

(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В СООТВЕТСТВИИ С
ДОГОВОРом О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)(19) ВСЕМИРНАЯ ОРГАНИЗАЦИЯ
ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
Международное бюро(43) Дата международной публикации:
28 ноября 2002 (28.11.2002)

РСТ

(10) Номер международной публикации:
WO 02/095953 A1(51) Международная патентная классификация:
H03M 13/13, 13/35

(21) Номер международной заявки: PCT/RU01/00417

(22) Дата международной подачи:
16 октября 2001 (16.10.2001)

(25) Язык подачи: русский

(26) Язык публикации: русский

(30) Данные о приоритете:
2001113567 22 мая 2001 (22.05.2001) RU

(71) Заявители и

(72) Изобретатели: ПЛОТНИКОВ Андрей Алексеевич [RU/RU]; 188800 Ленинградская обл., Выборг, бульвар Кутузова, д. 16, кв. 45 (RU) [PLOTNIKOV, Andrey Alexejevič, Vyborg (RU)]. АКАЕВ Саид Кахсруевич [RU/RU]; 188800 Ленинградская обл., Выборг, Ленинградское шоссе, д. 1, кв. 43 (RU) [AKAJEV, Said Kakhshuruevich, Vyborg (RU)]. ВЕЛИКОХАТСКИЙ Виктор Фёдорович [RU/RU]; 197101 Санкт-Петербург, ул. Кронверкская, д. 29/37, кв. 43 (RU) [VELIKOKHATSKY, Victor Fyodorovich, St.Petersburg (RU)]. ЛЫСЫЙ Вадим Евгеньевич [RU/RU]; 188800 Ленинградская обл., Выборг, ул. Первомайская, д. 7, кв. 22 (RU) [LYSY, Vadim Yevgenievich, Vyborg (RU)].

(74) Агент: ПЕВЦОВ Дмитрий Александрович; 129110 Москва, ул. Б.Переяславская, д. 5, корп. 1, кв. 28 (RU) [PEVTSOV, Dmitry Alexandrovich, Moscow (RU)].

(81) Указанные государства (национально): AE, AI, AU, BA, BR, CA, CN, CO, CR, CU, CZ, DZ, EE, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LT, LV, MA, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, UA, US, YU, ZA.

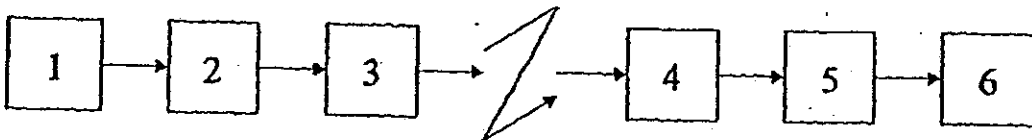
(84) Указанные государства (регионально): евразийский патент (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), европейский патент (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Декларация в соответствии с правилом 4.17:
Об авторстве изобретения (правило 4.17 (iv))
только для US.Опубликована
С отчётом о международном поиске.

В отношении двухбуквенных кодов, кодов языков и других сокращений см. «Пояснения к кодам и сокращениям», публикуемые в начале каждого очередного выпуска Бюллетеня РСТ.

(54) Title: METHOD FOR TRANSMITTING A DIGITAL MESSAGE AND SYSTEM FOR CARRYING OUT SAID METHOD

(54) Название изобретения: СПОСОБ ПЕРЕДАЧИ ДИСКРЕТНОГО СООБЩЕНИЯ И СИСТЕМА ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ



(57) Abstract: The invention relates to telecommunications, in particular to methods and means for transmitting digital messages and can be used for transmitting information through wire channels and telecommunication channels using electromagnetic waves. The use of said channels is simplified by excluding multiplication and division operators from the coding and a decoding process. Said invention makes it possible to transmit any messages from elements of Abelian group including code words whose elements are matrixes, polynomials, numbers of mixed-base notation and nonpositional notation. The inventive encoder comprises a driver clock (7), a function g^2 calculator (8), a pulse generator (9) having recurrent frequency of $f(k+1)/k$, a pulse recurrent frequency doubler (10), a ring counter (11) up to k , an adder-accumulator of elements of Abelian group (12), a key (13), a ring counter (14) up to $(2k+1)$, an AND component (15), a main memory unit (16), a key (17), a trigger (18), a main memory unit (19) and a ring counter (20) up to $(k+1)$. The inventive decoder comprises a driver clock (21), an adder-accumulator of elements of Abelian groupoid (21), a pulse generator (23) having recurrent frequency of $f(k(k+1)/k)$, a pulse recurrent frequency doubler (24), a ring counter (25) up to $(k+1)$, a key (26), a main memory unit (27), a key (28), an AND component (29), a ring counter up to $[2(k+1)+1]$ (30), an identification unit provided with a single element of Abelian group (31), a trigger (32), a main memory unit (33) a key (34), a ring counter (35) up to k .

[Продолжение на след. странице]

METHOD FOR TRANSMITTING DIGITAL MESSAGE AND SYSTEM FOR CARRYING OUT SAID METHOD

A field of technique

This invention relates to telecommunications, in particular to methods and means for transmitting digital messages, and can be used for transmitting information through wire channels and through telecommunication channels using electromagnetic waves.

A prior level of technique

A method for transmitting digital message, consisting of additive Abelian group modulating and its transmitting in a communication channel and demodulating received signal and its decoding [1].

A known system for transmitting digital messages, consisting of additive Abelian group elements, comprises serially connected at a transmitting side an encoder, a modulator and a transmitter and serially connected at a receiving side a receiver, a demodulator and a decoder [1].

Known method and system are rather complicated in a realization because they use four arithmetic operations for processes of encoding and decoding.

Disclosure of invention objects

A technical result, achieved when using proposed method and system, provides simplifying their realization due to excluding multiplication and division operations from processes of encoding and decoding. This provides, in its turn, an opportunity to transmit any messages, consisting of Abelian group elements, in particular encoded words with elements in a form of matrixes, polynomials, numerals in a mixed and non-positional number system, and codes, organized in accordance with proposed rules, correspond to a class of systematic linear block codes.

An above-mentioned technical result may be achieved by producing operations of encoding in accordance with an aspect of the present invention, in a method for transmitting digital message, consisting of additive Abelian group elements, comprising steps of coding message, its modulating and its transmitting to a communication channel, sequentially, and demodulating received signal and its decoding; and differs in producing operation of coding message in accordance with a rule: $Y_n = X_k \otimes G$, where

X_k – a vector-row of an initial message, consisting of k information elements,

Y_n – a vector-row of an encoded message, consisting of k information and one check elements,

G – a generating matrix of operations which consists of k rows and n columns, produced with a help of a $k \times k$ matrix, with operations g^0 at a diagonal and operations g^1 at other positions, and with a help of an additional $k \times m$ matrix, which is added to a $k \times k$ matrix from the right and non-repeated rows of which are sequences of operations g^1 and g^0 or operations g^1 and g^2 , chosen from any possible sequences, including not more than $(m-2)$ operations g^1 , or a matrix, determined with a help of an above-mentioned generating matrix of operations by rearranging rows and/or columns,

$\otimes$ – an operation of generalized matrix multiplication in accordance with the following rule: $y_j = \bigoplus g_{ij}^v(x_i)$ for $j \leq k$, $y_j = g^2[\bigoplus g_{ij}^v(x_i)]$ for $j = k+1$, if an additional column corresponds to a

sequence of operations g^0 , or in accordance with the following rule: $y_j = \bigoplus g^v_{ij}(x_i)$, if an additional column corresponds to a sequence of operations g^2 , where

y_j – a j -th element of a vector-row for an encoded message,

$$\bigoplus g^v_{ij}(x_i) = g^v_{1j}(x_1) \oplus g^v_{2j}(x_2) \oplus \dots \oplus g^v_{kj}(x_k),$$

$\oplus$ – an operation for summing elements in an Abelian group,

$g^v_{ij}(x_i)$ – an operation g^v for an element x_i in accordance with a rule for a ij -th matrix element,

$$v = [0, 2], i = [1, k], j = [1, k+1],$$

$$g^0 = x_i \oplus e, g^1 = x_i \oplus (-x_i), g^2 = x_i \oplus (-x_i) \oplus (-x_i),$$

e – a unity element of an Abelian group,

and producing operations of decoding message Y'_n by excluding, from a vector-row Y'_n , element, corresponding by its number to an additional column of a generating matrix of operations G , provided $H \otimes Y'^T_n = e$, where

Y'^T_n – a transposed vector-row Y'_n ,

H – a $1 \times (k+1)$ check matrix of operations, produced by an additional column transposition, adding operation g^0 to this column from the right, if an additional column corresponds to a sequence of operations g^0 , and rearranging columns, identically to rearranging columns of an generating matrix of operations, or in the same way with changing operations g^2 for operations g^0 , if an additional column corresponds to a sequence of operations g^2 .

An above-mentioned technical result may be achieved, also, by providing correspondence, in a situation when message elements belong to a ring with a unity, of an operation g^0 to an operation of a multiplication into a unity, of an operation g^1 to an operation of a multiplication into a zero and of an operation g^2 to an operation of a multiplication to a minus unity.

An above-mentioned technical result may be achieved, also, by providing a correspondence, in a situation when message elements belong to a residue class ring to the modulo q , where q is a natural number, of an operation $\oplus$ to an operation of summing to the modulo q .

An above-mentioned technical result may be achieved, also, by using in accordance with another aspect of the present invention, in a system for transmitting digital message, consisting of additive Abelian group elements, comprising serially connected at a transmitting side an encoder with an input corresponding to a system input, a modulator and a transmitter and serially connected at a receiving side, a demodulator and a decoder with an output forming a system output for a non-correctable message, and differs in producing encoder in a form, permitting to realize the following algorithm $Y_n = X_k \otimes G$, where

X_k – a vector-row of an initial message, consisting of k information elements,

Y_n – a vector-row of an encoded message, consisting of k information and one check elements,

G – a generating matrix of operations which consists of k rows and n columns, produced with a help of a $k \times k$ matrix, with operations g^0 at a diagonal and operations g^1 at other positions, and with a help of an additional $k \times m$ matrix, which is added to a $k \times k$ matrix from the right and non-repeated rows of which are sequences of operations g^1 and g^0 or operations g^1 and g^2 , chosen from any possible sequences, including not more than $(m-2)$ operations g^1 , or a matrix, determined with a help of an above-mentioned generating matrix of operations by rearranging rows and/or columns,

$\otimes$ – an operation of generalized matrix multiplication in accordance with the following rule: $y_j = \bigoplus g^v_{ij}(x_i)$ for $j \leq k$, $y_j = g^2[\bigoplus g^v_{ij}(x_i)]$ for $j = k+1$, if an additional column corresponds to a sequence of operations g^0 , or in accordance with the following rule: $y_j = \bigoplus g^v_{ij}(x_i)$, if an additional column corresponds to a sequence of operations g^2 , where

y_j – a j -th element of a vector-row for an encoded message,

$$\bigoplus g^v_{ij}(x_i) = g^v_{1j}(x_1) \oplus g^v_{2j}(x_2) \oplus \dots \oplus g^v_{kj}(x_k),$$

$\otimes$ – an operation for summing elements in an Abelian group,

$g_{ij}^v(x_i)$ – an operation g^v for an element x_i in accordance with a rule for a ij -th matrix element,

$$v = [0, 2], i = [1, k], j = [1, k+1],$$

$$g^0 = x_i \oplus e, g^1 = x_i \oplus (-x_i), g^2 = x_i \oplus (-x_i) \oplus (-x_i),$$

e – a unity element of an Abelian group,

and by using a decoder in a form, permitting to exclude, from a vector-row Y'_n , element, corresponding, by its number, to an additional column of an generating matrix of operations provided $H \otimes Y_n'^T = e$, where

$Y_n'^T$ – a transposed vector-row Y'_n ,

H – a $1 \times (k+1)$ check matrix of operations, produced by an additional column transposition, adding operation g^0 to this column from the right, if an additional column contains operations g^0 , and rearranging columns, identically to rearranging columns of an generating matrix of operations, or in the same way with changing operations g^2 for operations g^0 , if an additional column corresponds to a sequence of operations g^2 .

An above-mentioned technical result may be achieved, also, by providing encoder with the first operative memory unit with k outputs connected to corresponding first k information inputs of the second operative memory unit, an output of which forms an encoder output, serially connected the calculation unit for calculating function g^2 , the first adder, used for summing Abelian group elements, with an input connected to its second input, the first switch with an output connected to a $(k+1)$ -th information input of the second operative memory unit, serially connected the first pulse shape forming unit and the first ring counter, used for counting up to k , with an overflow output connected to a control input of the first switch and a reset input of the first operative memory unit, serially connected the pulse generator with a repetition frequency of $f(k+1)/k$, the second switch and the first ring counter, used for counting up to $(k+1)$, with an information output connected to an address input of the second operative memory unit, the first gate AND with an output connected to a control input of the second switch, the first flip-flop with an output connected to a direct input of the first gate AND, an inverting input of which is connected with an overflow output of the first ring counter, used for counting up to $(k+1)$, and to a reset input of the first flip-flop, serially connected the first pulse repetition frequency doubling unit with an input connected to an output of the pulse generator with a repetition frequency of $f(k+1)/k$, and the ring counter, used for counting up to $(2k+1)$, with an overflow output connected to a counting input of the first flip-flop, combined information inputs of the first operative memory unit and the calculation unit, used for calculating function g^2 , a start input of the pulse shape forming unit and a synchronization input of the pulse generator with a repetition frequency of $f(k+1)/k$ form an encoder input and f corresponds to a repetition frequency for a digital message elements.

An above-mentioned technical result may be achieved, also, by providing a decoder with the third operative memory unit with $(k+1)$ outputs connected to corresponding first $(k+1)$ information inputs of the fourth operative memory unit, an output of which forms a decoder output, serially connected the second adder, used for summing Abelian group elements, with an output connected to its second input, the third switch, the identification unit, used for identifying correspondence to a unity element of an Abelian group, and the fourth switch with an output connected to an address input of the fourth operative memory unit, serially connected the second pulse shape forming unit and the second ring counter, used for counting up to $(k+1)$, with an overflow output connected to a control input of the third switch and to a reset input of the third operative memory unit, serially connected the pulse generator with a repetition frequency of $f(k+1)/k$, the fifth switch and the second ring counter, used for counting up to k , with an information output connected to an information input of the fourth switch, the second gate AND with an output connected to a control input of the fifth switch, the second flip-flop with an output connected to a direct input of the second gate AND, an inverting input of which is connected to an overflow output of the second ring counter, used for counting up to k , and to a reset input of

the second flip-flop, serially connected the second pulse repetition frequency doubling unit with an input connected to an output of the pulse generator with a repetition frequency of $f_k/(k+1)$, and the ring counter, used for counting up to $[2(k+1)+1]$, with an overflow output connected to a counting input of the second flip-flop, combined information inputs of the third operative memory unit and the second adder, used for summing Abelian group elements, a start input of the second pulse shape forming unit and a synchronization input of the pulse generator with a repetition frequency of $f_k/(k+1)$ form a decoder input and f corresponds to a repetition frequency for elements of a code word in a digital message.

Short description of annexed figures

Fig. 1 illustrates an example of individual message coding and decoding, fig. 2 illustrates an electrical block scheme of a system for transmitting digital message, fig. 3 illustrates an electrical block scheme of an encoder, fig. 4 illustrates an electrical block scheme of a decoder.

A system for transmitting digital message consists of an encoder 1, a modulator 2, a transmitter 3, a receiver 4, a demodulator 5 and a decoder 6.

An encoder 1 consists of the first pulse shape forming unit 7, the calculation unit 8, used for calculating function g^2 , the pulse generator 9 with a repetition frequency of $f(k+1)/k$, the first pulse repetition frequency doubling unit 10, the first ring counter 11, used for counting up to k , the first accumulating adder 12, used for accumulating elements of an Abelian group, the second switch 13, the ring counter 14, used for counting up to $(2k+1)$, the first gate AND 15, the first operative memory unit 16, the first switch 17, the first flip-flop 18, the second operative memory unit 19 and the first ring counter 20, used for counting up to $(k+1)$.

A decoder 6 consists of the second pulse shape forming unit 21, the second accumulating adder 22, used for accumulating elements of an Abelian group, the pulse generator 23 with a repetition frequency of $f_k/(k+1)$, the second pulse repetition frequency doubling unit 24, the second ring counter 25, used for counting up to $(k+1)$, the fifth switch 26, the third operative memory unit 27, the third switch 28, the second gate AND 29, the ring counter 30, used for counting up to $[2(k+1)+1]$, the identification unit 31, used for identifying correspondence to a unity element of an Abelian group, the second flip-flop 32, the fourth operative memory unit 33, the fourth switch 34, the second ring counter 35, used for counting up to k .

Description of a present invention preferable embodiment

A method for transmitting digital message is realized as the following.

An generating matrix of operations G with k rows and $(k+1)$ columns is formed, said matrix is produced with a help of a $k \times k$ matrix with operations g^0 at its diagonal and operations g^1 at other positions and with a help of an additional column, which is added from the right to said $k \times k$ matrix and corresponds to a sequence of operations g^0 or operations g^2 , situated at every position. It's possible, also, to use an generating matrix of operations, produced with a help of said generating matrix of operations by rearranging its rows and/or columns. The resulting generating matrix of operations is a matrix, formed not of numbers, as usual matrixes, but of records, recommending to produce a corresponding operation in situations, when a corresponding element of a generating matrix of operations is initiated.

An operation of adding additional column is produced with a purpose to introduce, into a transmitted message, check elements which are used for finding out errors in a received message, if they appear in a process of a message transmission through a communication channel.

A digital message X_k , generated with a corresponding source, is encoded by producing generalized matrix multiplication of a vector-row X_k into an above-mentioned generating matrix of operations G .

A procedure of a generalized matrix multiplication operation is quite the same with a procedure of a usual matrix multiplication because it's produced in the same way, as the following: paired interaction operations are produced for a i -th element of a vector-row X_k and every ij -th element (which is situated at a crossing of a i -th row and a j -th column) of an operation matrix G and then results of i -th operations are summed with forming a j -th element of a vector-row Y_n . As a result, every above-mentioned operation, which is required for producing generalized matrix multiplication operation, can be interpreted as a summing operation in accordance with rules, formulated for elements of an Abelian group [2, p. 140], which contains elements of a digital message X_k (with k information elements), formed with a corresponding source. Operations g^v (g^0 , g^1 and g^2) correspond to summing operations with a unity element of a group [2, p. 139], to summing operations with an inverse element of a group [2, p. 140] and to two-fold summing operations with an inverse element of a group, correspondingly.

An encoded message is modulated and transmitted to a communication channel.

A received message is demodulated and decoded. Decoding is produced using operations of a generalized matrix multiplication of a check matrix H into a transposed vector-row Y_n^T .

A $1 \times n$ check matrix of operations H is formed by transposing additional matrix, by adding operation g^0 to this matrix from the right, if an additional column corresponds to a sequence of operations g^0 , or in the same way with changing operations g^2 for g^0 , if an additional column corresponds to a sequence of operations g^2 , and by rearranging columns (if an generating matrix of operations formation was done by rearranging columns) in the same way with rearranging columns for an generating matrix of operations.

If a value, got as a result of a multiplication, equals a unity element of a group (this fact informs about an error absence in a received message), an element with number, corresponding to a number of an additional column in an generating matrix of operations G , is excluded from a vector-row Y_n ; so, a check element, inserted into a message during a process of encoding, is discarded.

If message elements belong to a ring with a unity, which corresponds to one of the variants for an additive Abelian group, operations g^0 degenerate into operations with a multiplication into a unity, operations g^1 degenerate into operations with a multiplication into a zero and operations g^2 degenerate into operations with a multiplication into a minus unity.

If message elements belong to a residue class ring on the modulo q , which corresponds to one of the variants for a ring with a unity, an operation $\oplus \Sigma$ is transformed into an operation of summing on the modulo q .

Fig. 1 illustrates an example of transmitting message X_k , consisting of seven binary elements. An generating matrix of operations G is formed in accordance with the above-mentioned rule. In this case an additional column is inserted in the first position. After producing generalized matrix multiplication of a vector-row X_k into a matrix G an encoded message vector-row Y_n with a check element in the first position is formed.

A demodulated message Y_n is received without errors. So, producing generalized matrix Y_n^T element of a group. Than decoding is done by discarding check element, in particular by extracting elements of an initial message.

A system for transmitting digital message is operated in the following way.

Every element of a digital message X_k , formed with a corresponding source and consisting of consequently transmitted code words with a size of k elements each, gets at an input of an encoder 1 and further at information inputs of the first operative memory unit 16 and the calculation unit 8. At the same time this element starts the first pulse shape forming unit 7 and synchronizes the pulse generator 9. A pulse from an output of the first pulse shape forming unit 7 starts the first ring counter 11. The first counter 11 provides counting for pulses, coming at its input, and elements of a code word are stored in corresponding cells of the first operative memory unit 16 and are conversed with the calculation unit 8 in accordance with a rule g^2 . Results of a conversion, produced for message elements, are transferred to an input of a first

accumulating adder 12, where every next conversed element is summarized with a sum of previous elements in accordance with a rule for summing elements of an Abelian group, and forming a check element for its inserting into a transmitted code word. After transferring a k -th element of a code word to an input of the first ring counter 11 a pulse is formed at its overflow output and this pulse opens the first switch 17, resets the first operative memory unit 16 and transfers an information from outputs of the first operative memory unit 16 to first k memory cells of the second operative memory unit 19. At the same time this pulse transfers an information from outputs of the first adder 12 to a $(k+1)$ -th memory cell of the second operative memory unit 19. Pulses from an output of the generator 9 with a repetition frequency value, exceeding $(k+1)/k$ times a repetition frequency value for elements in a code word, get at an information input of the second switch 13, which, being kept initially in a closed state, doesn't transfer them to an input of the first ring counter 20. The same pulses are transferred to an input of the first frequency doubling unit 10, which doubles a repetition frequency for coming pulses. Then pulses are transferred from an output of the unit 10 to an input of the ring counter 14. When a $(2k+1)$ -th pulse is transferred (approximately in a middle of a time interval between a moment, when the last element of a current code word comes to an input of an encoder 1, and a moment, when the first element of a next code word comes to this input) to an input of the ring counter 14, a pulse is formed at an overflow output of the counter 14 and is transferred to a counting input of the first flip-flop 18, changing a state of this flip-flop. A voltage signal of a "logical unity", formed at an output of the first flip-flop 18, is transferred to a direct input of the first gate AND 15. The first ring counter 20 hasn't begun to count, yet, and a voltage signal of a "logical zero" is kept at its overflow output; so, a voltage signal of a "logical unity" appears at an output of the first gate AND 15 and this signal helps to open the second switch 13. Pulses from an output of the generator 9 begins to come to an input of the first ring counter 20; as a result, a code appears at an information output of the counter 20 and this code is changed with every next counted pulse. This code, after getting at an address input of the second operative memory unit 19, initializes an information reset in its corresponding memory cell, using the same sequential number with a pulse, counted with the first ring counter 20, and k information and one check elements of a code word are transferred sequentially to an input of a modulator 2. After transferring a n -th pulse to an input of the first ring counter 20 a voltage signal of a "logical unity" is formed at its overflow output and this voltage signal changes a state of the first flip 18; so, a voltage signal of a "logical zero" appears at an output of the first gate AND 15 and this voltage signal closes the first switch 13 and stops getting pulses from an output of the generator 9 to an input of the second ring counter 20, which gets prepared for a next operation cycle.

A modulated message is transferred from an output of a modulator 2 to an input of a transmitter 3 and further to a communication channel.

A received message, after being transferred through a receiver 4, gets demodulated in a demodulator 5 and is transferred to an input of a decoder 6.

Every element in a received code word gets, after being transferred to an input of a decoder 6, at information inputs of the third operative memory unit 27 and the calculation unit 22, starts the second pulse shape forming unit 21 and synchronizes the generator 23. A pulse from an output of the second pulse shape forming unit 21 starts the second ring counter 25. When the second ring counter 25 counts pulses, coming to its input, elements of a code word are stored in corresponding cells of the third operative memory unit 27 and the second accumulating adder 22 determines a result of summing elements of a code word, received at its input, in accordance with a rule of summing elements of an Abelian group. After transferring a $(k+1)$ -th element of a code word to an input of the second ring counter 25 a pulse is formed at its overflow output and this pulse opens the third switch 28, resets the third operative memory unit 27 and transfers an information from its outputs to memory cells of the fourth operative memory unit 33 and from outputs of the second accumulating unit 22 to the identification unit 31, correspondingly. When a sum, getting at an input of the identification unit 31, equals a unity

element of an Abelian group, a voltage signal of a "logical unity" is transferred to a control input of the fourth switch 34 and this switch gets opened. Pulses from an output of the generator 23 with a repetition frequency, value of which is exceeded $k/(k+1)$ times with a value of a repetition frequency for elements in a code word, get to an information input of the fifth switch 26, which, being kept initially in a closed state, doesn't transfer these pulses to an input of the second ring counter 35. The same pulses are transferred to an input of the second frequency doubling unit 24, which doubles a repetition frequency for coming pulses; pulses from an output of the unit 24 are transferred to an input of the second ring counter 30. When a $[2(k+1)+1]$ -th pulse gets (approximately in a middle of a time interval between a moment, when the last element of a current code word comes to an input of a decoder 6, and a moment, when the first element of a next code word comes to this input) at an input of the ring counter 30, a pulse from an overflow output of the counter 30 is transferred to a counting input of the second flip-flop 32 and changes a state of this flip-flop. A voltage signal of a "logical unity" appears at an output of the second flip-flop 32 and this voltage signal is transferred to a direct input of the second gate AND 29. The second ring counter 35 hasn't begun to count, yet, and a voltage signal of a "logical zero" is kept at its overflow output; so, a voltage signal of a "logical unity" appears at an output of the second gate AND 29 and opens the fifth switch 26. Pulses from an output of the generator 23 begins to come to an input of the second ring counter 35; as a result, a code appears at an information input of this counter and this code is changed with every next counted pulse. This code is transferred through the just opened fourth switch 38 and, after getting at address input of the fourth operative memory unit 33, initializes an information reset it its cell with a sequential number, corresponding to a number of a pulse, counted with the second ring counter 35, and k information elements of a code word are transferred sequentially to a decoder output, in particular to a user. A check element is kept, as discarded, in a $(k+1)$ -th memory cell of the fourth operative memory unit 33 and is changed in this cell with a check element of a next code word. After transferring a k -th pulse to an input of the second ring counter 35 a voltage signal of a "logical unity" appears at its overflow output and this voltage signal changes a state of the first flip-flop 32; then a voltage signal of a "logical zero" is formed at an output of the second gate AND 29 and this voltage signal closes the fifth switch 26 and stops getting pulses from an output of the generator 23 to an input of the second ring counter 35, which gets prepared for a next operation cycle.

LITERATURE

1. J. Clark, J. Cane. Coding with an error correction in digital communication systems, translated from English by S. I. Gelfand, Under edition of B. S. Tsybakov, Issue 28, Moscow, Publisher "Radio i svyaz", 1987. p.p. 9-18, fig 1.2.
2. A. I. Kostrikin, Introduction for an algebra, Moscow, Publisher "Nauka", 1977.

Claims

1. A method for transmitting digital message, consisting of additive Abelian group elements, comprises steps of coding message, its modulating and its transmitting to a communication channel, sequentially, demodulating received signal and its decoding **and differs in** producing operation of coding message in accordance with a rule: $Y_n = X_k \otimes G$, where

X_k – a vector-row of an initial message, consisting of k information elements,

Y_n – a vector-row of an encoded message, consisting of k information and one check elements,

G – a generating matrix of operations which consists of k rows and n columns, produced with a help of a $k \times k$ matrix, with operations g^0 at a diagonal and operations g^1 at other positions, and with a help of an additional $k \times m$ matrix, which is added to a $k \times k$ matrix from the right and non-repeated rows of which are sequences of operations g^1 and g^0 or operations g^1 and g^2 , chosen from any possible sequences, including not more than $(m-2)$ operations g^1 , or a matrix, determined with a help of an above-mentioned generating matrix of operations by rearranging rows and/or columns,

$\otimes$ – an operation of generalized matrix multiplication in accordance with the following rule: $y_j = \oplus g_{ij}^v(x_i)$ for $j \leq k$, $y_j = g^2[\oplus g_{ij}^v(x_i)]$ for $j = k+1$, if an additional column corresponds to a sequence of operations g^0 , or in accordance with a rule: $y_j = \oplus g_{ij}^v(x_i)$, if an additional column corresponds to a sequence of operations g^2 , where

y_j – a j -th element of a vector-row for an encoded message,

$\oplus g_{ij}^v(x_i) = g_{1j}^v(x_1) \oplus g_{2j}^v(x_2) \oplus \dots \oplus g_{kj}^v(x_k)$,

$\oplus$ – an operation for summing elements in an Abelian group,

$g_{ij}^v(x_i)$ – an operation g^v for an element x_i in accordance with a rule for a ij -th matrix element,

$v = [0, 2]$, $i = [1, k]$, $j = [1, k+1]$,

$g^0 = x_i \oplus e$, $g^1 = x_i \oplus (-x_i)$, $g^2 = x_i \oplus (-x_i) \oplus (-x_i)$,

e – a unity element of an Abelian group,

and in decoding message Y_n by excluding, from a vector-row Y_n , element, corresponding, by its numbers, to an additional column of an generating matrix of operations G , provided $H \otimes Y_n^T = e$, where

Y_n^T – a transposed vector-row Y_n ,

H – a $1 \times (k+1)$ check matrix of operations, produced by an additional column transposition, adding operation g^0 to this column from the right, if an additional column contains a sequence of operation g^0 , and rearranging columns, identically to rearranging columns of an generating matrix of operations, or in the same way with changing operations g^2 for operations g^0 , if an additional column corresponds to a sequence of operations g^2 .

2. A method for transmitting digital message in accordance with item 1, **which differs in** transforming, when message elements belong to a ring with a unity, an operation g^0 into an operation of a multiplication into a unity, an operation g^1 into an operation of a multiplication into a zero and an operation g^2 into an operation of a multiplication into a minus unity.

3. A method for transmitting digital message in accordance with item 1 or 2, **which differs in** transforming, when message elements belong to a residue class ring to the modulo q , where q is a natural number, an operation $\oplus$ into a summing operation to the modulo q .

4. A system for transmitting digital message, consisting of additive Abelian group elements, comprises serially connected at a transmitting side an encoder with an input forming a system input, a modulator and a transmitter and serially connected at a receiving side a demodulator and a decoder with an output forming a system output for a non-correctable message, and differs in producing encoder in a form, permitting to realize an algorithm: $Y_n = X_k \otimes G$, where

X_k – a vector-row of an initial message, consisting of k information elements,

Y_n – a vector-row of an encoded message, consisting of k information and one check elements,

G – a generating matrix of operations which consists of k rows and n columns, produced with a help of a $k \times k$ matrix, with operations g^0 at a diagonal and operations g^1 at other positions, and with a help of an additional $k \times m$ matrix, which is added to a $k \times k$ matrix from the right and non-repeated rows of which are sequences of operations g^1 and g^0 or operations g^1 and g^2 , chosen from any possible sequences, including not more than $(m-2)$ operations g^1 , or a matrix, determined with a help of an above-mentioned generating matrix of operations by rearranging rows and/or columns,

$\otimes$ – an operation of generalized matrix multiplication in accordance with the following rule: $y_j = \oplus \sum g_{ij}^v(x_i)$ for $j \leq k$, $y_j = g^2[\oplus \sum g_{ij}^v(x_i)]$ for $j = k+1$, if an additional column corresponds to a sequence of operations g^0 , or in accordance with a rule: $y_j = \oplus \sum g_{ij}^v(x_i)$, if an additional column corresponds to a sequence of operations g^2 , where

y_j – a j -th element of a vector-row for an encoded message,

$\oplus \sum g_{ij}^v(x_i) = g_{1j}^v(x_1) \oplus g_{2j}^v(x_2) \oplus \dots \oplus g_{kj}^v(x_k)$,

$\oplus$ – an operation for summing elements in an Abelian group,

$g_{ij}^v(x_i)$ – an operation g^v for an element x_i in accordance with a rule for a ij -th matrix element,

$v = [0, 2]$, $i = [1, k]$, $j = [1, k+1]$,

$g^0 = x_i \oplus e$, $g^1 = x_i \oplus (-x_i)$, $g^2 = x_i \oplus (-x_i) \oplus (-x_i)$,

e – a unity element of an Abelian group,

and in producing decoder in a form, permitting to exclude, from a vector-row Y'_n , element, corresponding, by its number, to an additional column of a generating matrix of operations G , provided $H \otimes Y_n'^T = e$, where

$Y_n'^T$ – a transposed vector-row Y'_n ,

H – a $1 \times (k+1)$ check matrix of operations, produced by an additional column transposition, adding operations g^0 to this column from the right, if an additional column corresponds to a sequence of operations g^0 , and rearranging columns, identically to rearranging columns of an generating matrix of operations, or in the same way with changing operations g^2 for operations g^0 , if an additional column corresponds to a sequence of operations g^2 .

5. A system for transmitting digital message in accordance with item 4, which differs in providing an encoder with the first operative memory unit with k outputs connected to corresponding first k information inputs of the second operative memory unit, an output of which forms an encoder output, serially connected the calculation unit for calculating function g^2 , the first accumulating adder, used for accumulating Abelian group elements, with an input connected to its second input, the first switch with an output connected to a $(k+1)$ -th information input of the second operative memory unit, serially connected the first pulse shape forming unit and the first ring counter, used for counting up to k , with an overflow output connected to a control input of the first switch and a reset input of the first operative memory unit, serially connected the pulse generator with a repetition frequency of $f(k+1)/k$, the second switch and the first ring counter, used for counting up to $(k+1)$, with an information output connected to an address input of the second operative memory unit, the first gate AND with an output connected to a control input of the second switch, the first flip-flop with an output connected to a direct input of the first gate AND, an inverting input of which is connected with an overflow output of the first ring counter, used for counting up to $(k+1)$, and to a reset input of the first flip-flop, serially connected the first pulse repetition frequency doubling unit with an input connected to an output of the pulse generator with a repetition frequency of $f(k+1)/k$, and the ring counter, used for counting up to $(2k+1)$, with an overflow output connected to a counting input of the first flip-flop, combined information inputs of the first operative memory unit and the calculation unit,

used for calculating function g^2 , a start input of the pulse shape forming unit and a synchronization input of the pulse generator with a repetition frequency of $f(k+1)/k$ form an encoder input and f corresponds to a repetition frequency for a digital message elements.

6. A system for transmitting digital message in accordance with item 4 or 6, which differs in providing a decoder with the third operative memory unit with $(k+1)$ outputs connected to corresponding first $(k+1)$ information inputs of the fourth operative memory unit, an output of which forms a decoder output, serially connected the second accumulating adder, used for accumulating Abelian group elements, with an output connected to its second input, the third switch, the identification unit, used for identifying correspondence to a unity element of an Abelian group, and the fourth switch with an output connected to an address input of the fourth operative memory unit, serially connected the second pulse shape forming unit and the second ring counter, used for counting up to $(k+1)$, with an overflow output connected to a control input of the third switch and to a reset input of the third operative memory unit, serially connected the pulse generator with a repetition frequency of $fk/(k+1)$, the fifth switch and the second ring counter, used for counting up to k , with an information output connected to an information input of the fourth switch, the second gate AND with an output connected to a control input of the fifth switch, the second flip-flop with an output connected to a direct input of the second gate AND, an inverting input of which is connected to an overflow output of the second ring counter, used for counting up to k , and to a reset input of the second flip-flop, serially connected the second pulse repetition frequency doubling unit with an input connected to an output of the pulse generator with a repetition frequency of $fk/(k+1)$, and the ring counter, used for counting up to $[2(k+1)+1]$, with an overflow output connected to a counting input of the second flip-flop, combined information inputs of the third operative memory unit and the second accumulating adder, used for accumulating Abelian group elements, a start input of the second pulse shape forming unit and a synchronization input of the pulse generator with a repetition frequency of $fk/(k+1)$ form a decoder input and f corresponds to a repetition frequency for elements of a code word in a digital message.