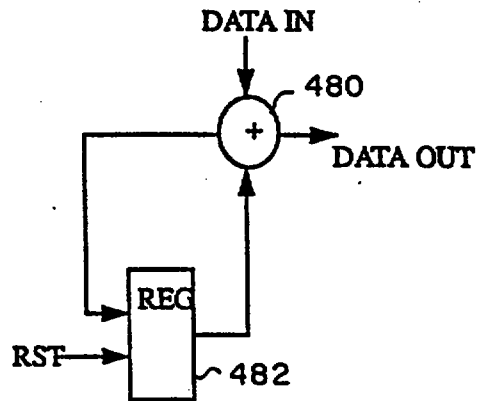


FIG. 5

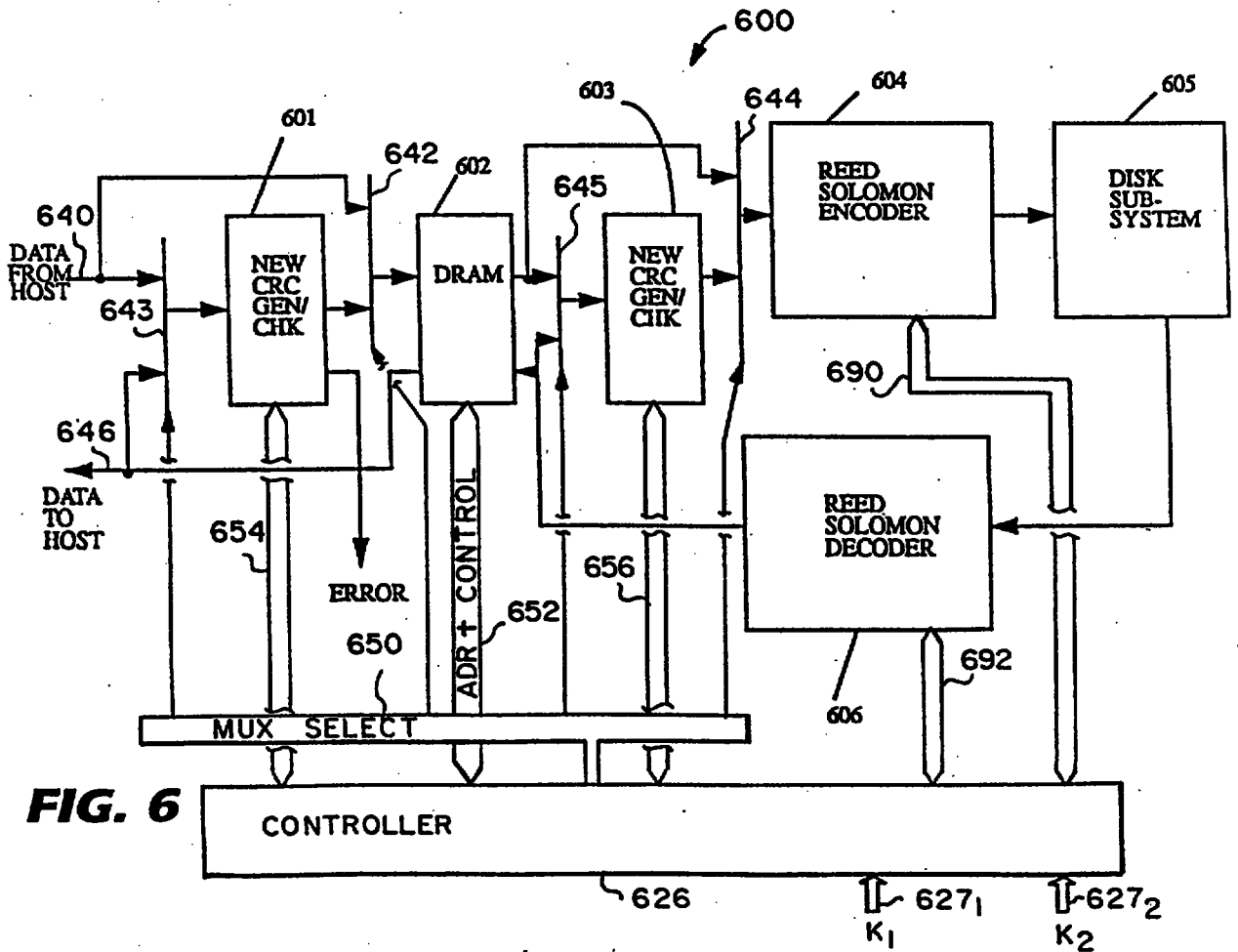
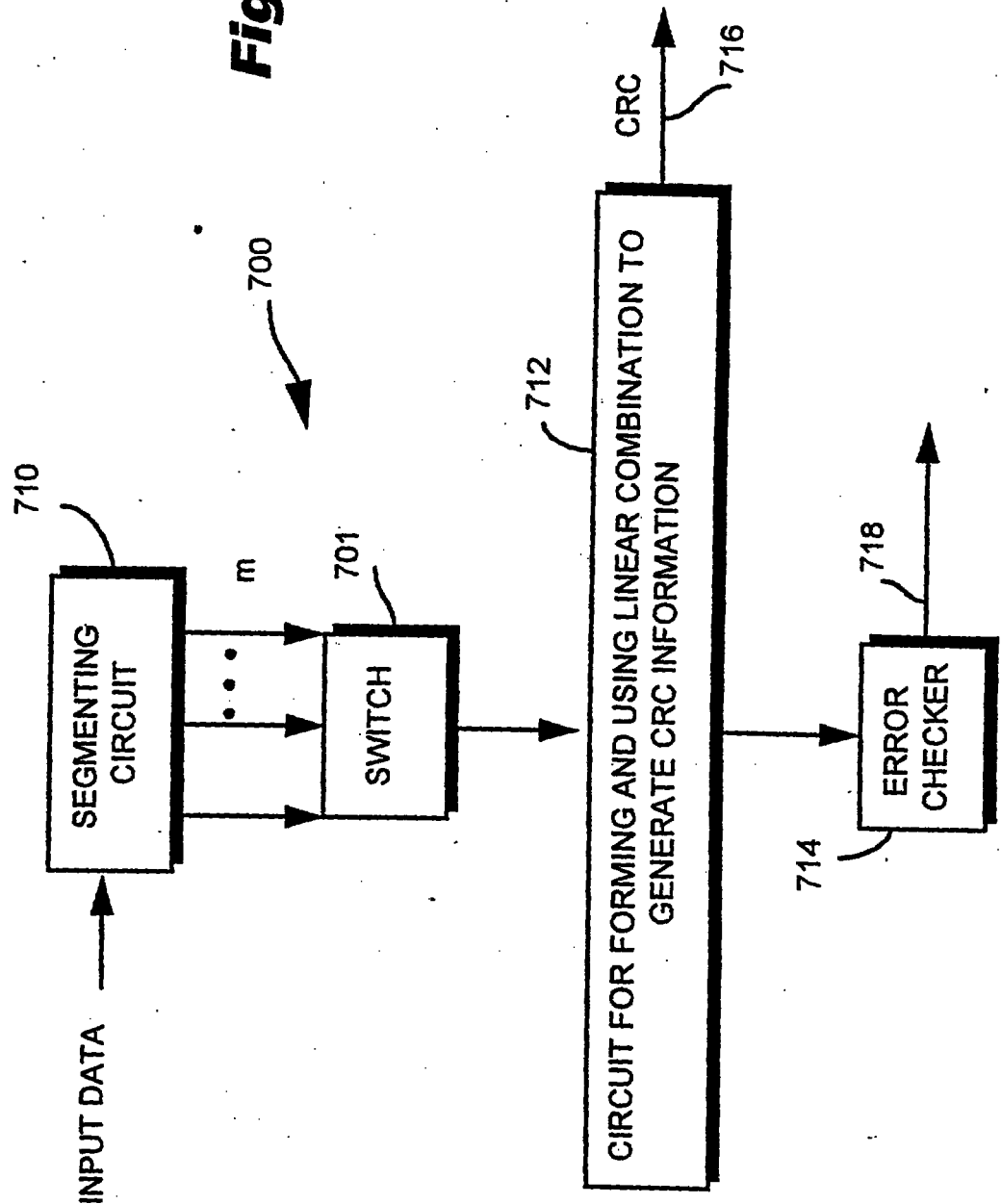


FIG. 6

THIS SHEET HAS BEEN
REPLACED

6/8

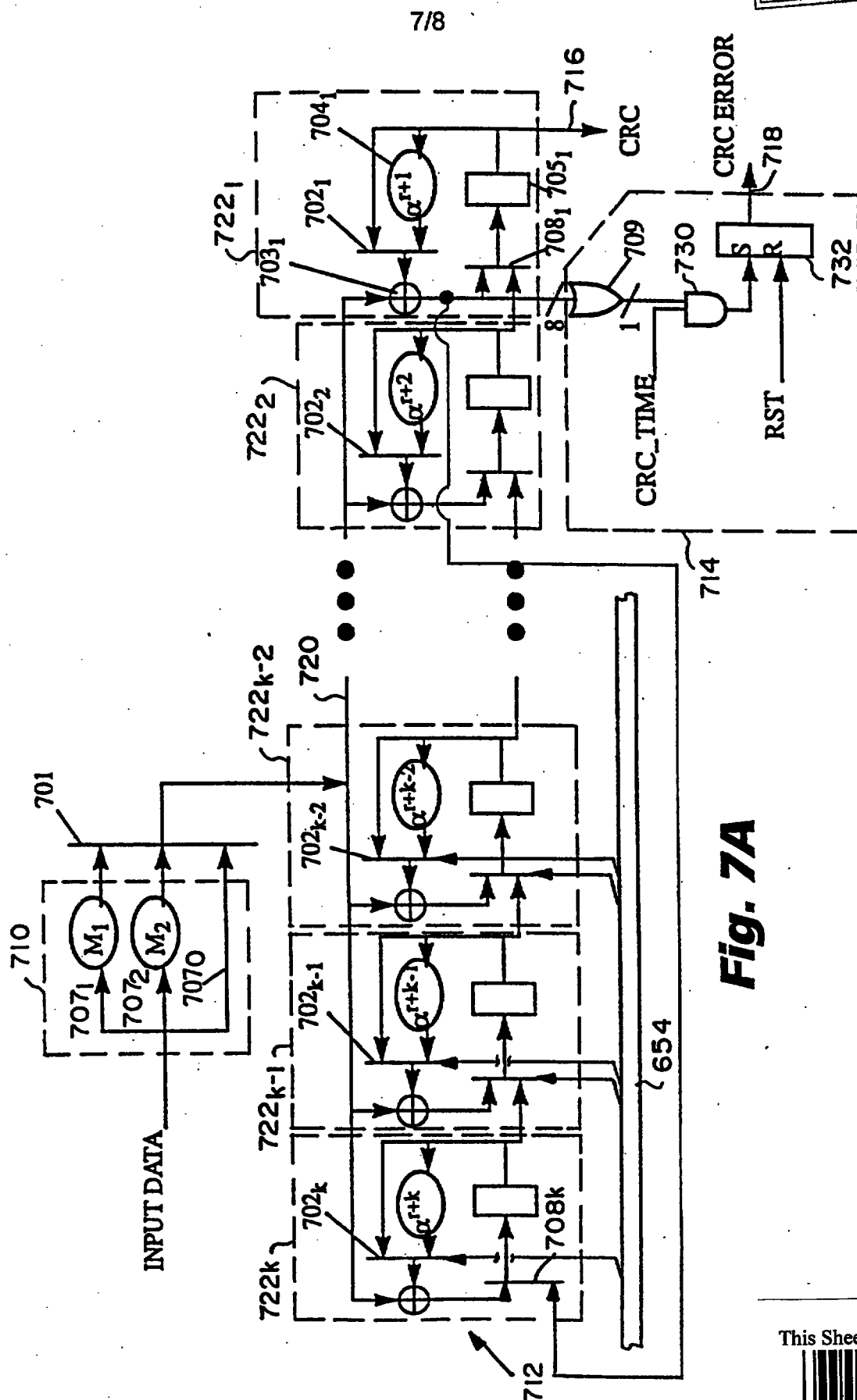
Fig. 7



This Sheet Has Been Replaced



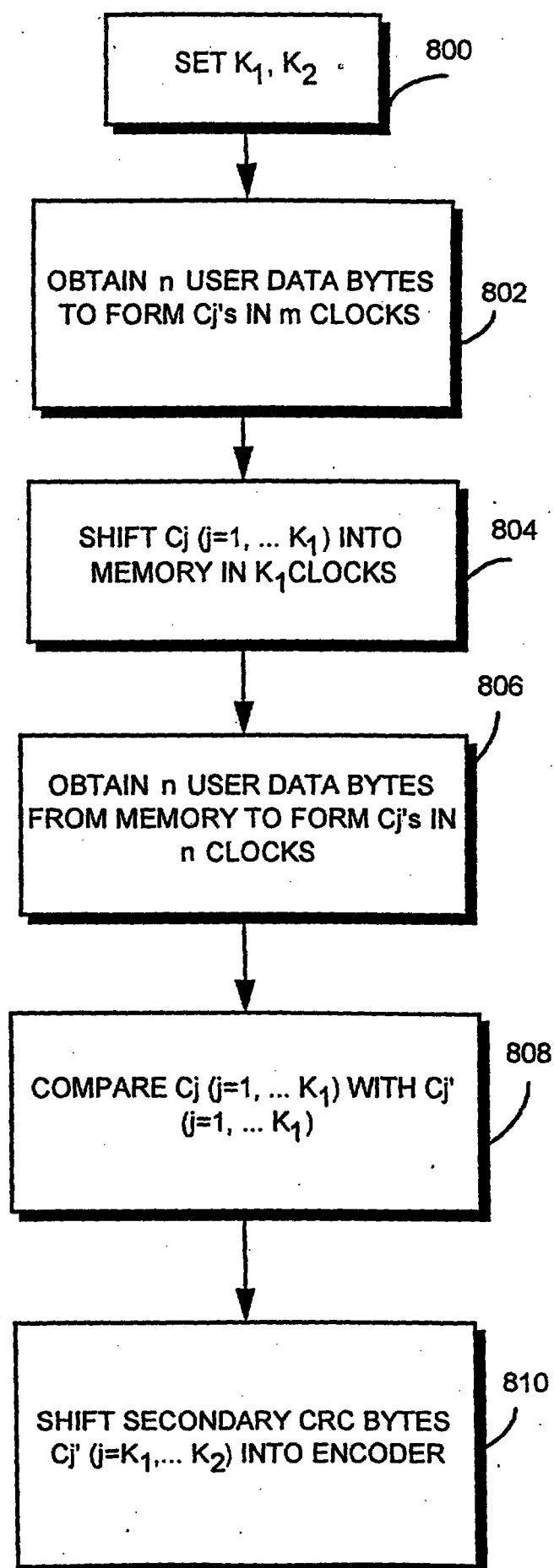
THIS SHEET HAS BEEN
REPLACED



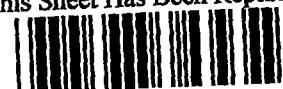
This Sheet Has Been Replaced



8 / 8

Fig. 8THIS SHEET HAS BEEN
REPLACED

This Sheet Has Been Replaced



-1-

**CYCLICAL REDUNDANCY CHECK
METHOD AND APPARATUS**

BACKGROUND

Cross-References to Related Applications

This patent application is a continuation application of United States Patent Application Serial Number 08/147,865, filed November 4, 1993, entitled DUAL PURPOSE CYCLICAL REDUNDANCY CHECK, which is incorporated herein by reference. Patent applications filed concurrently (inventor: Christopher P. Zook) with this patent application and incorporated herein by reference U.S. Patent Application Serial Number 08/____,____ (attorney docket: 1777-6) entitled "FINITE FIELD INVERSION"; U.S. Patent Application Serial Number 08/____,____ (attorney docket: 1777-9) entitled "BURST ERROR CORRECTOR", U.S. Patent Application Serial Number 08/____,____ (attorney docket: 1777-7) entitled "REED SOLOMON DECODER", and U.S. Patent Application Serial Number 08/____,____ (attorney docket 1777-10) entitled "ERROR CORRECTION METHOD AND APPARATUS". Patent applications filed concurrently with United States Patent Application Serial Number 08/147,865 filed November 4, 1993 (and all hereby incorporated herein by reference) include U.S. Patent Application Serial Number 08/147,758 entitled "FINITE FIELD INVERSION", U.S. Patent Application Serial Number 08/148,068 entitled "BURST ERROR CORRECTOR", and U.S. Patent Application Serial Number 08/147,650, entitled "REED SOLOMON DETECTOR".

1. Field of Invention

This invention relates generally to digital data communication systems, particularly to the detection of transmission errors by the use of codes.

31 DEC 1996

-2-

2. Related Art and Other Considerations

In a digital data communication system (including storage and retrieval from electronic memory, optical media or magnetic media) errors may occur as a result of noise, media defects or circuit failure. For reliable communications it is necessary to be reasonably sure of detecting all transmission errors. One way of doing this is by the use of cyclic redundancy check symbols or CRCs. In general CRCs are calculated by treating the data as the coefficients of a polynomial, dividing the data by another polynomial, and keeping the remainder. The data and CRC together make up a codeword which is then transmitted into the communication channel. At a receiving end of the channel a CRC is again calculated and compared to the original. A discrepancy between the two CRCs indicates a transmission error.

In some applications the data and CRC together are coded into an error-correcting code by adding error-correcting characters (ECC). After a correction procedure has been used the CRC can be used to detect errors that are either not detected or are miscorrected by the corrector.

The data can be viewed as a sequence of binary bits or a sequence of multi-bit symbols. In general a bit-oriented CRC is desired if the expected errors are random bit errors and a symbol-oriented CRC is desired if the expected errors are burst errors or random symbol errors.

Fig. 1 shows a typical bit-oriented 8-bit CRC generator where the serial input is on the DATA line. The generator in Fig. 1 will generate an 8-bit CRC character which can be used to detect any error which affects at most two bits in the serial data stream.

31 DEC 1996

-3-

Fig. 2 shows a typical byte-oriented 8-bit CRC generator where D_0 to D_7 make up the input data byte. The generator in Fig. 2 will generate an 8-bit CRC character which can be used to detect any single-byte error. It cannot, however, detect every two-bit error since the two errors could be in two different bytes.

Fig. 3 shows a data transmission system which includes a dynamic RAM (DRAM) for temporary storage and a communication channel which could be, for example, magnetic storage. The system uses an ECC system to correct errors occurring in the communication channel. It also employs a two-byte CRC to check for errors in data retrieved from the DRAM and to check the results of the corrector. For ECC purposes the data is partitioned into three interleaves. Each interleave makes up one ECC codeword containing two ECC bytes which can correct one byte in each interleave. This is a common technique for making a system capable of correcting a burst error of three bytes but using an ECC capable of correcting only one byte. Conceptually, during ECC generation using the system of Fig. 3, the first data byte goes into ECC generator 1, the second byte goes into ECC generator 2, the third byte goes into ECC generator 3, the fourth byte goes into ECC generator 1, etc. After the data has been input to the generators the first ECC byte comes from the generator which follows the generator which received the last data byte and the remaining ECC bytes are taken from the generators in the same sequence as previously described. All signal lines are 8 bits wide.

The CRC system of Fig. 3 will detect all two-byte errors (and consequently all two-bit errors) in a block of data read from the DRAM. However, regardless of which CRC and ECC polynomials are used, it is possible to have three errors in one interleave which are not detected by the ECC or CRC.

35

SUMMARY

The invention features both one stage and two stage CRC generation systems which include a programmable CRC generator/checker. The CRC generation/checker comprises
5 a segmenting circuit (for segmenting an input stream of user data into a plurality m of sub-streams); a circuit which forms a linear combination of the plurality m of sub-streams and operates upon the linear combination in order to generate CRC bytes; and, a checker circuit for comparing the
10 generated CRC bytes with previously generated CRC bytes.

In connection with preparation of CRC bytes prior to an encoding operation of a two stage system, input user data is first applied to a first CRC generator/checker for the generation of K_1 number of primary CRC bytes. The input
15 user data and associated resultant CRC bytes are then stored in a memory. Prior to encoding, a data block obtained from the memory (including both the user data and the primary CRC bytes) is applied to a second CRC generator/checker. User data from the memory is utilized by the second CRC
20 generator/checker to generate verification CRC bytes. Following generation of the verification CRC information units, during K_1 number of verification clock cycles, the first K_1^{th} verification CRC bytes are compared with the K_1 number of primary CRC bytes for the purpose of detecting any
25 errors occurring with respect to the memory. After the verification, a number $K_2 - K_1$ of verification CRC bytes generated by the second CRC generator/checker is optionally applied to the encoder as secondary CRC bytes, thereby adding additional CRC information prior to encoding and
30 storage of a block on a storage medium.

In connection with processing of CRC information after a decoding operation of a two stage system, decoded user data (including CRC bytes) is applied both to the
35 second CRC generator/checker and to the memory. The second CRC generator/checker receives the user data and CRC bytes

-5-

in much the same manner as it does prior to an encoding operation, generating K_2 number of verification CRC bytes for comparison with a like number of corresponding CRC bytes obtained from the decoded data. When the decoded data is
5 retrieved from the memory for sending to a host, the decoded data is sent to the first CRC generator/checker to check for memory errors.

The first CRC generator/checker and the second CRC generator/checker are configured to generate as many as k
10 number of CRC bytes. However, the number of CRC bytes K_1 and K_2 actually outputted by the respective first and second CRC generator/checkers is programmable, so that K_1 and K_2 may be unequal (e.g., $K_2 > K_1$) for a specified encoding/decoding operation and changeable from one
15 encoding/decoding operation to another.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features, and advantages of the invention will be apparent from the
20 following more particular description of preferred embodiments as illustrated in the accompanying drawings in which reference characters refer to the same parts throughout the various views. The drawings are not necessarily to scale, emphasis instead being placed upon
25 illustrating the principles of the invention.

Fig. 1 is a schematic block diagrammatic view of a typical bit-oriented 8-bit CRC generator.

Fig. 2 is a schematic block diagrammatic view of a typical byte-oriented 8-bit CRC generator.

30 Fig. 3 is a schematic block diagrammatic view of a data path which includes a CRC generator and checker, a DRAM, and a communication channel with ECC protection.

Fig. 4 is a schematic block diagrammatic view of a one stage CRC generation system according to an embodiment
35 of the invention and provided with memory error checking.

3 1 DEC 1996

REPLACEMENT SHEET

Date : 3 0 DEC 1996

-6-

Fig. 4A a schematic block diagrammatic view of a one stage CRC generation system of Fig. 4 which uses an adder and a conventional CRC generator.

5 Fig. 5 a schematic block diagrammatic view of the adder of Fig. 4A.

Fig. 6 is a schematic block diagrammatic view of a two stage CRC generation system according to an embodiment of the invention.

10 Fig. 7 is a schematic block diagrammatic view of a CRC generator/checker of the CRC generation system of Fig. 6.

Fig. 7A is a detailed schematic block diagrammatic view of an embodiment of the CRC generator/checker of Fig. 7.

15 Fig. 8 is a flowchart depicting basic steps executed by the CRC generation system of Fig. 6 in connection with two stage CRC generation prior to encoding.

DETAILED DESCRIPTION OF THE DRAWINGS

20 The invention includes both one stage and two stage CRC generation systems. Fig. 4 shows a generalized one stage CRC generation system 400 collaterally provided with memory error checking; Fig. 6 shows a generalized two stage CRC generation system 600 with in-line memory
25 checking. As discussed subsequently, both one stage CRC system 400 and two stage CRC system 600 employ a CRC generator/checker which can be a novel CRC generator/checker of the type basically illustrated in Fig. 7. In the
embodiments illustrated in Fig. 4 and Fig. 6 the CRC systems
30 400 and 600 are used in conjunction with an ECC system which, in the preferred embodiment, is a three-way interleaved Reed-Solomon code.

The invention includes a method and apparatus that is capable of generating and checking CRC information units
35 (e.g., bytes) and which is order-programmable. The CRC bytes

31 DEC 1996

-7-

are used to detect random errors occurring in DRAM and also to detect uncorrectable errors occurring in the communication channel.

5

SINGLE STAGE SYSTEM

The one stage CRC generation system 400 of Fig. 4 includes an encoding side and a decoding side. The encoding side of system 400 comprises CRC generator 401; memory (e.g., DRAM) 402; a set of ECC generators 420₁, 420₂, 420₃; and a CRC checker circuit 422, all under control of encoding controller 426. The encoding side of system 400 applies encoded data (including both CRC and ECC bytes) to a communication channel 430. Communication channel 430 in turn outputs received data to the decoding side. The decoding side of system 400 includes a error correction unit 432 and a CRC checker circuit 434, both under the control of decoding controller 436.

The encoding side of system 400 receives input electrical signals at a port 440 (e.g., a port from a host device). As used herein, a port such as port 440 receives a sequence of electrical signals representing a user data stream, the user data stream comprising bytes where each byte is an element of the finite field $GF(2^p)$ and where a byte can be of any p-bit arbitrary length. The user data stream is organized into blocks of electrical signals representing digital data, each block containing n data symbols, wherein each block is mathematically represented by the polynomial $D(x)$.

The electrical signals from port 440 are applied both to an input port CRC generator 401 and a first input port of a multiplexer 442. An output port of CRC generator 401 is connected to a second input port of multiplexer 442. An output port of multiplexer 442 is connected to a data input port of DRAM 402. A data output port of DRAM 402 is connected to: a first input port of channel multiplexer

31 DEC 1996

-8-

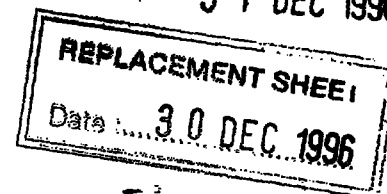
444; an input port of CRC checker 422; and (via ECC input multiplexer 446) to a selected one of the ECC generators 420₁, 420₂, 420₃. Output ports of the ECC generators 420 are connected to respective input ports of ECC output multiplexer 448.

Encoding controller 426 controls the sequencing (e.g., timing) and operating of the constituent elements of the encoding side of system 400, including the application of signals (e.g., multiplexing) to and from such elements. Controller 426 is connected to DRAM 402 by an address and control bus 450; to MUXes 442, 444, 446, and 448 by a MUX SELECT bus 452; to CRC generator 401 by CRC generator control bus 454; and, to CRC checker 422 by CRC checker control bus 456. These and other unillustrated connections of controller 426 are understood by the man skilled in the art, such as unillustrated connections for controlling ECC generators 420, for example.

On the decoding side of system 400, error correction unit 432 receives and corrects data from channel 430. The corrected data is output on data bus 460, which data is also applied to CRC checker 434. Decoding controller 436 is connected by CRC checker control bus 462 to control the operation of CRC checker 434.

In one embodiment, the CRC generator 401, CRC checker 422, and CRC checker 434 take the form of a novel generator/checker subsequently illustrated with respect to Fig. 7. However, in another embodiment (system 400A) illustrated in Fig. 4A, CRC generator 401, CRC checker 422, and CRC checker 434 are conventional CRC units augmented by m-way adder circuits 471, 472, and 474, respectively. That is, m-way adder circuits 471, 472, and 474 are connected upstream of the respective CRC generator/checkers 401, 422, 434. In other respects, the elements of system 400A resemble like-numbered elements of system 400.

3 1 DEC 1996



-9-

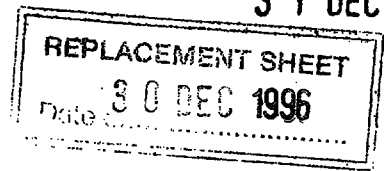
Fig. 5 illustrates the configuration of m-way adder circuits 471, 472, and 474. Each m-way adder circuit includes an adder 480 and a register 482. In the system 400B shown in Fig. 4A, each m-way adder circuit is a 3-way adder circuit.

The system 400A shown in Fig. 4A resembles that shown in Fig. 3 except, that the input user data from port 440 is segmented into groups of three bytes. The sum of the three bytes in each group is sent to the conventional CRC generator 410. The first byte in each group will ultimately be sent to ECC generator 420₁, the second byte in each group will ultimately be sent to ECC generator 420₂, and the third byte in each group will ultimately be sent to ECC generator 420₃. The CRC generator 401 is only clocked once for each three bytes. In Fig. 5 the register 482 is reset on the third clock of each three-byte group.

TWO STAGE SYSTEM

Fig. 6 shows a two stage CRC generation system 600 which generally comprises a first CRC generator/checker 601 for generating primary CRC information; a memory (e.g., DRAM) 602; a second CRC generator/checker 603 (for, e.g., generating secondary CRC information); an encoder (such as a Reed Solomon encoder) 604; a data utilization device (such as a disk sub-system) 605; a decoder (such as a Reed Solomon decoder) 606; and, a controller 626.

System 600 also includes a host port 640 connected to an unillustrated host device. Host port 640 is connected to apply an input user data stream to a first input port of DRAM input multiplexer 642 and to a first input port of first CRC generator multiplexer 643. An output port of multiplexer 643 is connected to an input port of first CRC generator/checker 601. An output port of generator/checker 601 is connected to a second input port of DRAM input multiplexer 642. An output port of DRAM multiplexer 642 is



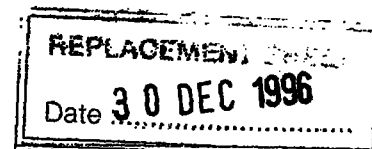
-10-

connected to a first input port of DRAM 602. A first output port of DRAM 602 is connected both to a first input port of encoder input multiplexer 644 and to a first input port of second CRC generator/checker multiplexer 645. An output port of multiplexer 645 is connected to an input port of second CRC generator/checker 603. An output port of generator/checker 603 is connected to a second input port of encoder input multiplexer 644. An output port of multiplexer 644 is connected to an input port of encoder 604.

Disk sub-system 605 has both a data input port and a data output port. The data input port of disk sub-system 605 is connected to receive data from an output port of encoder 604. The data output port of disk sub-system 605 is connected to apply data to an input port of decoder 606.

An output port of decoder 606 is connected both to a second input port of second CRC generator multiplexer 645 and to a second data input port of DRAM 602. DRAM 602 has a second output port which is connected both to a host port 646 and to a second input port of first CRC generator multiplexer 643.

Controller 626 is connected to control the timing and sequencing of the operation of the constituent elements of system 600 as explained herein and as otherwise understood by the man skilled in the art. For example, controller 626 is connected to multiplexers 642, 643, 644, and 645 by a multiplexer select bus 650; to DRAM 602 by a DRAM address and control bus 652; to first CRC generator/checker 601 by a first CRC generator control bus 654; to the second CRC generator/checker 603 by a second CRC generator control bus 656; to encoder 604 by encoder control bus 690; and, to decoder 606 by decoder control bus 692. Controller 626 has a plurality of input ports 627₁ and 627₂ for obtaining input values for programming system 600. In particular, input port 627₁ receives a value K₁



-11-

determinative of the number of CRC bytes to be outputted by first CRC generator/checker 601; input port 627₂ receives a value K₂ determinative of the number of CRC bytes to be outputted by second CRC generator/checker 603.

5 In system 600, the first CRC generator/checker 601 is connected (via MUX 643) to host port (640) for generating primary CRC information based on input user data received from the host device. Memory 602 stores input user data received from the host device and the primary CRC
10 information generated with respect thereto by the first CRC generator/checker 601. Second CRC generator/checker 603, connected to memory 602 via MUX 645, serves to check data retrieved from memory 602 and (optionally) to generate secondary CRC information based on data obtained from memory
15 602 including the primary CRC information. Encoder 604 forms encoded information by utilizing the data obtained from memory 602 including the primary CRC information as well as optional secondary CRC information obtained from second CRC generator/checker 603.

20 Decoder 606 receives input data and decodes the input data into decoded input data including decoded CRC information. Decoder 606 applies the decoded input data including the decoded CRC information to second CRC generator/checker 603 and to memory 602. Second CRC
25 generator/checker 603 validates the decoded CRC information included in the decoded input data. First CRC generator/checker 601 is connected to receive decoded input data including the decoded CRC information stored in memory 602 for validating decoded CRC information received from
30 memory 602.

35 Thus, in an encoding operation, second CRC generator/checker 603 compares the primary CRC information and verification CRC information generated by second CRC generator/checker 603 to determine errors attributable to memory 602. Encoder 604 is also connected to second CRC

REPLACEMENT SHEET

Date : 30 DEC 1996

-12-

generator/checker 603 and also utilizes the secondary CRC information to form the encoded information. Conversely, in a decoding operation, first CRC generator/checker 601 determines errors attributable to memory 602.

5

CRC GENERATOR/CHECKER STRUCTURE

Fig. 7 generally depicts a CRC generator/checker 700 suitable for use as the CRC generators and CRC checkers described herein. Generator/checker 700 basically includes a segmenting circuit 710; a switch or multiplexer 701; a circuit 712 for forming and using a linear combination of user data sub-streams to generate CRC information; and, an error checker circuit 714. Segmenting circuit 701 serves to segment an input stream of user data into a plurality m of sub-streams for application to switch 701. Switch 701 selects from the plurality of user data sub-streams in accordance with clock cycle and applies the selected user data sub-stream to circuit 712. The resultant CRC information, preferably in the form of CRC bytes, is outputted on parallel CRC bus 716. When generator/checker 700 is employed to check received CRC information previously generated on the basis of received data, the previously generated CRC information is compared by error checker 714 with verification CRC information currently generated (with respect to the same user data) by circuit 712. Should the previously generated and currently generated verification CRC information differ, an error signal is generated on CRC error line 718.

20

25

30

35

Fig. 7A shows structural details of one particular implementation of CRC generator/checker 700, and particular an implementation wherein $m=3$. Accordingly, segmenting circuit 710 of Fig. 7A is shown to include three sub-stream lines 707_0 , 707_1 , 707_2 . For reasons hereinafter discussed, sub-stream line 707_1 and 707_2 have multipliers M_1 and M_2 connected thereon. Switch 701 is a three-input multiplexer

REPLACEMENT SHEET

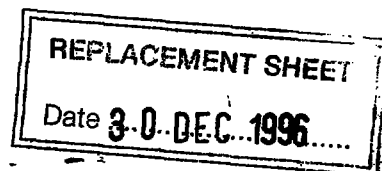
Date 3.0. DEC. 1996.....

-13-

having input selected by controller 626 (via a control bus). An output port of multiplexer 701 is connected to apply the sub-stream selected thereby to adder input bus 720.

As shown in Fig. 7A, circuit 712 comprises k
5 number of sub-circuits 722₁ - 722_k for generating as many as k bytes of CRC information with respect to the linear combination of sub-streams. As explained below, each sub-circuit 722 is a divider having a divisor which is a power of α . Each sub-circuit 722 comprises an adder input
10 multiplexer 702; an adder 703; a multiplier 704; a register 705 for storing CRC information; and, a register input multiplexer 708. Each adder 703 has a first input port, a second port, and an output port. The first port of each adder 703 is connected to adder input bus 720 so that the
15 plurality of sub-streams can be multiplexed thereto. Each multiplier 704 has an output port thereof selectively connected (via a first input port of associated multiplexer 702) to the second input port of its associated adder 703. Each register 705 has an input port connected to the output
20 port of associated adder 703 and its output port is selectively connected (via a first input port of associated multiplexer 702) to the second input port of the adder 703. Each register 705 stores CRC information in the form of a CRC byte which is related to an error correcting code. Each
25 of the multiplexers 702 and 708 are controlled by controller 626 (for example, via control bus 654).

From the foregoing it is understood that sub-circuits 722 are numbered from a first sub-circuit 722₁ to a kth sub-circuit 722_k. Registers 705 of the sub-circuits 722
30 are connected so that CRC information stored therein can be rightwardly shifted. The rightward shift occurs after the n clock cycles executed to generate the CRC bytes in registers 705. After the n clock cycles are executed to generate the CRC bytes, the CRC bytes in registers 705 are shifted
35 rightwardly a desired number of clocks (as input to



-14-

controller 626), one register (e.g., one sub-circuit) per clock. For example, considering the operation of first CRC generator/checker 601, if an input value of 4 is inputted at input port 627, of controller 626, during a first shift
5 clock cycle the CRC byte in register 705₁ is shifted out on CRC bus 716; the CRC byte in register 705₂ is shifted into register 705₁; the CRC byte in register 705₃ is shifted into register 705₂; and so forth. Such shifting continues for four shift clock cycles, so that the CRC values initially in
10 registers 705₁ - 705₄ are ultimately shifted out to CRC bus 716.

The values of the multipliers 704 are chosen so that the multiplier multiplies by a power of a field element α , the power being $r+1$ for the multiplier of the first sub-circuit 722₁ and $r+k$ for the multiplier of the k^{th} sub-circuit 722_k.
15

The output port of adder 703₁ is connected to error checker circuit 714 and to MUX 708_k. As illustrated in Fig. 7A, error checker circuit 714 comprises an 8-input
20 OR gate 709 which is connected to the output port of adder 703₁. Error checker circuit 714 further includes an AND gate 730 and an R/S flip-flop or latch 732. An output pin of OR gate 709 is connected to a first input pin of AND gate 730, a second input pin of AND gate 730 being connected to
25 receive a signal CRC_TIME from controller 626. An output pin of AND gate 730 is connected to a set pin of flip-flop 732; a reset pin of flip-flop 732 receives a signal RST from controller 626. Since adder 703₁ is involved in verifying previously-generated CRC information with currently
30 generated CRC information in the manner hereinafter described, sub-circuit 722₁ is denominated the "comparison" sub-circuit.

REPLACEMENT SHEET

Date 30 DEC 1996

-15-

TWO STAGE ENCODING OPERATION

Fig. 8 depicts basic steps executed by system 600 of Fig. 6 in connection with two stage CRC generation prior to encoding. Prior to actual CRC generation, as depicted by step 800 of Fig. 8, controller 626 is programmed with values K_1 and K_2 for determining the amount (e.g., number of bytes ranging from 1 to k) of CRC information to be shifted out of first CRC generator 601 and second CRC generator 602, respectively.

In connection with encoding aspects of the CRC generation of system 600 of Fig. 6, bytes of user data from the host are sent to first CRC generator/checker 601 and are written into DRAM 602. Step 802 of Fig. 8 shows first CRC generator/checker 601 obtaining n bytes of user data from the host and using the n bytes of user data to form CRC bytes C_j ($j=1,2,\dots,k$) during n clock cycles. After the n clock cycles for generating CRC bytes C_j ($j=1,2,\dots,k$), during the next K_1 clock cycles (step 804) first CRC generator/checker 601 shifts CRC bytes

$$C_1, \dots, C_{K_1}$$

also known as the primary CRC bytes, into DRAM 602.

In connection with the execution of step 802, and specifically with reference to generator/checker 700 illustrated in Fig. 7, during the first of the n clock cycles multiplexer 701 switches the first of the n user data bytes onto adder input bus 720. Concerning such first byte obtained on line 707₀ of segmenting circuit 710, M_0 for segmenting circuit 710 may always be selected as α^0 and hence no multiplier is needed for M_0 . During the second of the n clock cycles multiplexer 701 switches the second of the n user data bytes (multiplied by M_1) onto adder input bus 720; during the third of the n clock cycles multiplexer 701 switches the third of the n user data bytes (multiplied by M_2) onto adder input bus 720.

REPLACEMENT SHEET

Date 3.0 DEC 1996

-16-

Thus, during a data portion of generation or checking depicted by step 802, MUX 701 supplies the dividers (e.g., sub-circuits 722) with the input user data multiplied by M_0 (from lead 707₀) on the first clock and on every third clock following the first, it supplies the dividers 722 with the input user data multiplied by M_1 (from lead 707₁) on the second clock and on every third clock following the second and it supplies the dividers 722 with the input user data multiplied by M_2 (from lead 707₂) on the third clock and on every third clock following the third. In execution of step 802, MUXes 702 supply adders 703 with the outputs of constant multipliers 704 on the first clock and on every third clock following the first. MUXes 702 supply the adders 703 with the outputs of registers 705 on the other clocks. MUXes 708 supply the adder outputs to the inputs of registers 705.

During execution of step 804, which is a CRC portion of CRC generation or checking, i.e. when CRC bytes are being output, MUXes 708 connect the registers 705 into one shift register. During generation this allows the programmed number (K_1) of CRC bytes which reside in the registers 705 to be shifted out onto CRC bus 716. K_1 clock cycles are required in step 804 to shift out the K_1 number of desired CRC bytes. After the K_1 clock cycles, all registers 705 are re-initialized at zero, so that CRC bytes $K_1 \dots k$ are discarded.

As mentioned before, step 804 shows the shifting of the primary CRC bytes C_j ($j=1, \dots K_1$) into DRAM 602. At some later time (depicted by step 806), the block of data in DRAM 602 and the primary CRC bytes C_j ($j=1, \dots K_1$) are read from DRAM 602 and sent both to Reed-Solomon encoder 604 (via MUX 644) and to second CRC generator/checker 603 (via MUX 645). The data from the block in DRAM 602 is applied to second CRC generator/checker 603 in a manner such that n number of user data bytes are applied followed by the K_1

-17-

number of primary CRC bytes C_j ($j=1, \dots K_1$) generated by generator 601 with respect to those n bytes.

In step 806, second CRC generator/checker 603 receives the user data from DRAM 602 in groups of n number of input bytes. Using the n number of input bytes, during n number of clock cycles the second CRC generator/checker 603 generates k number of verification CRC bytes C_j' in similar manner as first CRC generator/checker 601 generated the primary CRC bytes C_j . If the user data bytes obtained from DRAM 602 in step 806 are identical to the user data bytes shifted into DRAM 602 from the host as occurs when DRAM is operating properly, then the verification CRC bytes C_j' will equal the respective primary CRC bytes C_j .

After second CRC generator/checker 603 has generated the verification CRC bytes C_j' during the n clock cycles of step 806, at step 808 secondary CRC generator/checker 603 performs a checking operation to compare primary CRC bytes C_j ($j=1, \dots K_1$) with the verification CRC bytes C_j' ($j=1, \dots K_1$). In so doing, MUX 701 is operated to apply the primary CRC bytes C_j ($j=1, \dots K_1$) from line 707₀ of segmenting circuit 710 to the first input port of ADDER 703₁, the application being made one byte per clock cycle for each of K_1 number of verification clock cycles. During a first of the verification clock cycles, the first primary CRC byte C_1 is applied to the first input port of ADDER 703₁ and the first verification CRC byte C_1' stored in register 705₁ is applied to the second input port of ADDER 703₁, so that the result of the addition operation of ADDER 703₁ is applied to check circuit 714. With each verification clock cycle, the verification CRC bytes C_j' in registers 705_j are shifted rightwardly by one sub-circuit 722 (e.g, to the next rightwardly adjacent register), as in the manner of CRC byte shift/readout described hereinbefore, so that after the first verification clock cycle register 705₁ will contain the verification CRC

-18-

byte C_2' . Similarly, during a second of the verification clock cycles, the second primary CRC byte C_2 is applied to the first input port of ADDER 703, and the second verification CRC byte C_2' now stored in register 705, is applied to the second input port of ADDER 703, again with the result of the addition operation of ADDER 703, is applied to check circuit 714. Such shifting and adding continues for each of the K_1 number of verification clock cycles, so that CRC bytes C_j are compared with corresponding bytes C_j' for $j=1, \dots K_1$.

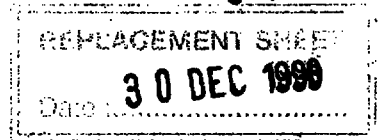
During execution of step 808, checker circuit 714 is effectively enabled by a signal CRC_TIME from controller 626. When checker circuit 714 is enabled, any inequality between a primary CRC byte C_j and its corresponding verification byte C_j' causes a non-zero output of OR gate 709 to be gated through AND gate 730 for application to flip-flop 732. The detected inequality causes flip-flop 732 to output a CRC ERROR signal to controller 626 on line 718.

If the value K_2 inputted to controller 626 with respect to second CRC generator/checker 603 is greater than the value K_1 , then at step 810 second CRC generator/checker 603 will shift out (on line 716) a number $(K_2 - K_1)$ of secondary CRC bytes, specifically CRC bytes C_j' ($j=K_1+1, \dots K_2$). In this regard, after execution of step 808, registers 705₁, 705₂, 705₃, etc. will contain

$$C_{K_1+1}, C_{K_1+2}, C_{K_1+3}, \text{etc.}$$

The shifting out of secondary CRC bytes C_j' ($j=K_1+1, \dots K_2$) occurs in $K_2 - K_1$ clock cycles, and is accomplished in the hereinbefore described manner of controlling multiplexers 708 for the rightward shift operation.

After a block of data including both the primary CRC bytes C_j ($j=1, \dots K_1$) and the secondary CRC bytes C_j' ($j=K_1+1, \dots K_2$) is encoded by encoder 604, the encoded block

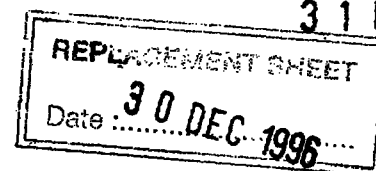


-19-

is written to disk subsystem 605. It will be appreciated by the man skilled in the art that encoder 604 generates ECC bytes for each interleave of data, preferably m number of interleaves using a ECC generator polynomial.

5 Thus, second CRC generator/checker 603 checks whether errors occurred in DRAM 602 and also may generate additional CRC bytes, known as secondary CRC bytes. These secondary CRC bytes may be written to the disk along with the primary CRC bytes. Inclusion of the secondary CRC bytes
10 can be important because the data read from disk may require more protection than the DRAM data owing to the fact that data from disk is more susceptible to error than data from DRAM 602.

 As described above, second CRC generator/checker
15 603 allows the incoming primary CRC bytes to be checked one at a time. It also shifts out as many of the $k-K_1$ remaining CRC bytes as are specified by the input value K_2 , these further shifted bytes being secondary CRC bytes). This facilitates a situation in which only the first K_1
20 number of primary CRC bytes are written into the DRAM 602 but K_2 are written to disk ($K_2 > K_1$). The checking of the primary CRC bytes is accomplished by adding the incoming primary CRC bytes to the newly generated verification CRC bytes by adder 703, and then detecting a non-zero byte with
25 OR gate 709. While CRC bytes are being input to the checker the CRC_TIME signal is ON and then any mismatches will set CRC_ERROR latch 732. The order of the generator is programmable since the CRC bytes are calculated independently of each other and hence only the desired
30 number of CRC bytes need be shifted out.



-20-

TWO STAGE DECODING OPERATION

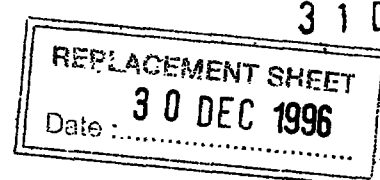
In connection with an decoding operation executed by system 600 of Fig. 6, a data block is read from the disk by disk sub-system 605 and is sent to Reed-Solomon decoder 606. Corrected data obtained by decoder 606 (including CRC bytes) is sent both to second CRC generator/checker 603 (to check for uncorrectable errors) and to DRAM 602.

Second CRC generator/checker 603 receives data bytes and CRC bytes from the decoded block in much the same manner as it does prior to an encoding operation. Upon receiving each group of n data bytes, second CRC generator/checker 603 generates K_2 number of verification CRC bytes for comparison with a like number of corresponding CRC bytes obtained from the decoded data. Operation of the second CRC generator/checker 603 in connection with post-decode CRC processing is analogous to steps 806 and 808 above-discussed, and understand with reference thereto. Second CRC generator/checker 603 performs a verification with respect to CRC bytes obtained from the disk sub-system 605.

In connection with post-decode CRC processing, when the data block is retrieved from DRAM 602 for sending to the host, the data block is again sent to first CRC generator/checker 601 to check for DRAM errors. Operation of the first CRC generator/checker 601 in connection with post-decode CRC processing is also analogous to steps 806 and 808 above-discussed, and understand with reference thereto, with the proviso that K_1 number of CRC bytes are processed by the first CRC generator/checker 601.

OPERATION: MATHEMATICAL BASES

In the illustrated embodiments, the data stream which feeds the CRC generator/checker 700 is segmented into groups of three bytes. A linear combination of the three bytes is then sent to a collection of circuits (e.g., sub-



-21-

circuits 722) which divide by $X + \alpha^{r^j}$ for $j = 1, 2, \dots, k$ where α is a primitive element of the field representation of the data bytes. In the preferred embodiment the field is $GF(256=2^8)$. The linear combination may be a simple sum, leading to the embodiment shown in Fig. 4A.

While a simple linear combination may be simple to implement, it is possible to have two bytes each with a single bit error in a block of data read from the DRAM which are not detectable owing to the fact that if the same error is in two bytes of a three-byte group then the two errors will cancel when summed together before being sent to the CRC generator/checker 700. Alternately the linear combination can be chosen so that if the three bytes in the group each have no more than a single "1" in each byte, then the linear combination will be non-zero. In that case, if every byte in error in a block of data contains only a single bit in error, then k CRC bytes can be used to detect k bytes in error even if some of the bytes in error are in the same three-byte group.

Using a linear combination of every three input bytes allows the CRC bytes to be generated in such a way as to increase the minimum distance of the ECC code by one for each CRC byte. This can be done because the ECC consists of three interleaves.

The CRC bytes are generated according to the following rule: Let the input bytes be denoted as D_0 to D_{n-1} . These bytes make up the coefficients of three polynomials, $F^0(x)$, $F^1(x)$ and $F^2(x)$, thusly:

$$F^s(x) = \sum_{k=0}^{t_s} D_{(3 \cdot k) + s} \cdot x^{t_s - k}$$

for $s = 0, 1, 2$ where t_s is the largest integer that is less than $(n-s)/3$. These polynomials represent the division of

-22-

D(x) into three groups, e.g. D_0 is in F^0 , D_1 is in F^1 , D_2 is in F^2 , D_3 is in F^0 , etc. These polynomials are precisely the same polynomials that are processed by the Reed-Solomon encoder 604 to form the three Reed-Solomon code words. $G(x)$ is defined as a linear combination of $F^0(x)$, $F^1(x)$ and $F^2(x)$ thusly:

$$G(x) = \sum_{s=0}^2 M_s \cdot F^s(x)$$

The system 400A in Fig. 4A corresponds to the case where the multipliers, M_s , are all 1. The system 600 in Fig. 6 corresponds to the case where the M_s are chosen so that $aM_0 + bM_1 + cM_2$ is non-zero as long as a, b and c each contain a single "1". The coefficients of $G(x)$ are linear combinations of three consecutive input bytes, e.g the first coefficient of $G(x)$ is $D_0M_0 + D_1M_1 + D_2M_2$, the second coefficient of $G(x)$ is $D_3M_0 + D_4M_1 + D_5M_2$, etc.

The j^{th} CRC byte, C_j , is defined as:

$$C_j = G(x) \bmod (x + \alpha^{r+j})$$

for $j = 1, 2, \dots, k$.

If only k or less of the input bytes D_i were non-zero, and the non-zero bytes each consisted of a single "1", then $G(x)$ would have at most k non-zero coefficients and $G(x)$ could not be zero. All of the CRC bytes are obtained by dividing $G(x)$ by consecutive powers of α , and therefore if there are k CRC bytes then at least one of the CRC bytes would be non-zero. This is equivalent to saying that any set of k or less single-bit errors would be detected.

The Reed-Solomon code to be used in conjunction with the new CRC generator has a generator polynomial which has, as roots, v consecutive powers of α , from α^{r-v+1} to α^r . Let $E(x)$ be an error polynomial which has been added to one of the ECC interleaves, i.e. one of the Reed-Solomon code

REPLACEMENT SHEET

Date: 30 DEC 1996

-23-

words. If the error is not detectable by the ECC, then $E(x)$ must have roots which include α^{r-v+1} to α^r . Since the factors used in CRC generation have as roots the k consecutive powers of α , from α^{r+1} to α^{r+k} , for the error not to be
 15 detected by the CRCs, $M_k E(x)$ must have roots which include α^{r+1} to α^{r+k} . This implies that $E(x)$ must have roots which include α^{r-v+1} to α^{r+k} , which means that the error has more than $k+v$ bytes in error.

The set of M_1 and M_2 constants which cause $a + bM_1 + cM_2$ to be non-zero for all a , b and c which have a single
 10 "1" is not unique. Therefore M_1 and M_2 are picked to satisfy that condition and to also cause linear combinations of other classes to be non-zero. For example, in the preferred embodiment the field generator polynomial is
 15 $X^8 + X^4 + X^3 + X^2 + 1$. M_1 is chosen to be α^{25} and M_2 is chosen to be α^{112} . This choice causes $a + bM_1 + cM_2$ to be non-zero for the case where only two of the three bytes a , b and c are non-zero and the two bytes each have a single 3-bit or shorter non-zero bit sequence. After adding this condition the
 20 choice of M_1 and M_2 is still not unique, therefore an additional condition is added which is to maximize the number of two-byte combinations where each byte can have a single 4-bit or shorter non-zero bit sequence. The M_1 and M_2 multipliers each consist of a set of XOR gates such that
 25 the output bits are linear combinations, i.e. XOR sums, of certain subsets of the input bits and these subsets are listed in Table I and Table II.

REPLACEMENT SHEET

Date : 30 DEC 1996

-24-

Table I
M₁ multiplier

OUT0 = IN0 + IN7
OUT1 = IN0 + IN1
OUT2 = IN1 + IN2 + IN7
OUT3 = IN2 + IN3 + IN7
OUT4 = IN3 + IN4 + IN7
OUT5 = IN4 + IN5
OUT6 = IN5 + IN6
OUT7 = IN6 + IN7

Table II
M₂ multiplier

OUT0 = IN0 + IN1 + IN5 + IN6 + IN7
OUT1 = IN1 + IN2 + IN6 + IN7
OUT2 = IN1 + IN2 + IN3 + IN5 + IN6
OUT3 = IN1 + IN2 + IN3 + IN4 + IN5
OUT4 = IN1 + IN2 + IN3 + IN4 + IN7
OUT5 = IN2 + IN3 + IN4 + IN5
OUT6 = IN3 + IN4 + IN5 + IN6
OUT7 = IN0 + IN4 + IN5 + IN6 + IN7

-25-

For example, the CRC generator/checker of this invention has been illustrated in conjunction with a three-way interleaved Reed-Solomon code. It may alternately be employed with, for example, a two-way or four-way interleaved code. The principles taught with the illustrated CRC can be applied to a CRC for use in conjunction with encoders not limited to the Reed-Solomon design. The method of this invention can be used for codeword generation, codeword checking or both. It can be used between a computer host and a DRAM, between a DRAM and a magnetic disk, or between two ends of any communication channel. The same CRC can be used in more than one communication channel of a system, for example both between the host and a DRAM and between the DRAM and storage disk.

The CRC of this invention can be programmed to generate k CRC bytes. In conjunction with a Reed-Solomon code the CRC allows detection of k more errors than the Reed-Solomon code is capable of detecting. The number k can be tailored to the propensity for errors of a given communication channel. When the same CRC is used for more than one communication channel, different values of k can be selected for each channel. The CRC of this invention can also be utilized in a non-programmable embodiment having a fixed number of CRC bytes.

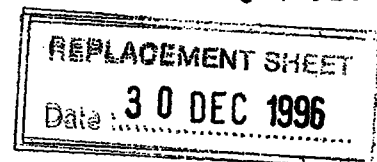
A hardware implementation of this invention has been illustrated. The CRC can also be implemented with software. Specific circuitry to implement the block diagram of Fig. 7 of this invention can be readily designed by a routiner in the electronic arts. Variations on the block diagram will also be apparent to those skilled in the art. Specific examples of a field generator polynomial and of the constant multipliers M_i have been supplied. Other constants and polynomials can be chosen, as taught herein. For example, instead of dividing by two eight bit polynomials, division can instead occur with one sixteen bit polynomial.

REPLACEMENT SHEET
3 0 DEC 1996
Date :

-26-

U.S. Patent Application Serial Number 08/____,____
(attorney docket 1777-10) simultaneously filed by Zook et
al., entitled "ERROR CORRECTION METHOD AND APPARATUS", and
incorporated herein by reference, provides one non-limiting
example of a specific utilization of the present invention.

While the preferred embodiment has been disclosed
and described in detail herein, it will be obvious to those
skilled in the art that various changes in form and detail
may be made therein without departing from the spirit and
scope thereof.



-27-

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A cyclical redundancy check (CRC) generator which generates CRC information for error checking purposes, comprising:
 - a segmenting circuit for segmenting an input stream of data into a plurality of sub-streams;
 - a circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information.
2. The apparatus of claim 1, wherein the segmenting circuit segments the input stream into three sub-streams.
3. The apparatus of claim 1, wherein the segmenting circuit includes a multiplier for multiplying at least one of the sub-streams by a constant.
4. The apparatus of claim 3, wherein the multiplier is chosen so that a linear combination of certain bytes in the sub-stream is non-zero.
5. The apparatus of claim 4, wherein the constant is a power of a field element α .
6. The apparatus of claim 5, wherein there are three sub-streams, each sub-stream constituting a byte of data, and wherein one sub-stream is multiplied by a constant M_1 and another sub-stream is multiplied by a constant M_2 , and wherein $M_1 = \alpha^{25}$ and $M_2 = \alpha^{112}$.



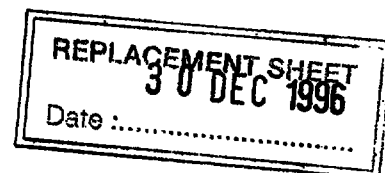
* C L M S *

REPLACEMENT SHEET
Date: 30 DEC 1996

-28-

7. The apparatus of claim 1, wherein each sub-stream constitutes a byte of data, and wherein the circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information comprises k number of sub-circuits for generating k bytes of CRC information with respect to the linear combination of sub-streams.
8. The apparatus of claim 1, wherein each sub-stream forms at least part of a data polynomial, and wherein the circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information comprises k number of divider sub-circuits for generating k bytes of CRC information with respect to the linear combination of sub-streams.
9. The apparatus of claim 8, wherein each divider sub-circuit divides the data polynomial by a divisor which is related to a root of an ECC polynomial.
10. The apparatus of claim 1, wherein the circuit which forms a linear combination of the plurality of sub-streams and operates upon the linear combination in order to generate the CRC information comprises a plurality of sub-circuits, each sub-circuit comprising:
- an adder, the adder having a first input port, a second port, and an output port, the first port of the adder having the plurality of sub-streams multiplexed thereto;
 - a multiplier, the multiplier having an output port thereof selectively connected to the second input port of the adder;
 - a register for storing CRC information, the register having an input port connected to the output port of the adder and an output port selectively connected to the second input port of the adder.





-29-

11. The apparatus of claim 10, wherein k number of sub-circuits are provided numbered from a first sub-circuit to a k^{th} sub-circuit, and wherein the registers of the sub-circuits are connected so that CRC information stored in the register of a K_i^{th} of the sub-circuits is shifted to the register of the first sub-circuit, K_i being a constant less than or equal to k.
12. The apparatus of claim 11, wherein K_i is programmable.
13. The apparatus of claim 10, wherein the multiplier multiplies by a factor related to a root of an ECC polynomial.
14. The apparatus of claim 10, wherein the output port of the adder of one of a comparison one of the sub-circuits is connected to a CRC comparator for comparing a value inputted to the input terminal of the adder of the comparison sub-circuit to CRC information stored in the register of the comparison sub-circuit.
15. The apparatus of claim 14, wherein the CRC comparator comprises an XOR gate.
16. A cyclical redundancy check (CRC) generator which generates CRC information for error checking purposes, comprising:
- means for segmenting an input stream of data into a plurality of sub-streams;
 - means for forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information.
17. The apparatus of claim 16, wherein the segmenting means segments the input stream into three sub-streams.



REPLACEMENT SHEET

Date :

-30-

18. The apparatus of claim 16, wherein the segmenting means multiplies at least one of the sub-streams by a constant.

19. The apparatus of claim 18, wherein the constant is chosen so that a linear combination of certain bytes in the sub-stream is non-zero.

20. The apparatus of claim 19, wherein the constant is a power of a field element α .

21. The apparatus of claim 20, wherein there are three sub-streams, each sub-stream constituting a byte of data, and wherein one sub-stream is multiplied by a constant M_1 and another sub-stream is multiplied by a constant M_2 , and
15 wherein $M_1 = \alpha^{25}$ and $M_2 = \alpha^{112}$.

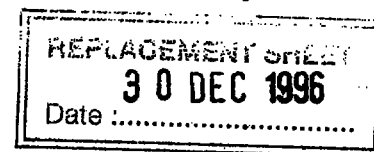
22. The apparatus of claim 16, wherein each sub-stream forms at least part of a data polynomial, and means for forming a linear combination of the plurality of sub-streams and for operating upon the linear combination in order to
5 generate the CRC information comprises k number of dividers for generating k bytes of CRC information with respect to the linear combination of sub-streams.

23. The apparatus of claim 22, wherein the means for forming a linear combination of the plurality of sub-streams and for operating upon the linear combination in order to generate the CRC information actually outputs K_1 number of
5 bytes of CRC information, K_1 being a constant less than or equal to k.

24. The apparatus of claim 23, wherein K_1 is programmable.



* C L M S *



-31-

25. The apparatus of claim 22, wherein each divider divides the data polynomial by a divisor which is related to a root of an ECC polynomial.

26. A cyclical redundancy check (CRC) method which generates CRC information for error checking purposes, the method comprising:

5 segmenting an input stream of data into a plurality of sub-streams; and,
forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information.

27. The method of claim 26, wherein the input stream into three sub-streams.

28. The method of claim 26, further comprising multiplying at least one of the sub-streams by a constant.

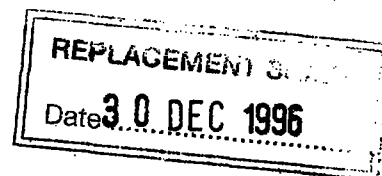
29. The method of claim 28, wherein the constant is chosen so that all linear combinations of the sub-streams are non-zero.

30. The method of claim 29, wherein the constant is a power of a field element α .

31. The method of claim 30, wherein there are three sub-streams, each sub-stream constituting a byte of data, and wherein one sub-stream is multiplied by a constant M_1 and another sub-stream is multiplied by a constant M_2 , and
5 wherein $M_1 = \alpha^{25}$ and $M_2 = \alpha^{112}$.



* C L M S *



-32-

32. The method of claim 26, wherein the steps of forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information comprises applying the plurality of sub-streams to k number of sub-circuits for generating k bytes of CRC information with respect to the linear combination of sub-streams, the sub-circuits being numbered from a first sub-circuit to a k^{th} sub-circuit
- 5
33. The method of claim 32, wherein for sub-circuit j, the linear combination applied thereto is divided by a factor related to a root of an ECC polynomial.
- 10
34. The method of claim 32, further comprising storing CRC information in a register of each sub-circuit and shifting CRC information stored in the register of the k^{th} sub-circuit to the register of the first sub-circuit.
35. The method of claim 32, further comprising comparing a CRC value inputted to a comparison one of the sub-circuits to CRC information stored in the register of the comparison sub-circuit.
36. A cyclical redundancy check (CRC) method which generates CRC information for error checking purposes, the method comprising:
- (a) segmenting an input stream of data into a plurality of sub-streams, the input stream being obtained from a communication channel;
- 5
- (b) forming a linear combination of the plurality of sub-streams and operating upon the linear combination in order to generate the CRC information;
- (c) comparing the generated CRC information with decoded CRC information obtained from the communication channel; and
- 10



-33-

(d) producing an error signal when a discrepancy is detected between the generated CRC information and the decoded CRC information obtained from the communication channel.

37. The method of claim 36, wherein the CRC information generated in step (b) constitutes K_1 number of bytes stored in registers $j=1, \dots, k$, wherein the decoded CRC information constitutes K_1 number of decoded CRC bytes $j=1, \dots, k$ sequentially applied to a comparator, and wherein the comparison step comprises using the comparator to compare the contents of register j with decoded CRC byte j .

38. The method of claim 37, wherein K_1 is a programmable integer.

39. The method of claim 36, further comprising sequentially shifting K_1 number of values stored in registers $j=1, \dots, k$ into a selected one of the registers for comparison with a corresponding decoded CRC byte.

40. The method of claim 39, wherein K_1 is a programmable integer.

41. A cyclical redundancy check (CRC) system comprising:
 a host port connected to a host device;
 a first CRC generator connected to the host port for generating primary CRC information based on input data received from the host device;
 a memory for storing therein input data received from the host device and the primary CRC information generated with respect thereto by the first CRC generator;
 a second CRC generator connected to the memory for generating verification CRC information for checking data retrieved from the memory;



REPLACEMENT SHEET

Date: 30 DEC 1996

-34-

an encoder connected to form encoded information by utilizing the data obtained from the memory including the primary CRC information.

42. The apparatus of claim 41, wherein the second CRC generator compares the primary CRC information and the verification CRC information generated by the second CRC generator to determine errors attributable to the memory.

43. The apparatus of claim 41, wherein the second CRC generator also generates secondary CRC information based on data obtained from the memory; and wherein the encoder is also connected to the second CRC generator and also utilizes the secondary CRC information to form the encoded information.

44. The apparatus of claim 41, further comprising:

a utilization port connected to a utilization channel;

a decoder connected to receive input data at the utilization port and to decode the input data into decoded input data including decoded CRC information, the decoder being connected to apply the decoded input data including the decoded CRC information to the second CRC generator and to the memory, whereby the second CRC generator validates decoded CRC information included in the decoded input data, and

wherein the first CRC generator is connected to receive decoded input data including the decoded CRC information stored in the memory for validating decoded CRC information received from the memory.

45. The apparatus of claim 41, wherein the first CRC generator comprises the cyclical redundancy check (CRC) generator of claim 1.



* C L N S *

REPLACEMENT SHEET

Date 30 DEC 1996

-35-

46. The apparatus of claim 41, wherein the second CRC generator comprises the cyclical redundancy check (CRC) generator of claim 1.

47. A cyclical redundancy check (CRC) method comprising:
using a first CRC generator to generate primary CRC information based on input data received from a host device;

15 storing in a memory the input data received from the host device and the primary CRC information generated with respect thereto by the first CRC generator;

using a second CRC generator connected to the memory for generating verification CRC information with
10 respect to data retrieved from the memory;

forming encoded information by utilizing the data obtained from the memory including the primary CRC information.

48. The method of claim 47, further comprising using the second CRC generator to compare the primary CRC information and verification CRC information generated by the second CRC generator to determine errors attributable to the memory.

49. The method of claim 47, wherein the second CRC generator generates secondary CRC information with respect to data retrieved from the memory.

50. The method of claim 49, further comprising forming the encoded information by also using the secondary CRC information.



-36-

51. The method of claim 47, further comprising:

decoding input data received from a utilization channel into decoded input data including decoded CRC information;

5 applying the decoded input data including the decoded CRC information to the second CRC generator and to the memory;

storing the decoded input data including the decoded CRC information in the memory;

10 using the second CRC generator to validate the decoded CRC information included in the decoded input data;

applying the decoded input data including the decoded CRC information from the memory to the first CRC generator; and

15 using the first CRC generator to validate the decoded CRC information received from the memory.



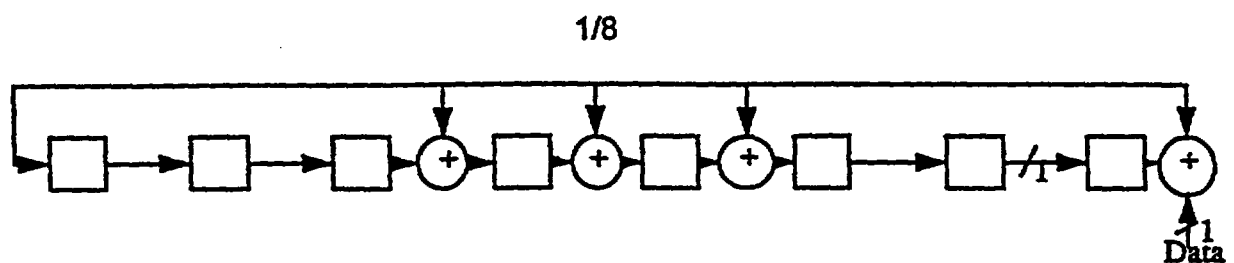
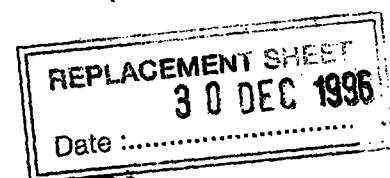


Fig. 1 (Prior Art)

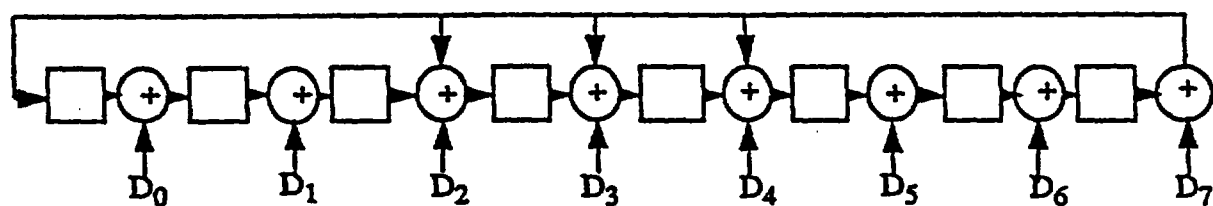


Fig. 2 (Prior Art)

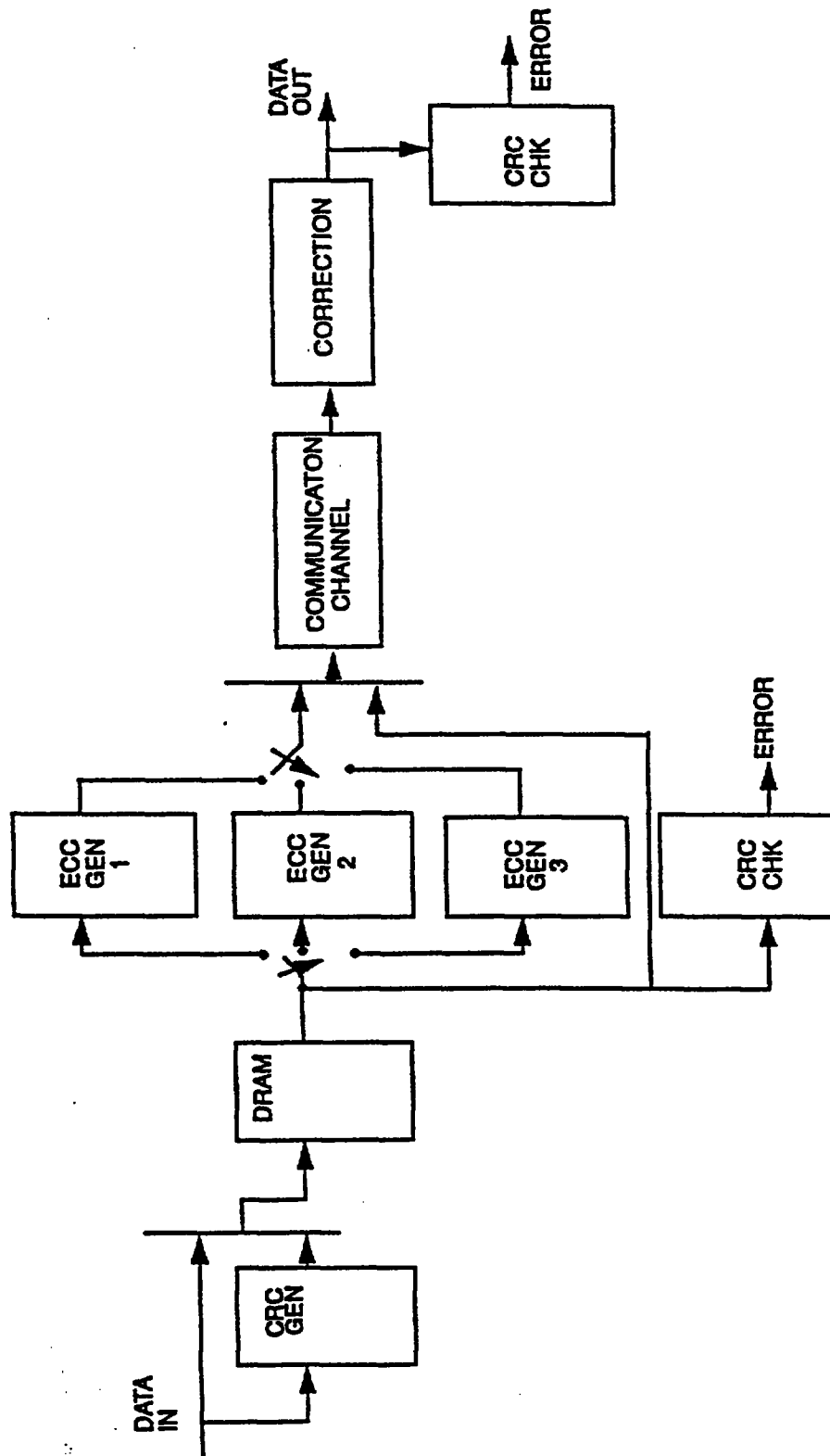
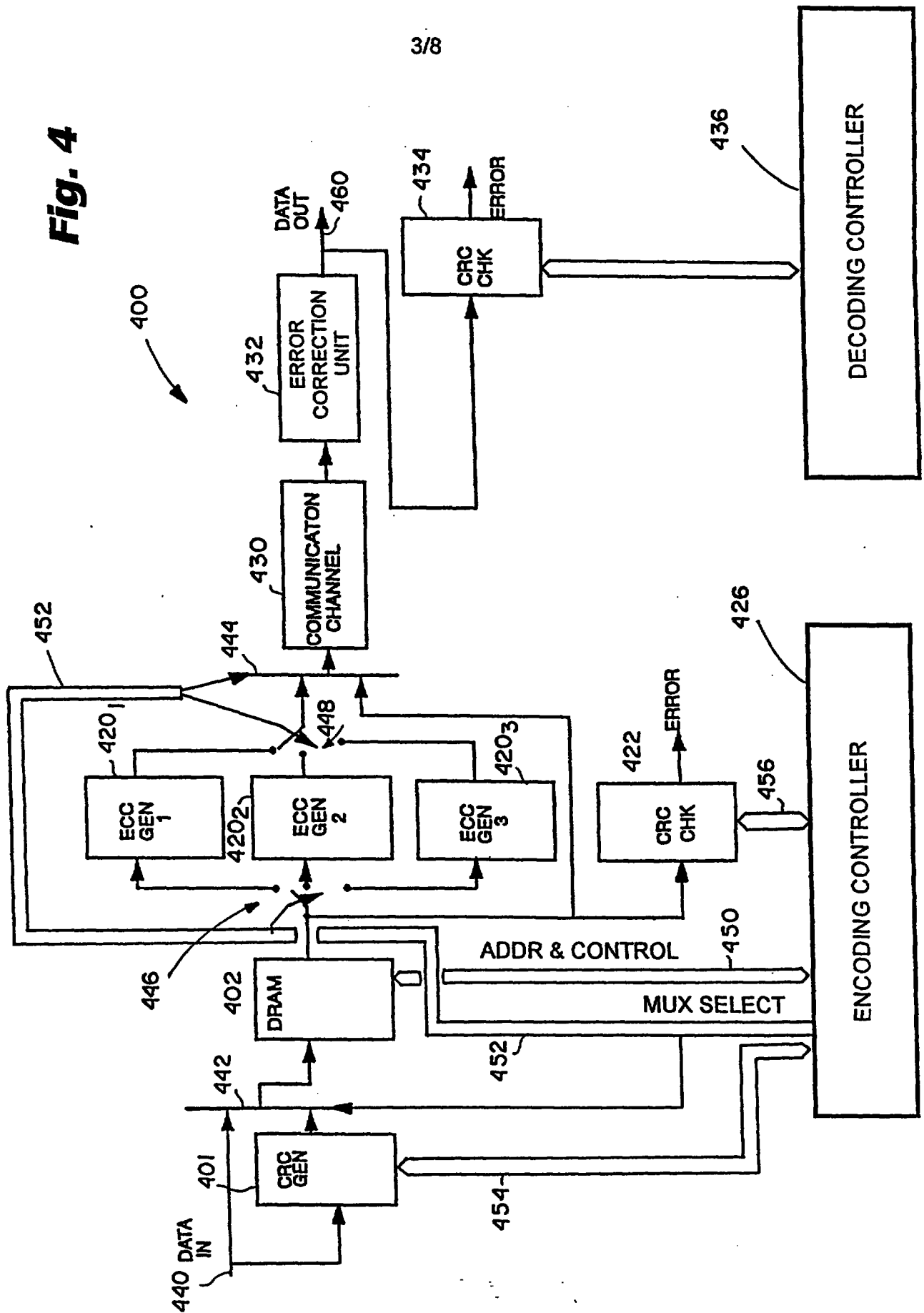
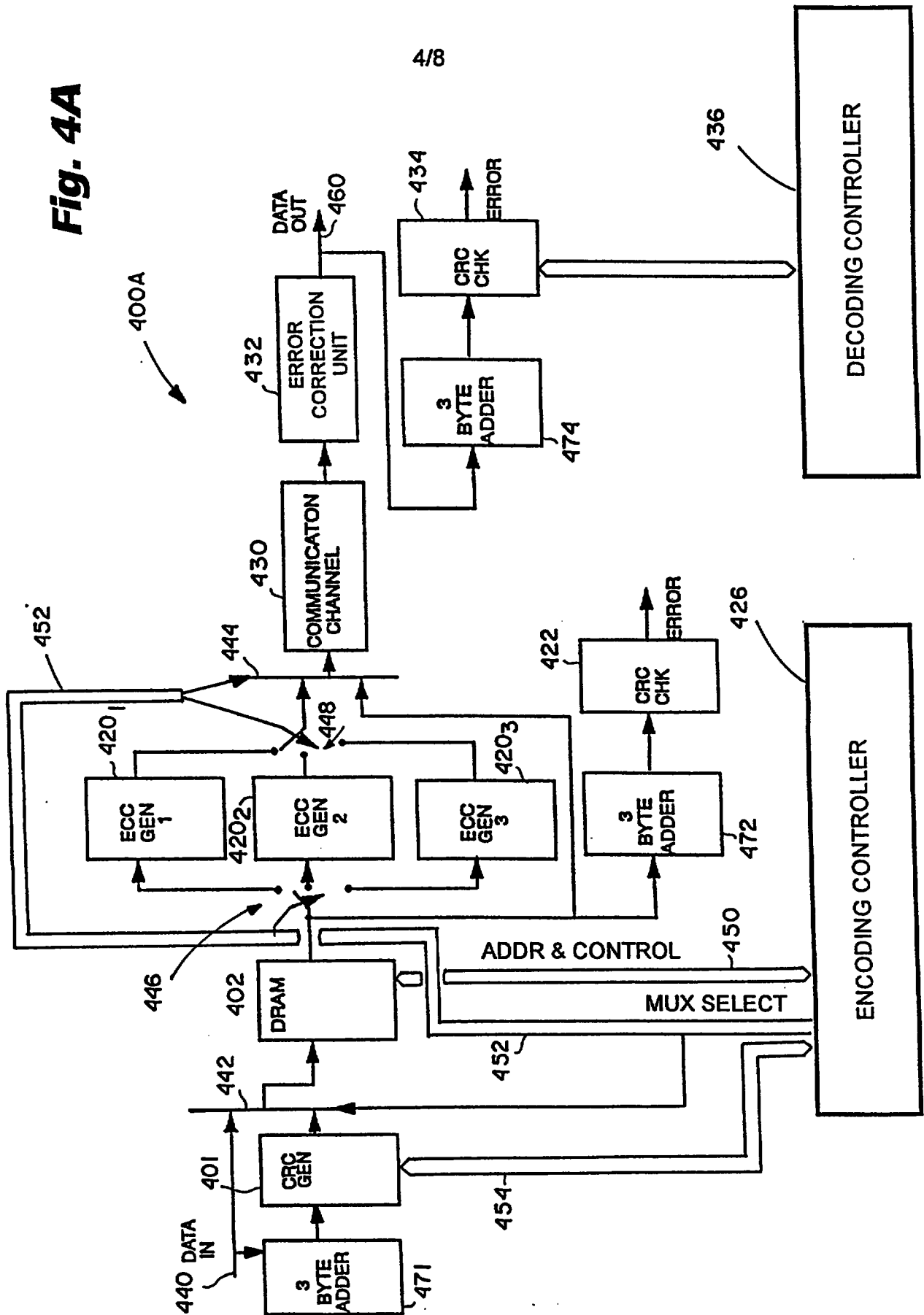


Fig. 3 (Prior Art)



4/8



5/8

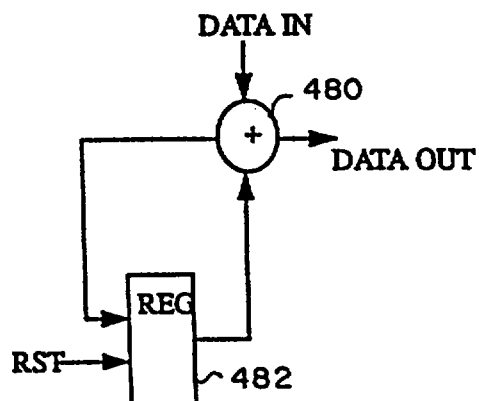


FIG. 5

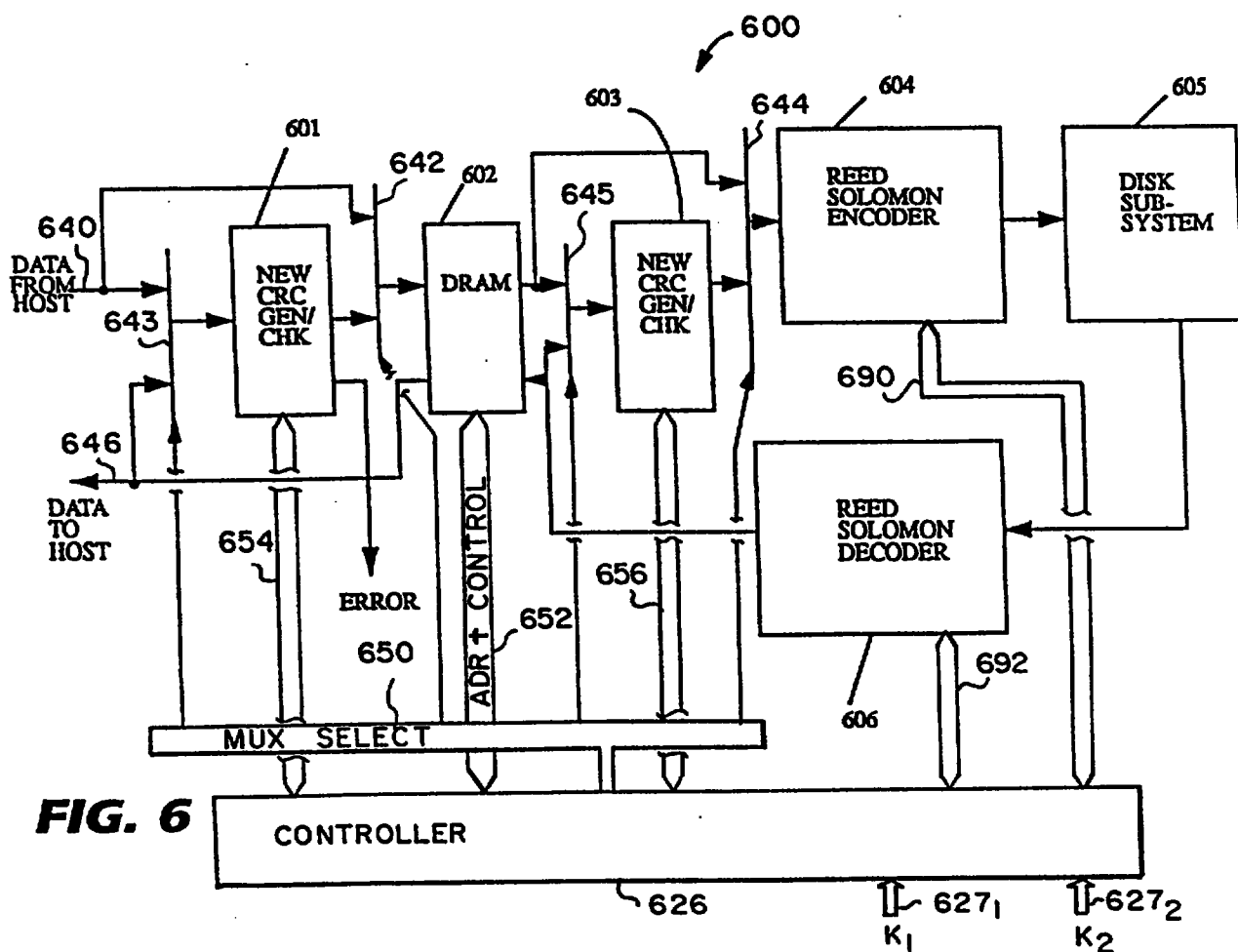
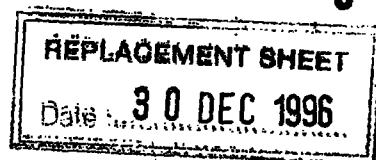
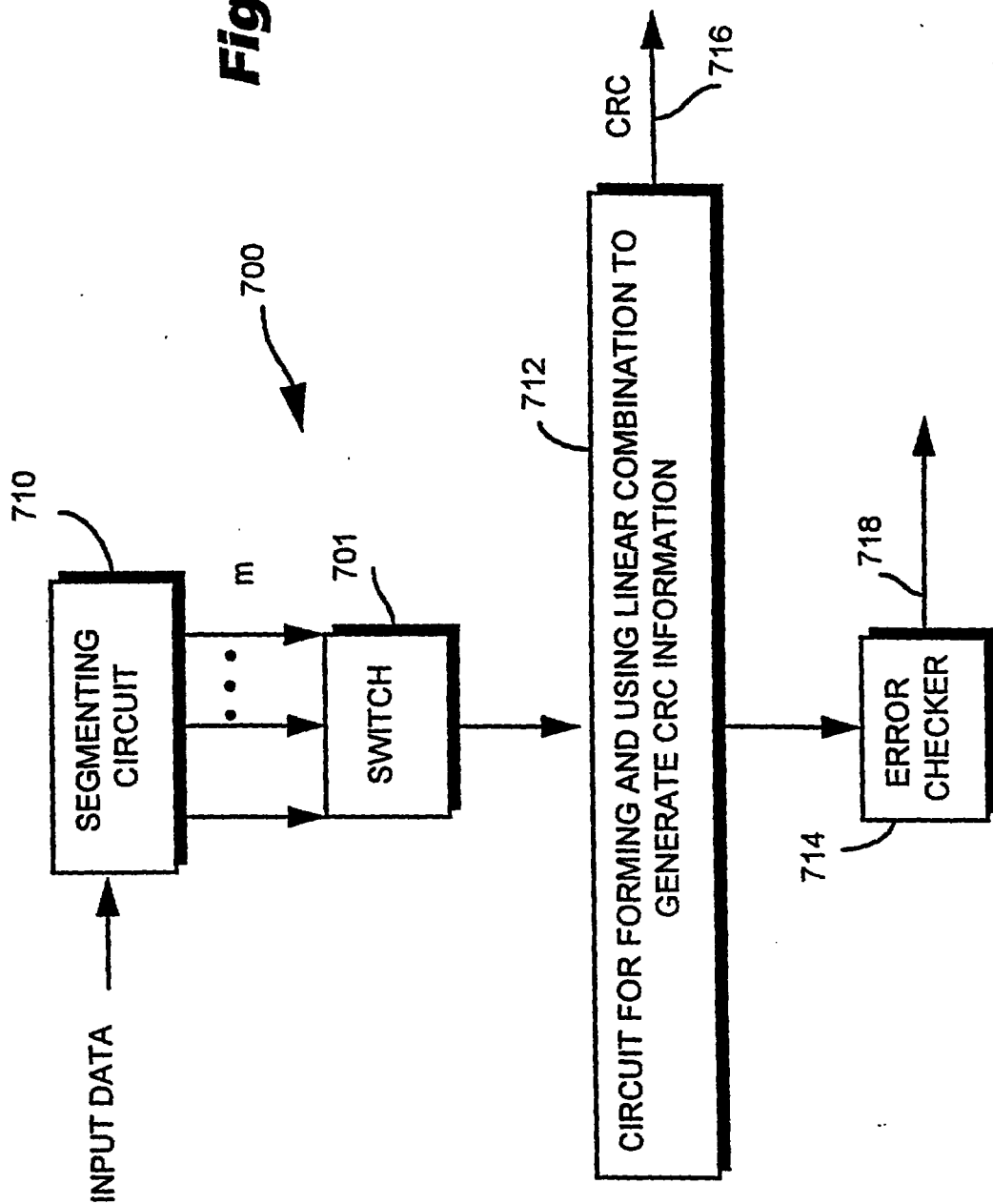


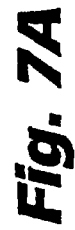
FIG. 6



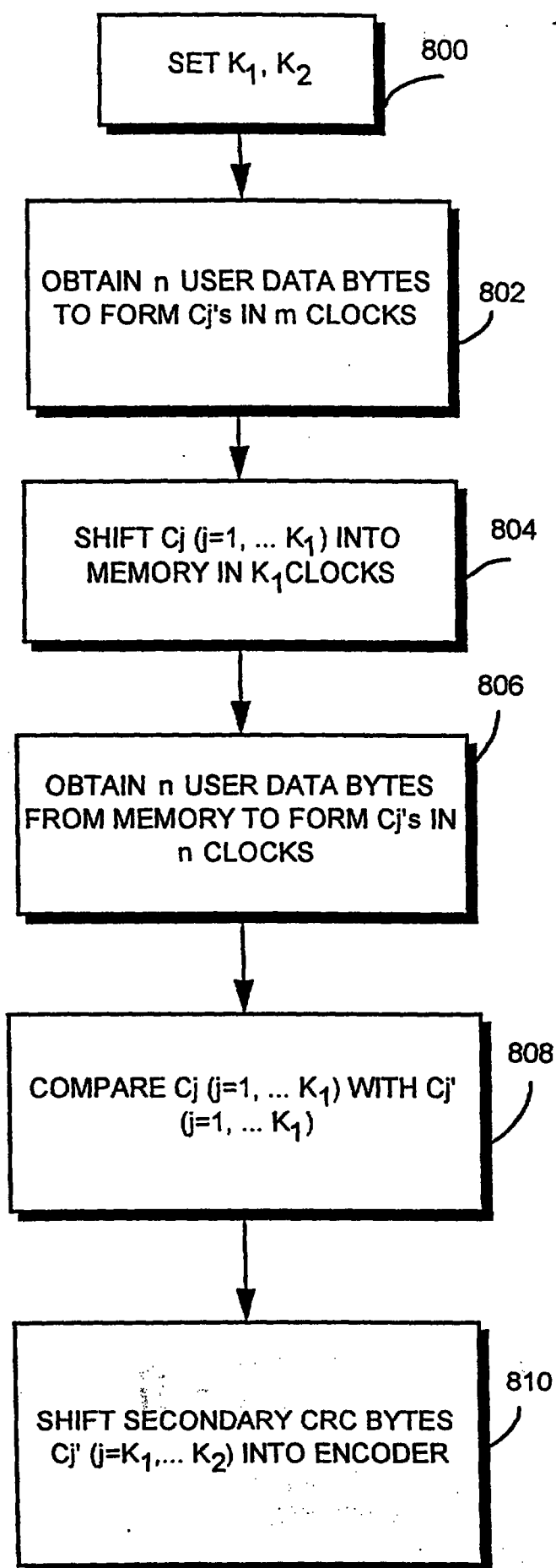
6/8

Fig. 7





8 / 8

Fig. 8

CYCLICAL REDUNDANCY CHECK METHOD AND APPARATUS

ABSTRACT

One-stage and two-stage CRC generation systems (400, 600) feature a CRC generator/checker (700) comprising a segmenter (710) of an input data stream into substreams, a circuit (712) forming a linear combination of the substreams and generating CRC bytes therefrom, and a checker (714) comparing the CRC bytes with previously generated CRC bytes. The two-stage system (600) includes a first CRC generator/checker (601) generating primary CRC bytes, a memory (602) receiving the input data and the primary CRC bytes, and a second CRC generator/checker (603) generating verification CRC bytes for comparison with the primary CRC bytes to check the input data after retrieval from the memory (602) and before input to an encoder (604). The second CRC generator/checker (603) can optionally apply some of the verification CRC bytes to the encoder (604) for use as secondary CRC bytes. The number of CRC bytes outputted by the CRC generator/checkers (601, 603) is programmable.

Figure 6

0-2022036