Control
and Cybernetics
VOL. 1 (1972) No. 1/2

An error-correcting-error-detecting procedure for arbitrary cyclic BCH codes

by

CZESŁAW KOŚCIELNY

Institute of Automatic Control of Power Systems
Wrocław

A decodong procedure for any cyclic Bose-Chaudhuri-Hoquenghem code over arbitrary field GF (q) with $q=p^m$ is described. The method presented requires no calculations over extension field GF (q^M) and utilizes the cyclic property of the code for a combination error-correction-error-detection procedure. Therefore, this method is very simple in principle and can be easily implementated.

1. Introduction

This paper deals with decoding arbitrary cyclic BCH codes. The general solutions of decoding problem of BCH codes, given by Peterson, and subsequently by Gorenstein and Zierler [9, 4] require many arithmetic operations over the extension field GF (q^M). It is generally understood, that the above algorithms, in spite of considerable simplifications [1, 2, 6, 11], can not be reasonably implementated. Therefore, the others interesting methods have been developed [5, 8, 10], and it seems true, that the key to practically acceptable decoding procedure lies in utilization of cyclic property of the code.

It is the purpose of this paper to apply the cyclic properties of BCH codes for a combination error-correction-error-detection scheme. This problem of great practical importance seems to have been largely neglected, while, in the first place the problem of use of BCH codes for independent-error-correction only have been thoroughly and frequently investigated.

2. Notations and preliminaries

The sequence of n elements from GF (q) can be written as n-dimensional vector

$$F=(f_0, f_1, ..., f_{n-1}) \tag{1}$$

which is associated with the polynomial of variable x of degree $n-1$ or less

$$f(x)=\sum_{i=0}^{n-1} f_i\, x^i. \tag{2}$$

Let β be any element of the extension field GF (q^M). If the order of β is n, the cyclic BCH code of length n consists of all vectors F, such that

$$f(\beta^i)=0 \tag{3}$$

for all $i=m_0,\ m_0+1, \ldots, m_0+d-2$, where m_0 and d are arbitrary integers.

The described code is BCH (q, m_0, d) (n, k) cyclic code and it is generated by the polynomial

$$g(x)=\text{L.C.M.}\left\{\prod_{i=m_0}^{m_0+d-2} m_i(x)\right\} \tag{4}$$

where L.C.M. denotes least common multiplier, $m_i(x)$ denotes the minimum function of β^i. If the degree of $g(x)$ is r, then the redundancy of a code is r q-nary digits and the code word of length n consists of $k=n-r$ information digits. The minimum Hamming distance of such a code is at least d. If $d=2t+1$, the code will be capable of correcting t independent errors in the received vector.

Any decoding procedure resolves itself into examining the received vector and calculation of error-vector. Let

$$V=(v_0, v_1, \ldots, v_{n-1}) \tag{5}$$

denote the received vector, which is the sum of the code vector (1) and error-vector

$$E=(e_0, e_1, \ldots, e_{n-1}). \tag{6}$$

The syndrome of the received vector will be an r-dimensional vector

$$S=(s_0, s_1, \ldots, s_{r-1}). \tag{7}$$

With the vectors (5), (6) and (7) are associated received, error and syndrome polynomials respectively

$$v(x)=\sum_{i=0}^{n-1} v_i\, x^i, \tag{8}$$

$$e(x)=\sum_{i=0}^{n-1} e_i\, x^i, \tag{9}$$

$$s(x)=\sum_{i=0}^{r-1} s_i\, x^i. \tag{10}$$

The polynomial (10) is the remainder in the division of (8) by (4). Let

$$R_g\,[a(x)]$$

denote the remainder resulting from dividing $a(x)$ by $g(x)$. Then

$$s(x)=R_g\,[v(x)]. \tag{11}$$

It is clear that by virtue of condition (3) the equation (12) is valid

$$R_g[v(x)] = R_g[f(x)+e(x)] = R_g[e(x)]. \tag{12}$$

Therefore

$$s(x) = R_g[e(x)]. \tag{13}$$

3. The principle of error-vector calculation and implementation of decoding procedure

After the introduction of preliminary definitions, now an essential part of proposed decoding algorithm will be explained. Let us denote

$$v_l(x) = x^l\, v(x) \tag{14}$$

$$s_l(x) = R_g[v_l(x)] = R_g[e_l(x)] \tag{15}$$

$$e_l(x) = x^l\, e(x). \tag{16}$$

Because of cyclic property of the code, which is an ideal in the polynomials' algebra modulo $x^n - 1$, we have

$$v_l(x) = \sum_{i=0}^{l-1} v_{n-l+i}\, x^i + \sum_{i=l}^{n-1} v_{i-l}\, x^i, \tag{17}$$

$$e_l(x) = \sum_{i=0}^{l-1} e_{n-l+i}\, x^i + \sum_{i=l}^{n-1} e_{i-l}\, x^i. \tag{18}$$

The polynomials (17) and (18) are associated with vectors respectively

$$V_l = (v_{n-l}, v_{n-l+1}, \ldots, v_{n-1}, v_0, \ldots, v_{n-l-1}), \tag{19}$$

$$E_l = (e_{n-l}, e_{n-l+1}, \ldots, e_{n-1}, e_0, \ldots, e_{n-l-1}). \tag{20}$$

Vectors (19) and (20) are the original vectors (5) and (6), cyclically shifted l places to the right.

The method, proposed here, is simply to calculate (15) for $l = 0, 1, \ldots, m$, where m is the least integer, so that

$$w(S_m) \leqslant t. \tag{21}$$

In the inequality (21) $w(S_m)$ denotes the Hamming weight of vector S_m. It is evident [6, 9, 11], that when inequality (21) is satisfied, t or less errors are scattered on the first r positions from the left of the vector V_m. Therefore, the syndrome vector S_m agrees with the first r positions from the left of error-vector E_m and the remaining components of error-vector are equal to zero. To obtain error-pattern of original received vector V, one must only cyclically shift the vector E_m m positions to the left or $n-m$ positions to the right

$$e(x) = x^{-m}\, e_m(x) = x^{n-m}\, e_m(x). \tag{22}$$

The implementation of error-correcting-error-detecting procedure results immediately from the principle of error-vector calculation. A mechanization of error-correction depends upon two cases. In the first case, when

$$r \geqslant \frac{n}{2} \tag{23}$$

the described method for finding error-vector may be efective for two independent errors, because every double error-pattern, by means of cyclic shifts, can be reduced to r or less consecutive positions in the code word. Thus, accepting the symbols of elements according to Fig. 1 the general error-vector calculating and error-detecting circuit for arbitrary BCH code with $r \geqslant n/2$ is shown in the block diagram form in Fig. 2. The circuit consists of well known syndrome calculator, connected from the left side with k-stage shift register, of two gates, and of controlled, r-input threshold element. The inputs of threshold element are connected to the outputs

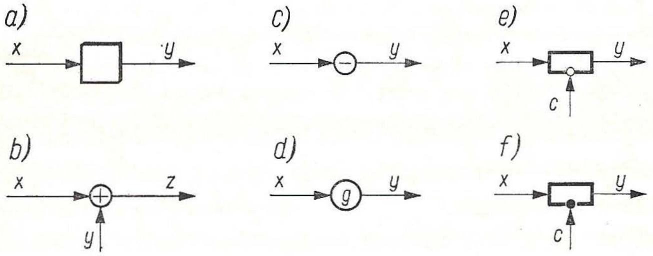

Fig. 1. Symbols of elements used in block-diagrams: (a) single stage of q-nary shift register: after the next clock-period $y=x$; (b) GF (q) adder $z=x+y$ (can be more than two inputs); (c) GF (q) by -1 multiplier $y=-x$; (d) GF (q) by constant g multiplier $y=gx$; (e) controlled gate $y=cx$, c is 0 or 1 from GF (q); (f) controlled gate $y=(1-c)\,x$, c is 0 or 1 from GF (q) Note. x, y, z — elements from GF (q)

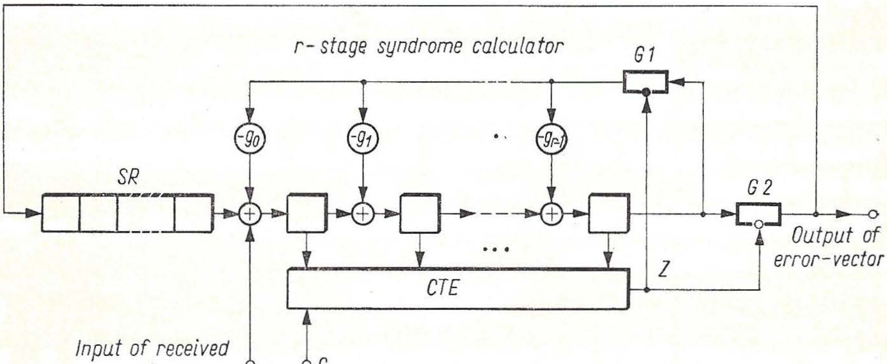

Fig. 2. General error-vector-calculating circuit for arbitrary (n, k) cyclic BCH code with $(n-k) \geqslant (n/2)$ CTE — controlled threshold element; Z — output of CTE; c — control signal for CTE; SR — k-stage shift register, $G1$, $G2$ — gates

Note. Received vector V is introduced to the circuit with v_{n-1}-th component first of r stages of syndrome-calculating shift register. The output of threshold element is

$$Z = cw_i \tag{24}$$

where

$$c \text{ is } 0 \text{ or } 1 \text{ from } GF(q),$$

$$w_i = \begin{cases} 1 & \text{if} \quad w(S_i) \leqslant t. \\ 0 & \text{if} \quad w(S_i) > t \end{cases}$$

The control signal c, during calculating $s(x)$ is equal to zero and it is equal to one just after it, till error-correction has been completed. Therefore, the circuit in Fig. 2 acts in two phases during decoding. The first phase remains n clock-periods and in this time the syndrome $s(x)$ is calculated. Just then $c=0$.

In the second phase $c=1$ and the registers of the circuit are shifted r times with zero input into the syndrome calculator. During this phase, if the number of errors does not exceed t and if the error-pattern is a member of the set of correctable error-patterns, for some least number of clock-periods m $(0 \leqslant m \leqslant r)$, the inequality (21) will be valid, gate 1 will be open and gate 2 closed, and in the next clock-periods, serially connected memory cells act as a usual shift register. This way, after $n+r$ clock-periods of two phases, in the memory of the circuit the error-vector E is stored. The component arrangement of error-vector strictly agrees with the contents of shift registers. Thus, the error-correction procedure is simply to subtract error-vector E from the received vector V, in a paralell or a serial manner.

It should be noted, that if after r clock-periods of the second phase there is no output of threshold element, equal to one, we say, that either an error-pattern of weight at least $t+1$ has been detected, but it can not be corrected, or, when $t \geqslant 3$, an error-pattern of weight at least 3 can not be reduced by means of cyclic shifts to r or less consecutive places.

The second case refers to such BCH codes, for which

$$r < \frac{n}{2}. \tag{25}$$

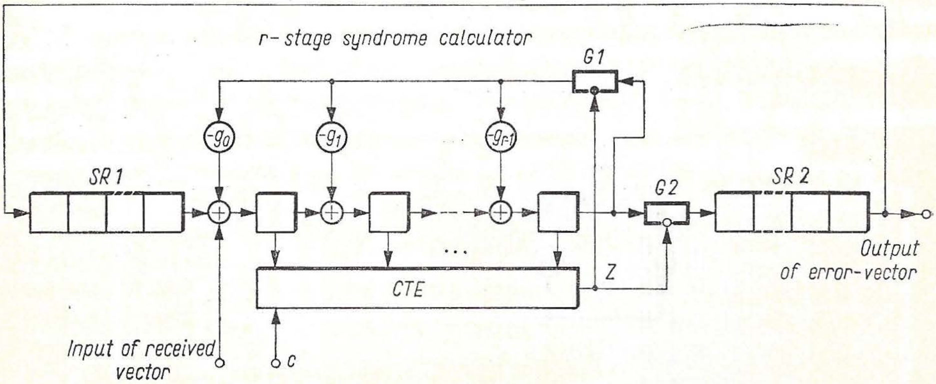

Fig. 3. General error-vector-calculating circuit for arbitrary (n, k) cyclic BCH code with $(n-k) < (n/2)$

$SR1$ — $(n-k)$-stage shift register; $SR2$ — $(2k-n)$-stage shift register

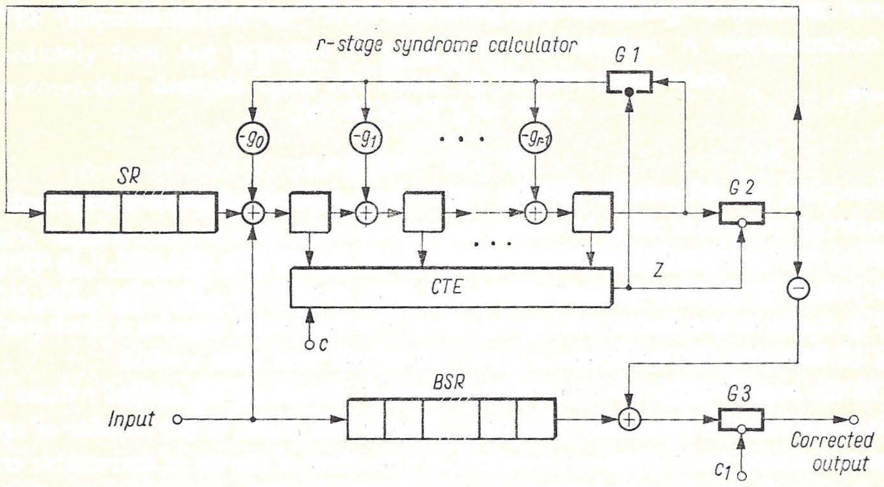

Fig. 4. General decoder circuit for arbitrary cyclic BCH codes with $(n-k)\geqslant(n/2)$
SR — as in Fig. 2; BSR — n-stage buffer shift register

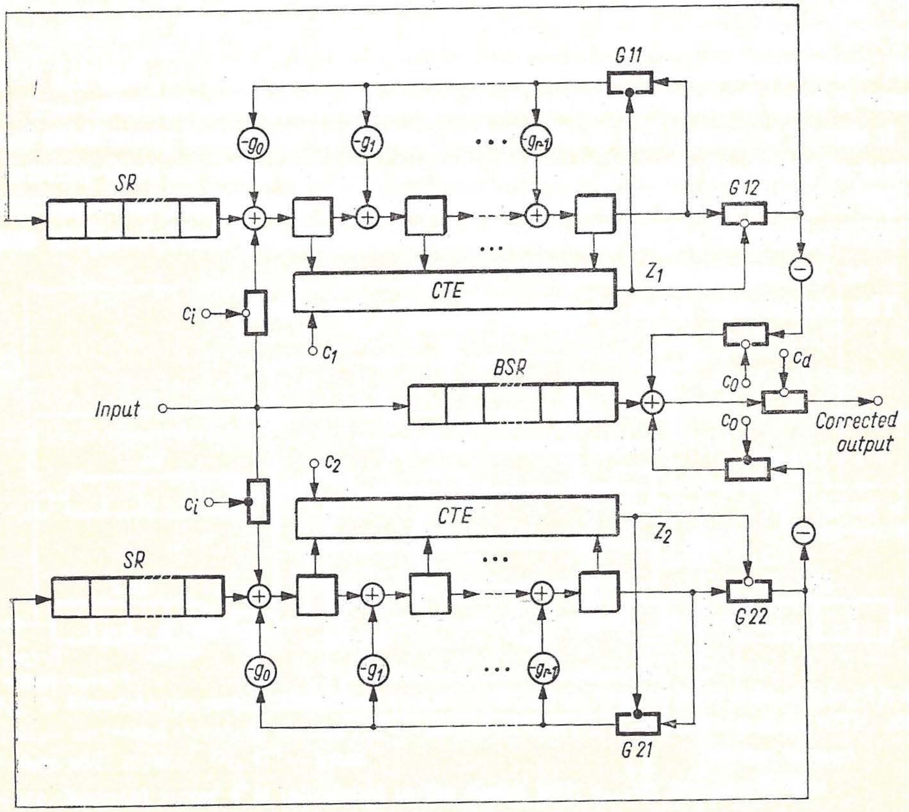

Fig. 5. General decoder circuit for arbitrary cyclic BCH codes with $(n-k)\geqslant(n/2)$, operating with transmission rate

Note. BSR — $2n$-stage buffer

The proposed decoding procedure leads in this case to a general error-correction-error-detection circuit, shown in Fig. 3. Some of error-patterns of weight t or less, distributed in r consecutive positions of a received vector V is now correctable (because of cyclic property of the code, components v_{n-1} and v_0 are considered to be adjacent). On the other hand, such any error-pattern, which cyclically shifted $n-r$ places to the right gives for any shift a syndrome of weight at least $t+1$ can be successfully detected.

The decoding procedure for a circuit in Fig. 3 is similar to that in Fig. 2, except of a number of clock-periods of a second phase, which is here equal to $k=n-r$.

It is easy now to apply the above considerations to decoder circuits construction. The samples of general decoders are given in Figs. 4 and 5. The only two remarks ought to be made now. First, in the error-vector-calculating and error-detecting circuits, presented in this paper, both the error-correction in the information and in the check positions have been taken into account. If there is only a requirement for error-correction in the information digits, the described circuits could be simplified by removing shift register stages, which store error-vector components in check positions, by shortening buffer shift registers, and by withdrawing feedback loops with suitable gates.

The second remark touchs the circuit in Fig. 5. The two error-vector calculating circuits work here alternately, i.e. when the upper circuit participates in the error-correction procedure, at the same time in the lower circuit the error-pattern of a next received vector is calculated and vice versa. Such arrangement makes possible a continuous flow of received vector stream through the decoder with the line transmission rate and it has self-evident practically usefull advantages.

4. Practical example

The application of the described general procedure for BCH decoding to the codes over GF (2), because of its simplicity, is trivial. Therefore, more sophisticated example of a BCH code over GF (4) will be presented.

Let the field GF (4) be a set of elements GF (4) = {0, 1, 2, 3} with the operations of addition and multiplication, defined by means of presented tables:

Addition over GF (4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Multiplication over GF (4)

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Let α denote the root of primitive polynomial x^3+x^2+x+2 on which the Galois field GF (4^3) may be based. If $\beta=\alpha^3$, then the order of β is 21 and the cyclic

BCH (4, 1, 7) code of length 21 will be generated, in accordance with (4), by the polynomial

$$g(x) = \text{L.C.M.}\left\{\prod_{i=1}^{6} m_i(x)\right\}.$$

But

$$m_1(x) = m_4(x) = x^3 + 2x^2 + 1,$$

$$m_2(x) = x^3 + 3x^2 + 1,$$

$$m_3(x) = m_6(x) = x^3 + x + 1,$$

$$m_5(x) = x^3 + 2x + 1.$$

Thus

$$g(x) = (x^3 + 2x^2 + 1)(x^3 + 3x^2 + 1)(x^3 + x + 1)(x^3 + 2x + 1)$$

and finally

$$g(x) = x^{12} + x^{11} + 2x^{10} + 3x^9 + x^7 + 2x^6 + 2x^5 + 3x^3 + 3x^2 + 3x + 1.$$

The redundancy of BCH (4, 1, 7) code will consequently be 12 quaternary digits. Thus, the BCH (4, 1, 7) code of length 21 is a (21, 9) code. Such a code is a null space of an ideal, generated by the polynomial

$$h(x) = (x^{21} - 1)/g(x)$$

i.e.

$$h(x) = x^9 + x^8 + 3x^7 + 2x^6 + 2x^3 + x^2 + 3x + 1$$

The polynomial $h(x)$ may be used, as for example in the circuit in Fig. 6, for an encoder construction. The application of a generator polynomial $g(x)$ to the circuit in Fig. 4 leads to the decoder circuit as in Fig. 7.

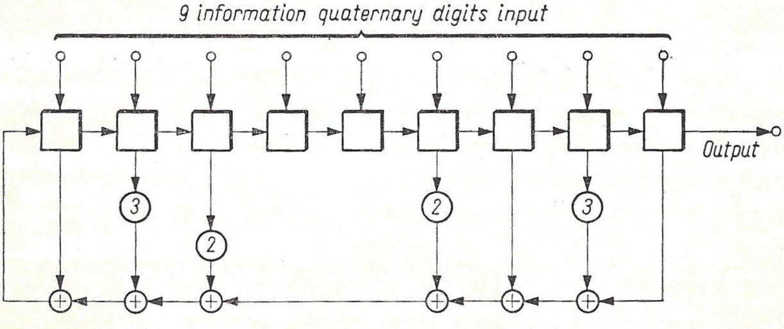

Fig. 6. Encoder for BCH (4, 1, 7) (21, 9) cyclic code over GF (4)
Note. After paralell introduction of 9 information digits, circuit is 21 times shifted

The BCH (4, 1, 7) (21, 9) code may be practically employed for error-control in data transmission systems with four-level (quadrature) modulation. This may be done by mapping GF (4) onto a column-vector space of four 2-tuples over GF (2),

9. Peterson W. W., Error-correcting codes. J. Wiley a. Sons, New York, 1961.

10. Prange E., The use of information sets in decoding cyclic codes. *IRE Trans. on Information Theory* **IT-8** (1962).

11. Szwaja Z., On step by step decoding of the BCH binary codes. *IEEE Trans. on Information Theory* **IT-13** (Apr. 1967).

Procedura korekcji i detekcji błędów dla dowolnych cyklicznych kodów BCH

Przedstawiono procedurę dekodowania cyklicznych kodów Bose-Chaudhuri-Hoquenghema nad dowolnym ciałem GF (q) przy $q=p^m$. Opisana metoda nie wymaga obliczeń nad rozszerzeniem ciała GF (q^M) i wykorzystuje cykliczne właściwości kodu dla korekcji i detekcji błędów. Prostota proponowanego algorytmu dekodowania prowadzi do łatwej realizacji układowej.

Процедура исправления и обнаружения ошибок для произвольных циклических кодов БЧХ

В статье представлена процедура декодирования произвольных циклических кодов Боуза-Чоудхури-Хоквинхема над полем GF (q) при $q=p^m$. Описываемый метод не требует вычисления над расширением поля GF (q^M) и использует циклическое свойства кода для исправления и обнаружения ошибок. Следовательно, принцип предлагаемого метода прост, а схемная реализация легко выполнима.

Wskazówki dla Autorów

W wydawnictwie "Control and Cybernetics" drukuje się prace oryginalne nie publikowane w innych czasopismach. Zalecane jest nadsyłanie artykułów w języku angielskim. W przypadku nadesłania artykułu w języku polskim, Redakcja może zalecić przetłumaczenie na język angielski. Objętość artykułu nie powinna przekraczać 1 arkusza wydawniczego, czyli ok. 20 stron maszynopisu formatu A4 z zachowaniem interlinii i marginesu szerokości 5 cm z lewej strony. Prace należy składać w 2 egzemplarzach. Układ pracy i forma powinny być dostosowane do niżej podanych wskazówek.

1. W nagłówku należy podać tytuł pracy, następnie imię (imiona) i nazwisko (nazwiska) autora (autorów) oraz w porządku alfabetycznym nazwę reprezentowanej instytucji i nazwę miasta. Po tytule należy umieścić krótkie streszczenie pracy (do 15 wierszy maszynopisu).

2. Materiał ilustracyjny powinien być dołączony na oddzielnych stronach. Podpisy pod rysunki należy podać oddzielnie.

3. Wzory i symbole powinny być wpisane na maszynie bardzo starannie.

Szczególną uwagę należy zwrócić na wyraźne zróżnicowanie małych i dużych liter. Litery greckie powinny być objaśnione na marginesie. Szczególnie dokładnie powinny być pisane indeksy (wskaźniki) i oznaczenia potęgowe. Należy stosować nawiasy okrągłe.

4. Spis literatury powinien być podany na końcu artykułu. Numery pozycji literatury w tekście zaopatruje się w nawiasy kwadratowe. Pozycje literatury powinny zawierać nazwisko autora (autorów) i pierwsze litery imion oraz dokładny tutuł pracy (w języku oryginału), a ponadto:

a) przy wydawnictwach zwartych (książki) — miejsce i rok wydania oraz wydawcę;

b) przy artykułach z czasopism: nazwę czasopisma, numer tomu, rok wydania i numer bieżący.

Pozycje literatury radzieckiej należy pisać alfabetem oryginalnym, czyli tzw. grażdanką.

Recomendations for the Authors

Control and Cybernetics publishes original papers which have not previously appeared in other journals. The publications of the papers in English is recommended. No paper should exceed in length 20 type written pages (210×297 mm) with lines spaced and a 50 mm margin on the lefthand side. Papers should be submitted in duplicate. The plan and form of the paper should be as follows:

1. The heading should include the title, the full names and surnames of the authors in alphabetic order, the name of the institution he represents and the name of the city or town. This heading should be followed by a brief summary (about 15 typewritten lines).

2. Figures, photographs tables, diagrams should be enclosed to the manuscript. The texts related to the figures should be typed on a separate page.

3. Of possible all mathematical expressions should be typewritten. Particular attention should be paid to differentiation between capital and small letters. Greek letters should as a rule be defined. Indices and exponents should be written with particular care. Round brackets should not be replaced by an inclined fraction line.

4. References should be put on the separate page. Numbers in the text identified by references should be enclosed in brackets. This should contain the surname and the initials of Christian names, of the author (or authors), the complete title of the work (in the original language) and, in addition:

a) for books — the place and the year of publication and the publisher's name;

b) for journals — the name of the journal, the number of the volume, the year of the publication, and the ordinal number.