ON THE COMPUTATION OF MINIMUM REDUNDANCY CYCLIC CODES ABLE TO CORRECT GIVEN ERROR PATTERN TYPES

E. Gorog

Centre d'Etudes et Recherches
IBM FRANCE
LA GAUDE, FRANCE

Institute of Statistics Mimeo Series No. 484.6

September, 1966

Presented at the NATO Summer School on
Combinatorial Methods in Coding and
Information Theory, Royan, France
August 26 - September 8, 1965

Organized by:

The Department of Statistics
University of North Carolina
and
The Institute of Statistics
University of Paris

This research was supported by the Air Force Office of Scientific Research Contract No. AF-AFOSR-760-65 and also partially supported by the Contract No. AF-19-(604)-8516.

DEPARTMENT OF STATISTICS
UNIVERSITY OF NORTH CAROLINA
Chapel Hill, N. C.

STATEMENT OF THE PROBLEM

INTRODUCTION

The "error correction coding theory" is of undeniable interest at present. The number of publications in the last ten years on this subject is impressive and the results are attractive :

> Classes of codes able to correct either one error burst, or multiple errors (most studied case) or several error bursts have been constructed[1]; others will surely be. Limits on their capabilities have been estimated[1].

If the numerous points of view on the choice of codes are somewhat different, none the less, two most important aspects of the problem are:

1 - the redundancy of the code

2 - the feasibility of the code.

Among all possible different codes, we chose to study the "cyclic code" family the implementation of which is relatively easy (aspect 2).

The purpose of this paper is to give definitively and for a well defined (and limited) type of problem the best existing cyclic code, that is the code with minimum redundancy (aspect 1). It will particularly be shown that the best cyclic codes appear to be at least as good as every code ("optimum" quasi optimum"...) which has been published in the coding literature until now.

ERROR PATTERN TYPE

We denote by <u>K</u> the number of check bits $K > 0$

<u>I</u> the number of information bits $I \leq 0$

<u>L</u> the total message length

$$L = K + I$$

- We call "error pattern" a pattern which represents the structure of a set of errors occuring within the message of length L.

We denote by <u>E</u> a set of <u>n</u> different error patterns which have to be corrected.

by <u>C(E, K)</u> a code with K check bits which corrects any of the n elements belonging to the set E.

The total number of error patterns which can be corrected by C is $2^K - 1$.

If C is such that $2^{K-1} - 1 < n \leq 2^K - 1$ the code is said to be "optimal" in the sense that the minimum number of check bits which are necessary to correct the set E of n error patterns in a message length L is K.

If C satisfies $n = 2^K - 1$ the code is said to be "perfect"

Two different error patterns belong to the same "error pattern type" if one can be obtained from the other by shifting only.

An error pattern which can be shifted s times in the message, and no more, belongs to an error pattern type of length ℓ such that:

$$\ell = L - s$$

$$s = L - \ell$$

We say than an error pattern type is "corrected" when its $s + 1$ error patterns are all corrected.

We denote by $\underline{T}$ the set of the $\underline{m}$ different error pattern types of E such that we may write:

$$T = (T_1, T_2, \dots\dots\dots\dots , T_m)$$

and

$$C(E, K) = C(T, L, K)$$

We shall represent an error pattern type of length ℓ by a polynomial $T(x)$ of degree $\ell - 1$ such that:

$$T(x) = 1 + \sum_i t_i x^i + x^{\ell-1}$$

We call the syndrome (or the error vector) of an error pattern its representation given by the code $C(T, L, K)^1$

The syndrome of an error pattern belonging to an error pattern type $T(x)$ will be denoted by $S[x^i T(x)]$

CORRECTION OF THE SET T OF ALL THE ERROR PATTERN TYPES

Correction of one error pattern type $T_1(x)$

An error pattern type $T_1(x)$ of length ℓ_1 is corrected by the code in a message of length L if, and only if:

$$\left.\begin{array}{l} S[\,x^{i}T_1(x)] \neq S[\,x^{j}T_1(x)] \\ \text{for} \quad 0 \leq i,\ j \ \leq L-\ell_1 \ \text{and} \ \ i \neq j \end{array}\right\} \quad (1)$$

The $L-\ell_1 + 1$ syndromes of $T_1(x)$ can never be confused.

Correction of two error pattern types $T_1(x)$ and $T_2(x)$

Two different error pattern types $T_1(x)$ of length ℓ_1 and $T_2(x)$ of length ℓ_2 are corrected by the code in a message of length L if, and only if the the three following conditions are simultaneously satisfied.

$$\left.\begin{array}{ll} S[\,x^{i}\ T_1(x)] \neq S[\,x^{j}\ T_1(x)] & 2.1 \\ \text{for} \quad 0 \leq i,j \leq L-\ell_1 \ \text{and} \ i \neq j & \\ & \\ S[\,x^{i}\ T_2(x)] \neq S[\,x^{j}\ T_2(x)] & 2.2 \\ \text{for} \ 0 \leq i,j \leq L-\ell_2 \ \text{and} \ i \neq j & \\ & \\ S[\,x^{i}\ T_1(x)] \neq S[\,x^{j}\ T_2(x)] & 2.3 \\ \text{for} \ 0 \leq i \leq L-\ell_1 \ \text{and for} \ 0 \leq j \leq L-\ell_2 & \end{array}\right\}$$

Conditions (2) state that the $2L + 2 - \ell_1 - \ell_2$ syndromes corresponding to the two error pattern types can never be confused since they are all different.

Correction of the set T of all the error pattern types

The whole set T will be corrected by the code in a message of length L, if for any two error pattern types of T, conditions (2) are always satisfied.

CYCLIC CODES

Any code within the "cyclic codes family" may be represented by its generator polynomial F(x) of degree K such that

$$F(x) = 1 + \sum_i f_i x^i + x^K$$

$$1 \leq i \leq K-1 \qquad f_i \text{ equals 0 or 1.}$$

We denote by F the set of the 2^{K-1} polynomials F(x) of degree K.

The syndrome $S[x^i\ T(x)]$ for a cyclic code is an element which characterizes the equivalence class of $x^i\ T(x)$ defined modulo F(x)

In order to simplify the presentation of this paper, we shall assume that every following equivalence relation $\equiv$ will be implicitly written modulo F(x).

We call the cycle length n of T(x) the least positive integer n such that:

$$x^n T(x) \equiv T(x)$$

ESTABLISHMENT OF THE ALGORITHM

PRELIMINARY STUDY

For any cyclic code, condition (1) may be written:

$$x^i T_1(x) \equiv T_1(x)$$

$$\text{for } 0 \leq i \leq L - \ell_1$$

but n_1 being the cyclic length of $T_1(x)$, we have necessarily $i < n_1$ which implies $L - \ell_1 < n_1$.

Condition (1) may be reduced to

$$L - \ell_1 + 1 \leq n_1 \qquad (1')$$

The maximum length of the message in which $T_1(x)$ is corrected will be denoted by L_1

$$L_1 = n_1 + \ell_1 - 1$$

In the same way, n_1 and n_2 being the respective cycle lengths of $T_1(x)$ and $T_2(x)$, conditions (2) may be written (2')

$$\left.\begin{array}{ll} L - \ell_1 + 1 \leq n_1 & 2'.1 \\ L - \ell_2 + 1 \leq n_2 & 2'.2 \\ \left.\begin{array}{l} x^k T_1(x) \equiv T_2(x) \\ \text{for } 0 \leq k \leq L - \ell_1 \\ x^k T_2(x) \equiv T_1(x) \\ \text{for } 0 \leq k \leq L - \ell_2 \end{array}\right\} & 2'.3 \end{array}\right\} (2')$$

One of two cases may happen:

1 - $S[T_1(x)]$ and $S[T_2(x)]$ are in different cycles.

Conditions 2'3 are always verified and condition (2') may be reduced to (2")

$$\left.\begin{array}{l} L - \ell_1 + 1 \leq n_1 \\ L - \ell_2 + 1 \leq n_2 \end{array}\right\}$$

The maximum length L_2 of the message in which $T_1(x)$ and $T_2(x)$ are corrected is given by:

$$L_2 = \min[n_1 + \ell_1 - 1,\ n_2 + \ell_2 - 1]$$

that is:

$$L_2 = \min\ [L_1,\ n_2 + \ell_2 - 1]$$

2 - $S[T_1(x)]$ and $S[T_2(x)]$ are in the same cycle.

- $n_1 = n_2$
- there exists a value d such that

$$x^d T_1(x) \equiv T_2(x)$$

$$x^{n_1 - d} T_2(x) \equiv T_1(x)$$

Conditions 2'.3 then imply:

$K < d$ and $K < n_1 - d$

Since conditions 2'. 1 and 2'. 2 are included in 2'. 3 ($d < n_1$) condition (2') may be reduced to (2" bis)

$$\left.\begin{array}{l} L - \ell_1 + 1 \leq d \\ L - \ell_2 + 1 \leq n - d \end{array}\right\} \qquad \text{(2" bis)}$$

The maximum length L_2 of the message in which $T_1(x)$ and $T_2(x)$ are corrected is given by:

$L_2 = \min (d + \ell_1 - 1, \ell_2 + n - d - 1)$

GENERALISATION OF THESE RESULTS

We shall denote by $\underline{L_p}$ the maximum length of the message in which

$T_1 (x), T_2(x), \ldots\ldots\ldots\ldots, T_p (x)$ with $p < m$

are all corrected by $F(x)$

$L_p \leq L_{p-1} \leq L_{p-2} \leq \ldots\ldots\ldots\ldots, \leq L_1$

We shall assume that we know the p respective positions in their cycles of the syndromes $S[T_1 (x)]$, $S[T_2 (x)]$, ..., $S[T_p (x)]$ and that, from these positions, the value L_p has already been deduced.

Let us consider now the error pattern type $T_{p+1} (x)$ and its syndrome $S[T_{p+1} (x)]$

One of two cases may happen:

1 - $S[T_{p+1} (x)]$ is in a different cycle from the cycles (or the cycle) which contain (or contains):

$$S[T_1 (x)] , S[T_2 (x)] ,\ldots\ldots\ldots\ldots, S[T_p (x)]$$

L_{p+1} will be given by:

$$L_{p+1} = \min [L_p, n_{p+1} + \ell_{p+1} - 1]$$

2 - $S[T_{p+1} (x)]$ is in one of these cycles (or this cycle)

suppose α and β are the minimum values for any existing couple (ab) with $1 \leq a, b \leq p$ and such that

$$x^{\alpha} T_a (x) \equiv T_{p+1} (x)$$

$$x^{\beta} T_{p+1} (x) \equiv T_b (x)$$

L_{p+1} will be given by:

$$L_{p+1} = \min[L_p,\ a + \ell_a - 1,\ \ \beta + \ell_{p+1} - 1]$$

Remarks

- if a=b $\beta = n_a - \alpha$

$S[T_{p+1}(x)]$ belongs to a cycle which only contains one other syndrome $S[T_a(x)]$

- If $L_p = n_a + \alpha - 1$

$L_{p+1} = \min\ [\alpha + \ell_a - 1,\ \ n_a - \alpha + \ell_2\ -1\ ]$ since $\alpha < n_a$

This is the case of p = 1.

- but, in general, it could happen that $L' = \min\ [\alpha + \ell_a - 1, \beta + \ell_{p+1} - 1]$ with $L' > L_p$ such that $T_a(x)$, $T_b(x)$, $T_{p+1}(x)$ would be corrected in L' but not the set $T_1(x)$, ..., $T_a(x)$, ..., $T_b(x)$, ...$T_{p+1}(x)$ and we have

$$L_{p+1} = \min\ [L_p,\ L']$$

CONSEQUENCES OF THE ALGORITHM

F(x) will correct the set T in a message of length L if, and only if we have:

$L \leq L_m$

Let us consider the same set T of error pattern types. We shall denote by <u>L(h)</u> the value L_m corresponding to each polynomial $F_h(x)$ of the set F

$$1 \leq h \leq 2^{K-1}$$

The code generated by F_h (x) will be: C(T, L(h), K)

The best cyclic codes will be generated by polynomials such as F_M (x) where L(M) $\geq$ L(h) for each value of h

If a cyclic code C(T, L(M), K-1) does not exist, these codes are the best in the sense that:

1 - for a message length of L(M) they correct the set T of error patterns with the minimum possible check bits and

2 - for a message length greater than L(M), all the existing cyclic codes which correct the set T need more than K check bits.

APPLICATION OF THIS ALGORITHM

To apply this algorithm we need

1 - to generate the set T

2 - to compute the value L(h) from the values L_1, L_2, ..., L_{m-1} for a given polynomial $F_h(x)$ of degree K.

3 - to select the best generator polynomials $F_M(x)$ with the value L(M) among the 2^{K-1} possible polynomials $F_h(x)$

4 - to select the best codes for a maximum number of different values of K.

OPTIMISATION

This general procedure, which permits the computation of the best cyclic codes in the correction of any error pattern set, may easily be optimized by the following considerations:

1 - if the m elements of T are defined independently from the final message length the whole set T has to be generated only once.

2 - if we have, for a certain $i < m$, $L_i(h_2) < L(h_1)$ with $1 \leq h_1 < h_2 \leq 2^{K-1}$ we don't need to compute the values $L_j(h_2)$ with $i < j \leq m$ since the polynomial $F_{h_2}(x)$ has to be eliminated in the search for the best cyclic codes.

3 - the 2^{K-1} possible polynomials do not have to be treated one after the other as a theoretical study permits to eliminate some of them before their treatment by the computer.

Examples of cyclic codes which will never be the best ones are those whose generating polynomial is of the form:

$$F(x) = T_a(x) + x^{K-\ell_b+1} T_b(x)$$

Other such improvements can be brought in each special case studied but we shall not mention them here since they are different for different sets T and are given by some theoretical properties of the algebra of polynomials modulo F(x).

4 - If the maximum <u>weight</u>[1] of the elements in T is <u>w</u> the minimum value of K from which we need to start the study is $K = 2w$ since for $K < 2w$ we have necessarily $L = K$ thus $I = 0$

In spite of all these improvements, computer time and memory capacity necessary to apply the algorithm increase very rapidly with K. We have generally limited the computation to:

$$2w - 1 < K < 14$$

But this limitation may also be justified by the fact that the obtained results (which would be limited in any way, even with $K \geq 14$) give us already a good idea of the best cyclic codes capabilities for the 4 different types of error which were treated.

THE RESULTS

Each result is presented in a graphic form and is obtained for a given set T of error types.

The solid lines on the diagram indicate the minimum possible number of check bits K necessary for a cyclic code to correct the set T in a message of length L.

The number of information bits can easily be deduced as $I = L - K$.

The dotted lines above the solid lines of the diagram indicate the limit of the best published cyclic codes found in the coding literature.

The lower dotted lines indicate the theoretical limit for any code. This limit which is effectively reached by an optimal cyclic code, cannot necessarily be reached, at every point, by a systematic (or linear) code.

Problem 1

Correction of a single burst of errors

An error pattern type corresponding to a burst of b errors may be written:

$$T(x) = 1 + \Sigma t_i x^i \qquad \text{with } 1 \leq i \leq b-1,$$

where t_i equals 0 or 1, m is given by $m = 2^{b-1}$.

A study has shown how to construct many new classes of codes with very good single burst error correction properties [2] providing an important gain over some previously published cyclic codes [3 4 5 6].

The codes given by the algorithm have confirmed those theoreticals results for:

$K < 17$

$2 < b < 9$

The algorithm used in this particular case has already been described (7) and the complete corresponding tables of the best burst error correction cyclic codes obtained have been published before (16).

(Only the maximum length of the error pattern type studied was taken into account in the computation).

Problem 2

Correction of e, or less than e, multiple errors

Let us define the symbol Δ by: $x^{\Delta} = 0$

an error pattern type of the set T will have the following form:

$$T(x) = 1 + \sum_i x^{\mu_i} \text{ with } 1 \leq i \leq e - 1$$

Each of the e values μ_i is necessarily taken in the set of the values (Δ, 1, 2, ..., L-1)

Problem 2 has been already studied in its general form [8 9 10 11 12 13 14] and the improvement concerning the number of check bits brought by the best cyclic codes which are described in this paper is slight. Nevertheless it appears that the correction properties of every published systematic code is accomplished by at least a cyclic code.

The results are given for

$K < 14$

$1 < e < 5$ see fig 1, 2, 3

Problem 3

Correction of any e, or less than e, multiple bursts of b errors.

The error pattern type is

$$T(x) = 1 + \sum_i x^{\mu_i}(1 + \sum_j t_j x^j) \text{ with } 1 \leq j \leq b-1$$

where t_j equals 0 or 1 and $1 \leq i \leq e-1$

Each μ_i is taken in the set of the values (Δ, 1, 2, ..., $L-\nu-1$)

ν is the greatest value of j such that $t_j = 1$

The length of T(x) is $e + \nu$, when μ_{e-1} is different from Δ.

Well known codes capable of correcting these errors are not very numerous at the present time [15] and the results obtained here are full of promise.

$K < 14$

$1 < b < 4$ see fig 4, 5.

In the error analysis of actual telephone lines [16] it was established that, independently of an error burst which often may occur in erroneous messages, the percentage of isolated errors (1 error burst) is very high.

In this train of thought we searched the best cyclic codes for $K < 14$ able to correct simultaneously a burst of 3 errors and a burst of 1 error in the message. See fig 6

No theoretical results being available on these types of codes the upper dotted line describes codes correcting 2 bursts of 3 errors.

Problem 4

Correction of any single burst of B errors consisting in e, or less than e, multiple bursts of b errors

The type of error was also suggested by the above mentioned statistics on the errors [16]

The correlation between the errors is not strong enough to necessitate the correction of all possible combination of errors within B bits, when B is relatively large. It is preferable to correct several separated bursts of b errors (in the previously defined sense) which may occur in an interval of maximum length B within the message.

Problem 4 is a particular case of 1 as well as of 3.

The error pattern type has the following form:

$$T(x) = 1 + \sum_i x^{\mu_i} \left(1 + \sum_j t_j x^j\right)$$

with $1 \leq j \leq b-1$ t_j equals 0 or 1

and $1 \leq i \leq e-1$ μ_i is taken in $(\Delta, 1, 2, \ldots, B-\nu-1)$

The cases which were treated are:

$K < 14$

$b = 2$ $B = 8, 11, 15$ see fig. 7, 8.

$b = 3$ $B = 9$ see fig. 9

No codes of this type have previously been derived.

Problem 5

Comparative study of the minimum redundancy cyclic codes as a function of the corrected error pattern types

Fig. 10 shows that if, in a message length L, K bits are used for error checking we may correct any error pattern type corresponding to a curve which crosses the rectangle L K.

The "dot-dash" lines (·-·-) concern problem 1

the number 1 line corresponds to b = 4
" 2 " " to b = 5
" 3 " " to b = 6

The "long dash" lines (— — —) concern problem 2

the number 1 line corresponds to e = 2
" 2 " " e = 3
" 3 " " e = 4

The solid lines concern problem 3

the number 1 line corresponds to b = 2
" 2 " " $b = 1$ $b_2 = 3$
" 3 " " b = 3

The dotted lines concern problem 4

the number 1 line corresponds to B = 8 b = 2

" 2 " " B = 11 b = 2

" 3 " " B = 9 b = 3

Examples of the interpretation of this diagram are as follows:

For L = 50 and K = 12 we may correct either

- any burst of 5 errors or
- any 2 errors or
- a burst of 8 consisting in 2 bursts of 2 errors.

For L = 20 and K = 11 we may correct either

- any burst of 6 errors
- any 3 errors or
- a burst of 8 consisting in 2 bursts of 2 errors.

In each case we cannot do better.

Remarks

In problems 1 and 4 the definition of T(x) is independent of the message length L and the algorithm is straightforward.

It is interesting to note that the algorithm may be applied even when T(x) is a function of the final message length which is in fact the unknown of the problem. We do not know, a priori, the value of m but since we have:

$$L_1 \geq L_2 \geq \cdots\cdots\cdots \geq L_m$$

$$\ell_1 \leq \ell_2 \leq \cdots\cdots\cdots \leq \ell_m$$

$$K < 14$$

the value L_m is given by the first value L_k such that $L_k = \ell_k$ for the latest error pattern type.

CONCLUSIONS

The diversity of the error pattern types for which the computation of the best correcting cyclic codes is possible shows the power of the algorithm. Henceforth, if a statistical analysis of the errors is consistent enough to give the error pattern types which are to be corrected, we are able to fit the best cyclic codes within limited message lengths.

Except for some specific error pattern types and for some given message lengths, a general law for deriving all the best computed cyclic codes has not been formed. Most of them are shortened cyclic codes. However, in the given limits, we may ensure that there is no cyclic code with less check bits than those which are presented and that better systematic codes are not likely to exist. When cyclic codes are optimal, and in this case only, we can say with certainty that better systematic codes do not exist, as for problems 1 and 2.

Among the set of the minimum redundancy cyclic codes corresponding to C(T, L(M), K) we selected one only which appears on the given table (see fig. 17, 18, 19, 20).
A generating polynomial as : $x^6 + x^4 + x^2 + x + 1$ is denoted by 6, 4, 2, 1, 0 and the number of check bits K is given by the first number on the

left (6 in this example).

We also indicate the number of equivalent cyclic codes (same set T, same values of L and K). This number is very often even since 2 symmetrical polynomials G(x) and F(x), the properties of which are:

$G(x) = x^K F(x^{-1})$, have the same coding capabilities.

Error correction only was mentioned in this paper but the best correction codes have also good detection properties. A code C(T, L, K) will detect with the least redundancy any 2 elements of T if the message length is less or equal to L, as well as an important number of other error patterns.

References.

1. W. Peterson, "Error Correcting and Error Detecting Codes," Technology Press, 1961.

2. E. Gorog, "Some New Classes of Cyclic Codes Used for Burst-Error Correction," IBM Journal, 4.63

3. M. Melas, "A New Group of Codes for Correction of Dependent Errors in Data Transmission", IBM Journal 4,58 (1960).

4. L. H. Zetterberg, IRE Trans. on Information Theory, IT-8, 13 (1962).

5. P. Fire, "A Class of Multiple-Error-Correcting Binary Codes for Non-Independent Errors", Stanford Electronics Laboratories, Technical Report No. 55, April 24, 1959.

6. B. Elspas and R. S. Short, IRE Trans. on Information Theory, IT-8, 39(1962).

7. E. Gorog, "Les meilleurs Codes Cycliques correcteurs d'un paquet d'erreurs dans un message de longueur donnée", IFIP Congress, Aug. 62.

8. Bose, R. C. and D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes", Inf. and Control. 3, 68-79 (1960)

9. Hocquenghem, "Codes Correcteurs d'erreurs", "Chiffres", Sept. 59

10. Golay, M.J.E., "Binary Coding", IRE Trans., PGIT-4, 23-28 (1954).

11. Melas, C. M. "A New Group of Codes for Correction of Dependent Errors in Data Transmission", IBM J. Research Develop., 4, 58-65 (1960.)

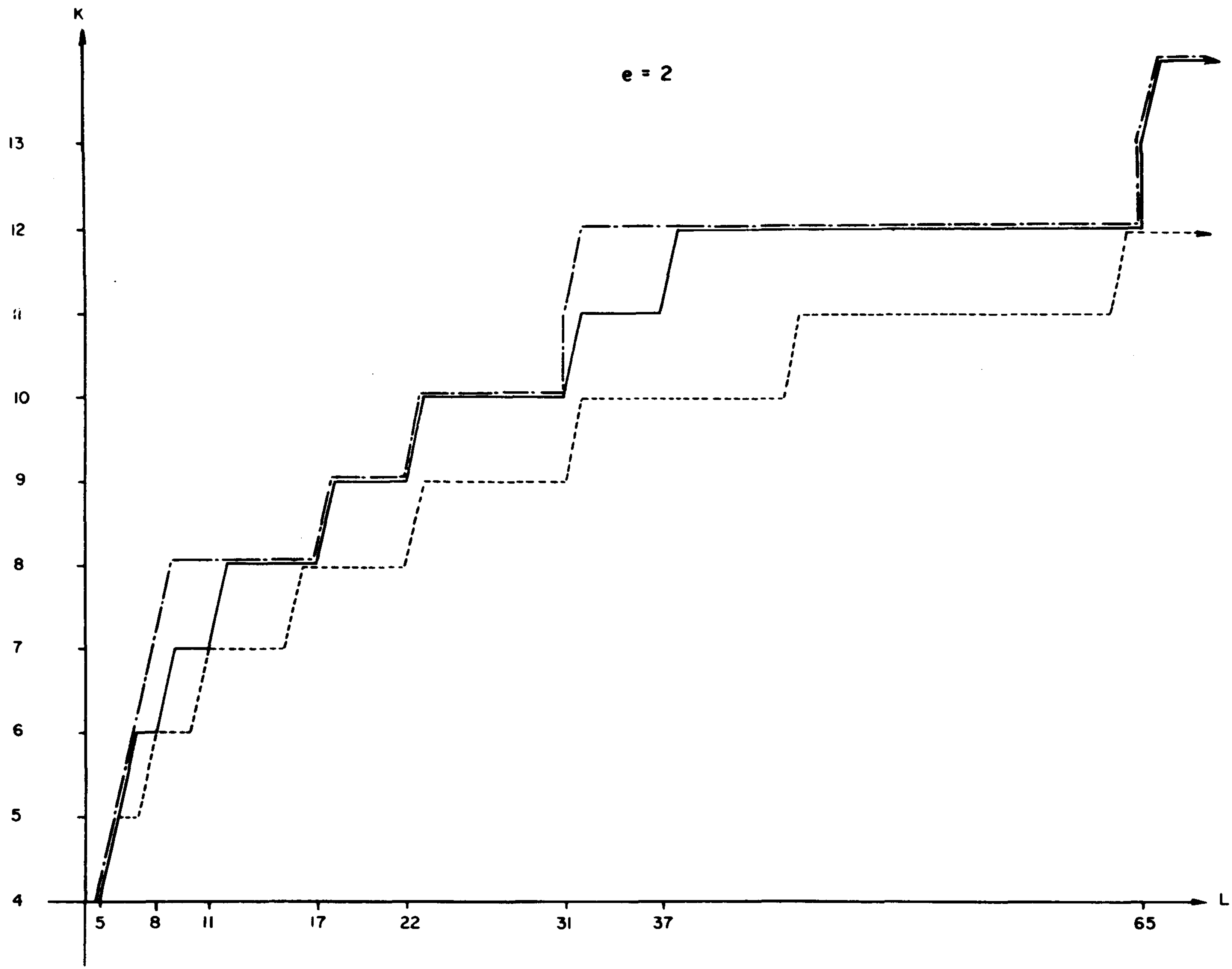
12. Prange, E. "Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms", AFCRC-TN-58-156, Air Force Cambridge Research Center, Bedford, Mass. (April, 1958).

13. Slepian D., "A Class of Binary Signaling Alphabets," Bell System Tech. J. 203-234 (1956).

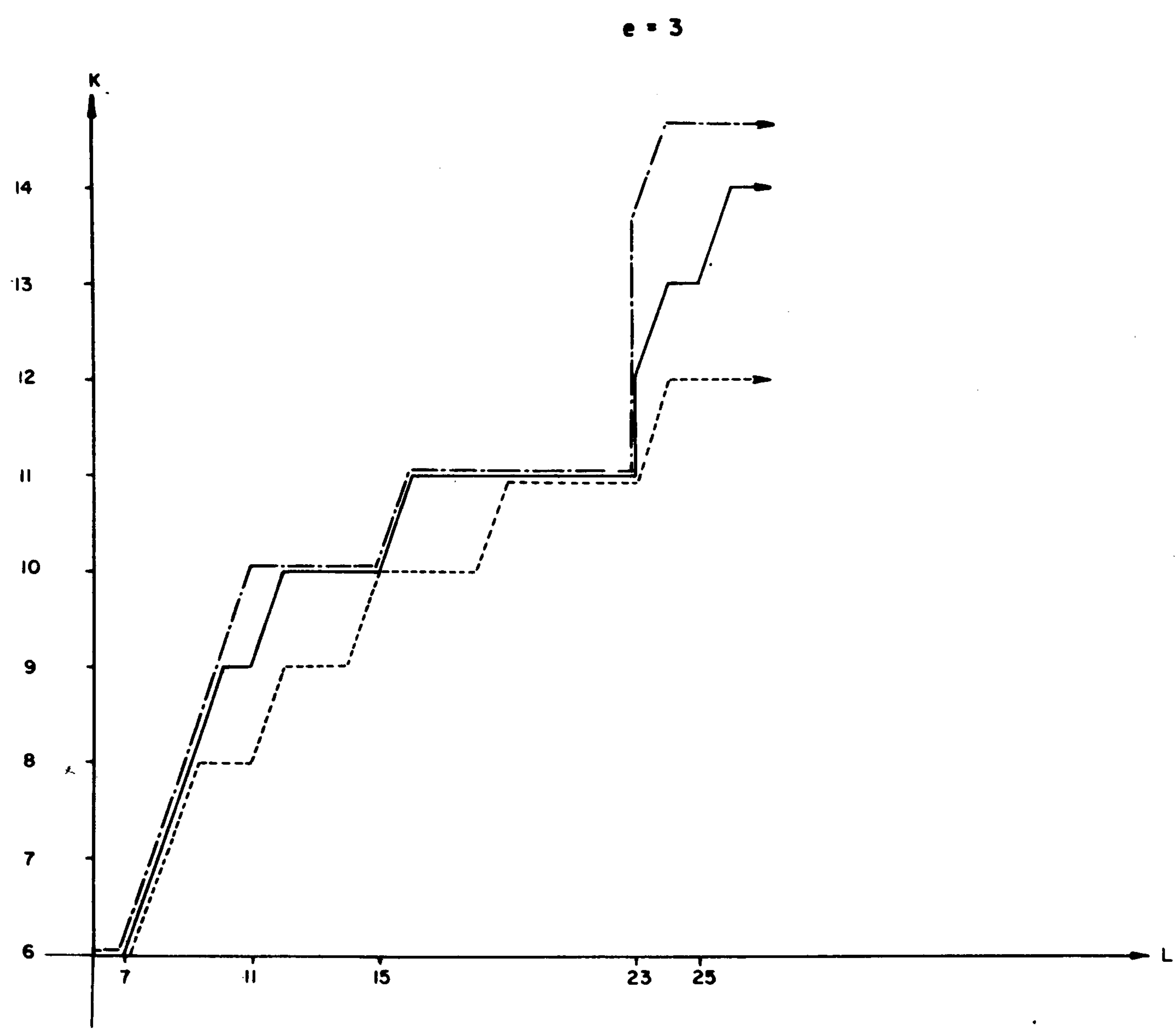
14. Fontaine, A. B., and W. W. Peterson, "Group Code Equivalence and Optimum Codes", IRE Trans. IT-5, Special Supplement, 60-70 (1959).

15. F. Corr, "Multiple Burst Detection", Proc. IRE, Aug. 61

16. F. Corr and E. Gorog, "Les Codes capables d'assurer une sécurité contre les erreurs dans la transmission de données ", to be published in Onde Electrique.



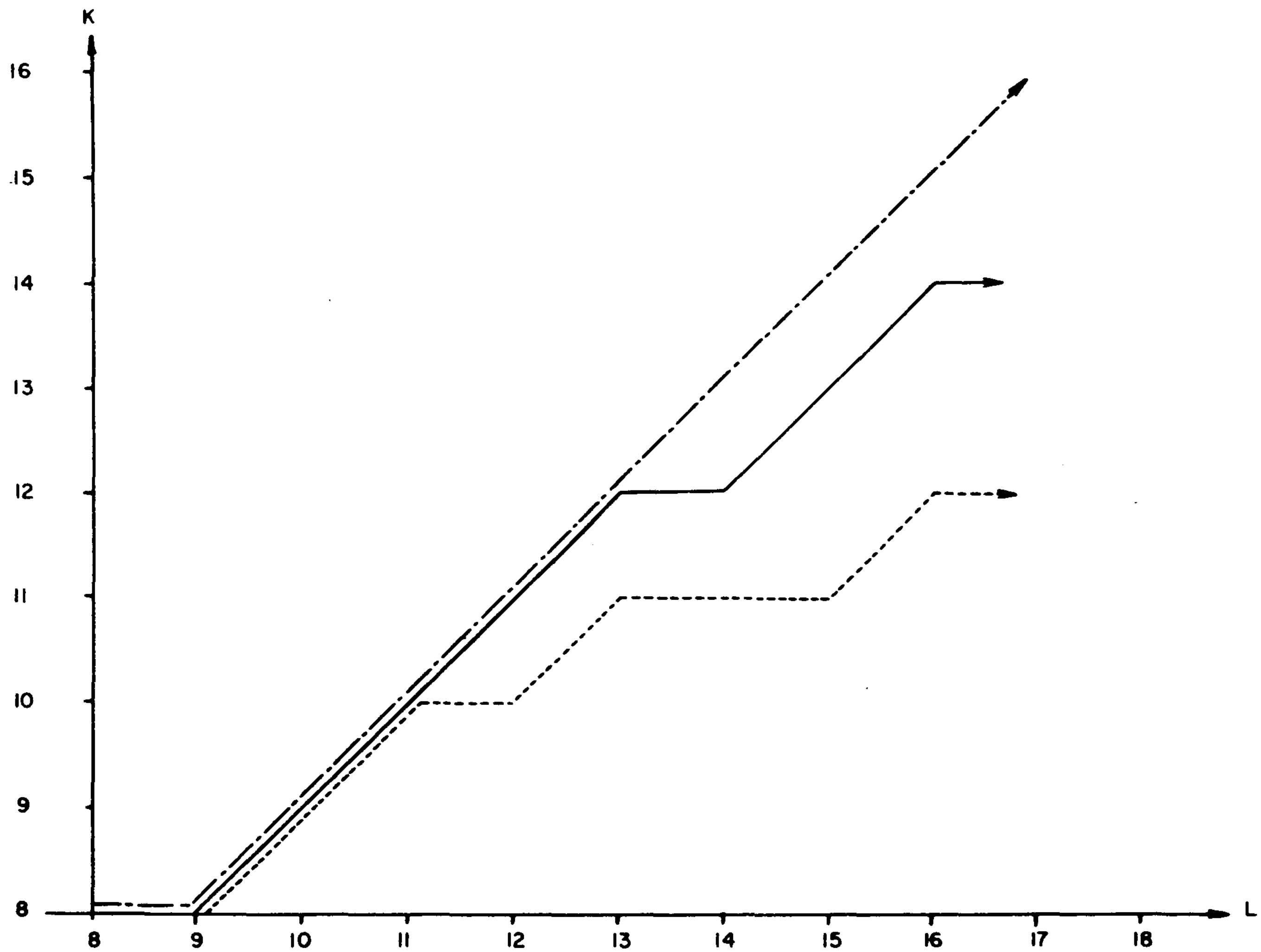
PROBLEME 2



PROBLEME 2

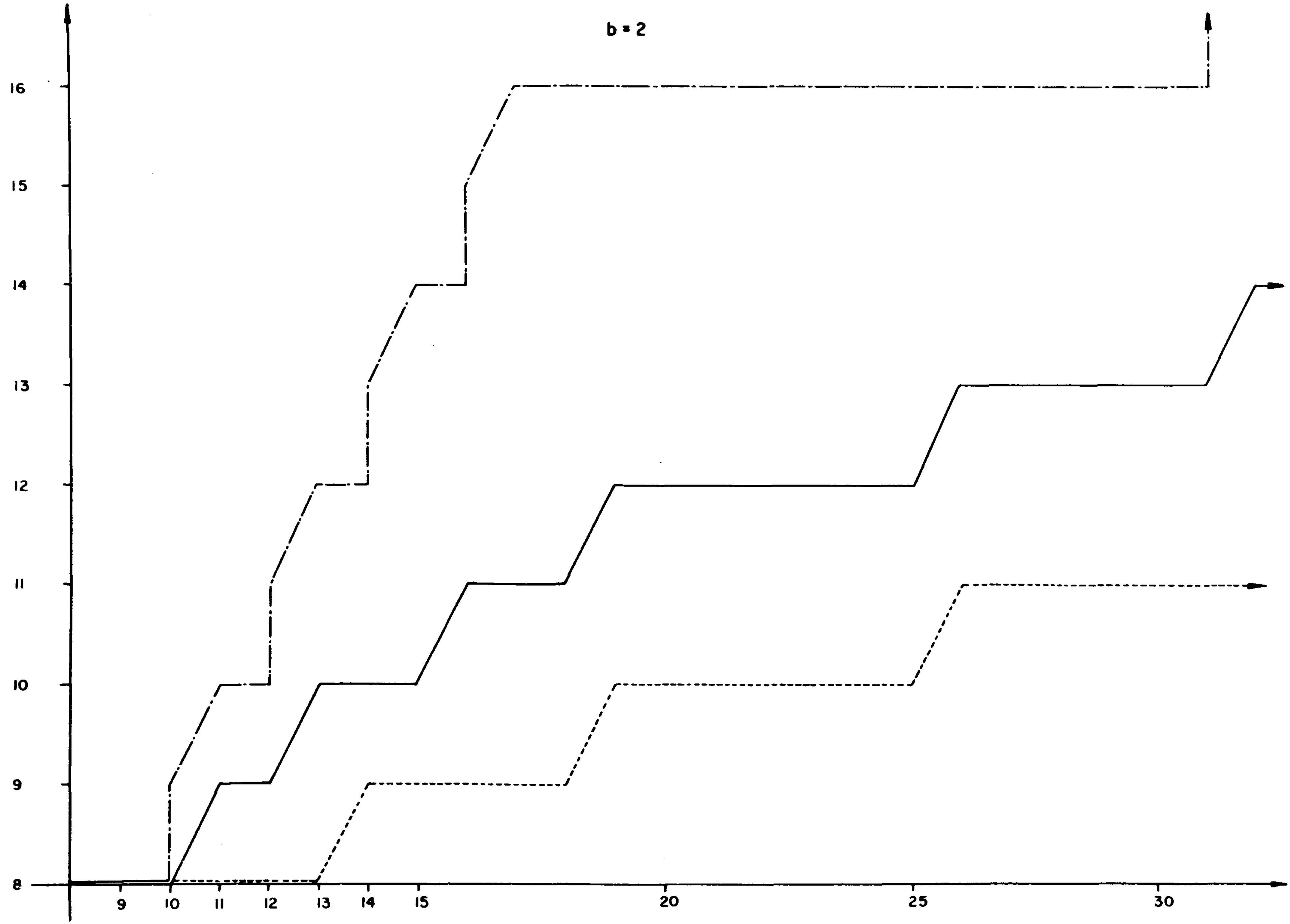
FIG : 2

e = 4



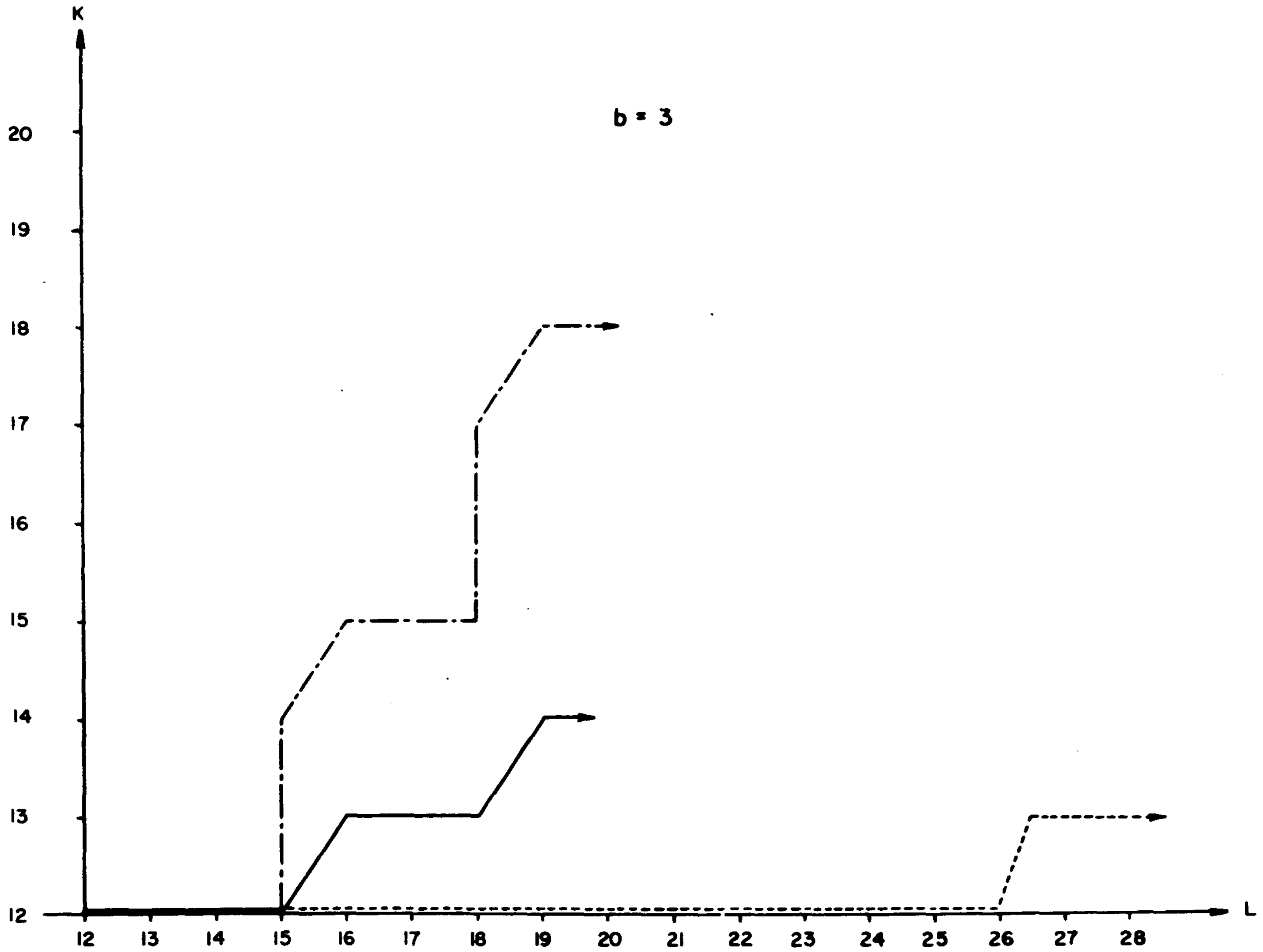
PROBLEME 2

FIG : 3



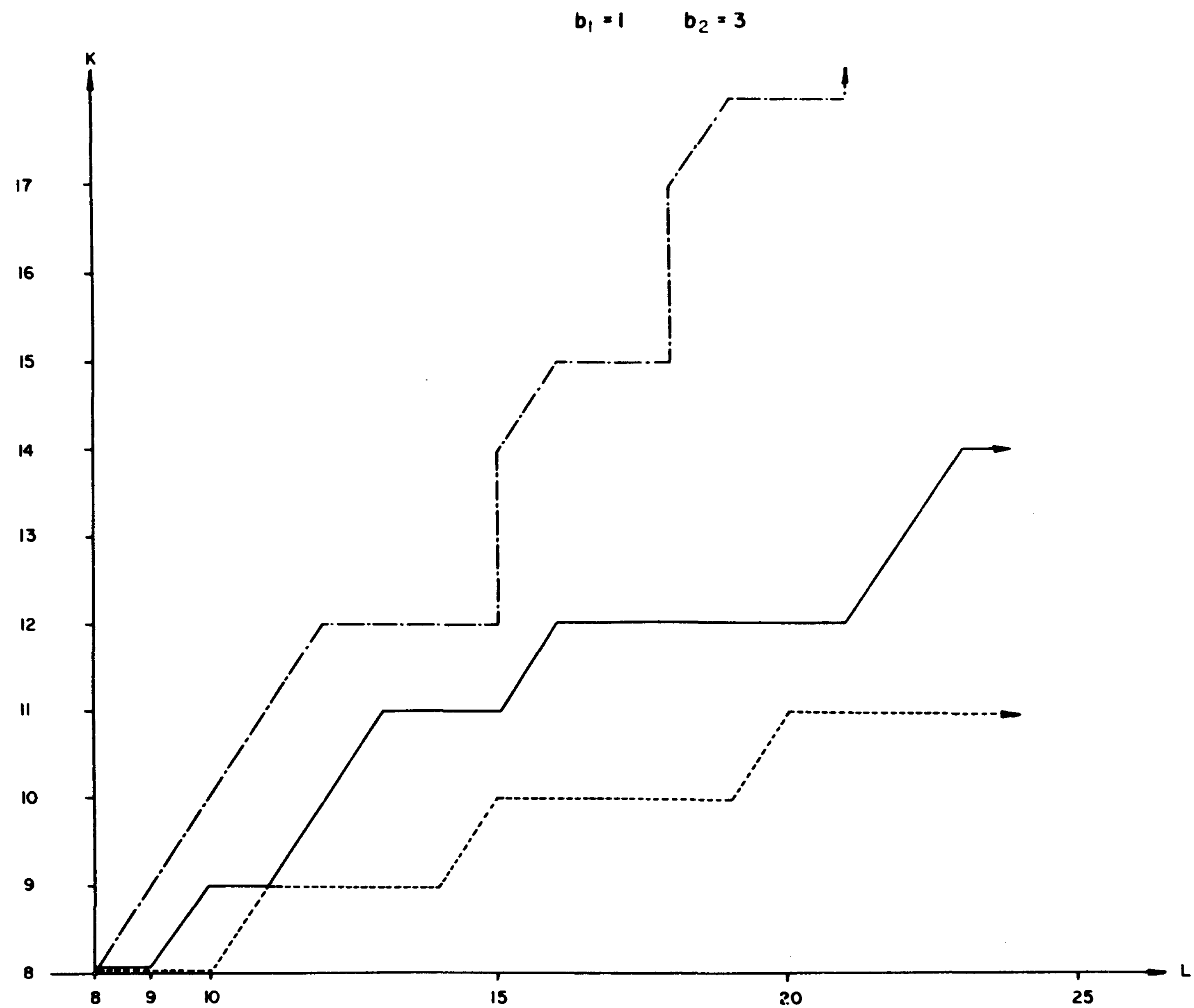
PROBLEME 3

FIG : 4



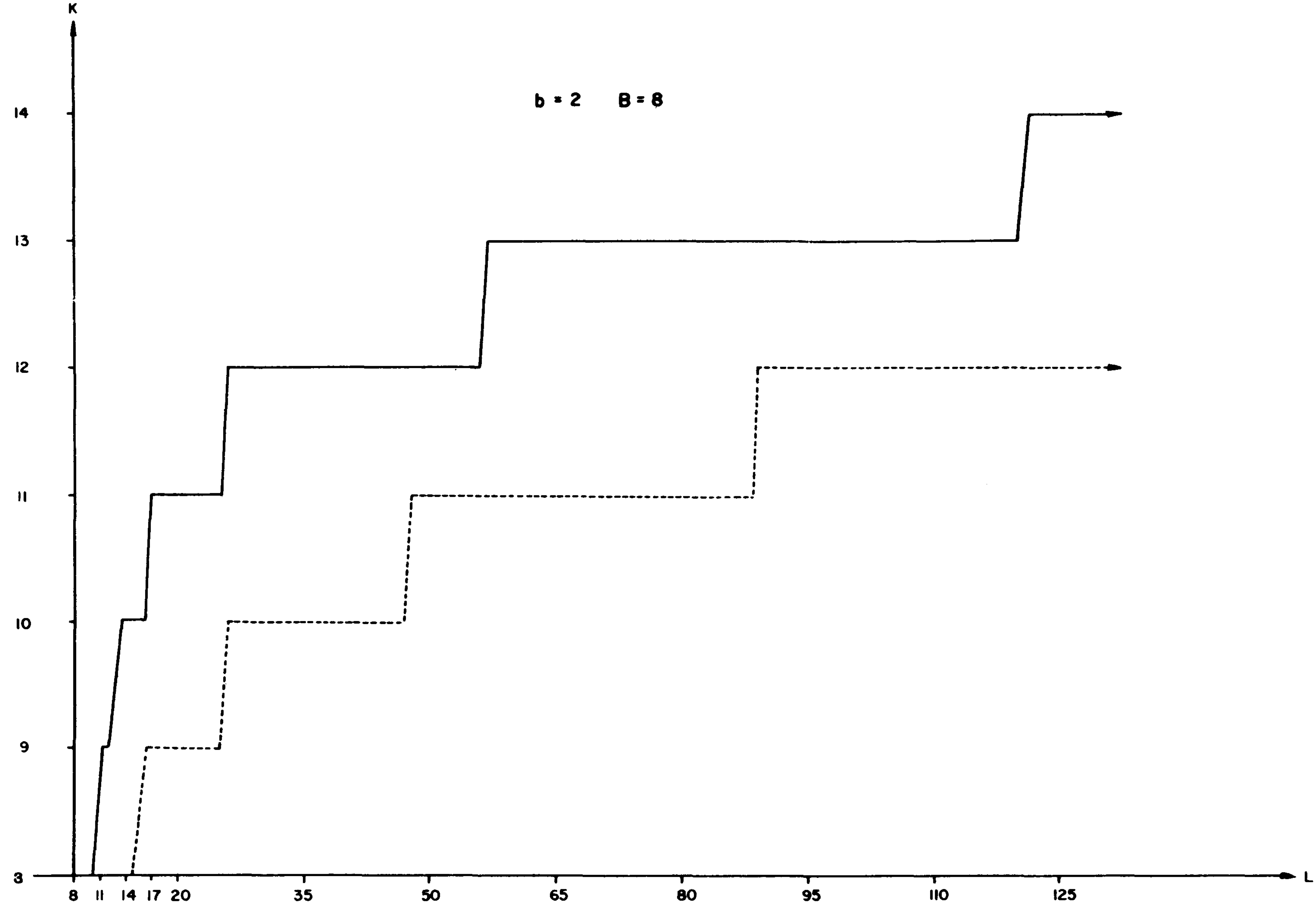
PROBLEME 3

FIG: 5



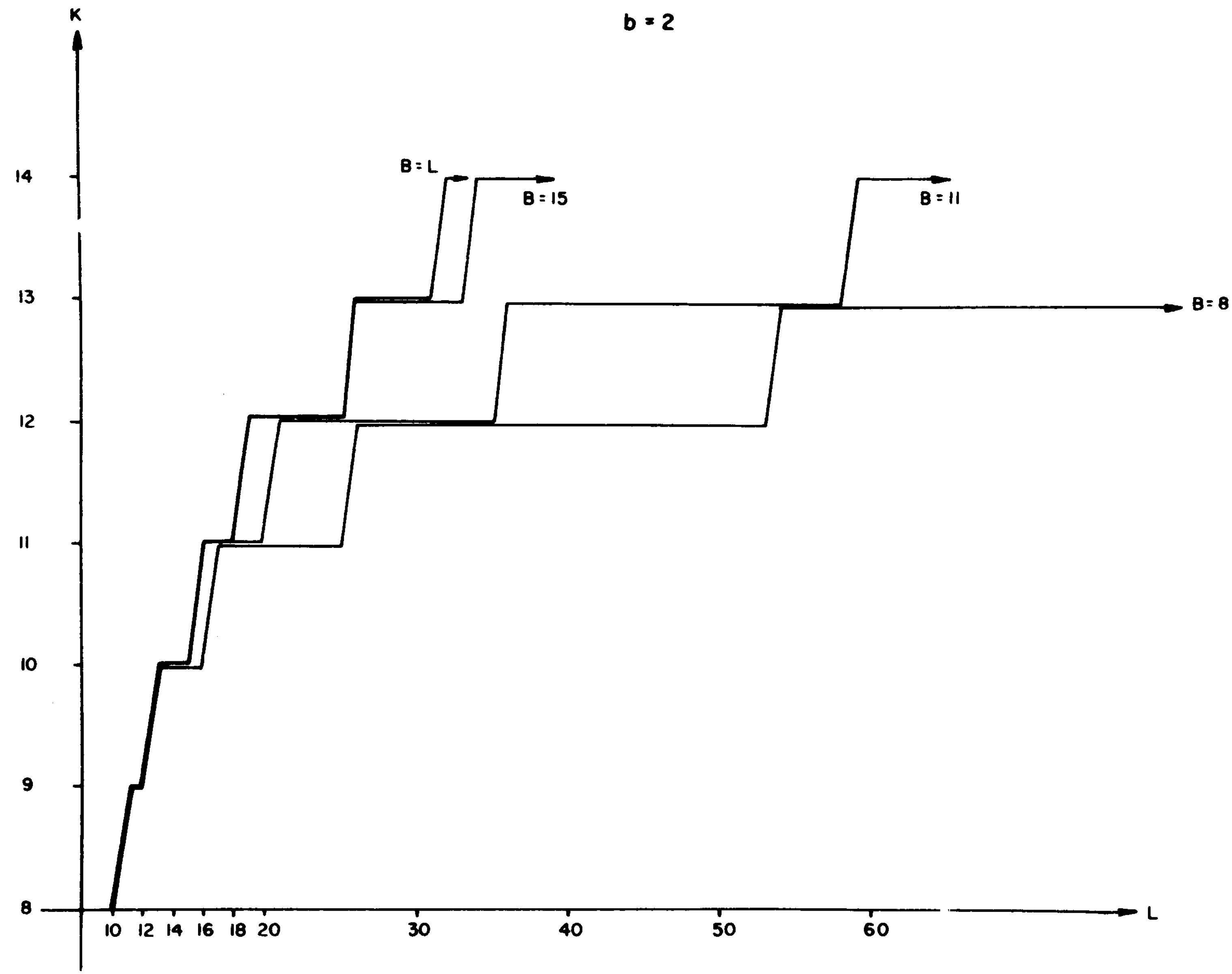
PROBLEME 3

FIG : 6



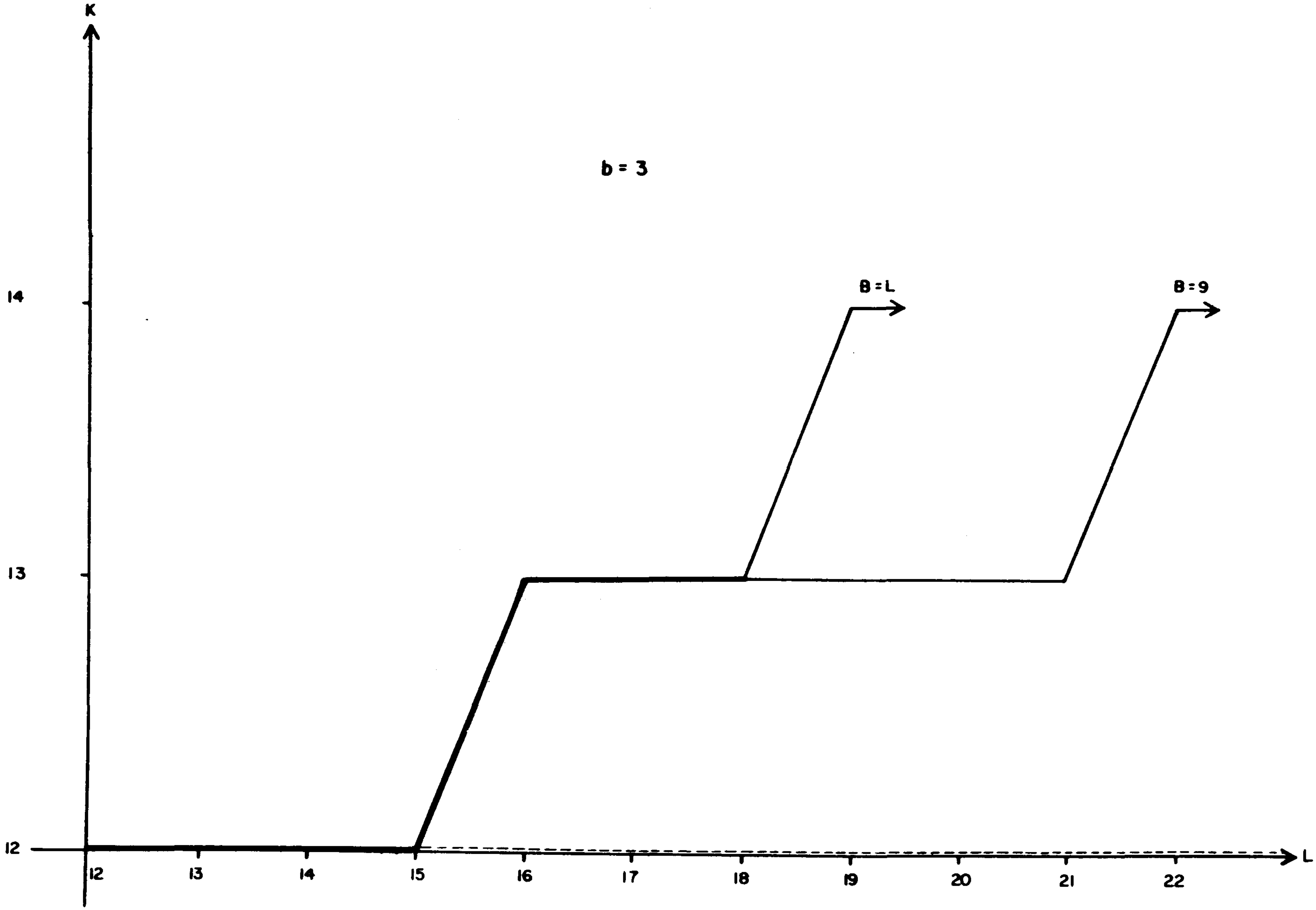
PROBLEME 4

FIG: 7



PROBLEME 4

FIG : 8



PROBLEME 4

FIG : 9

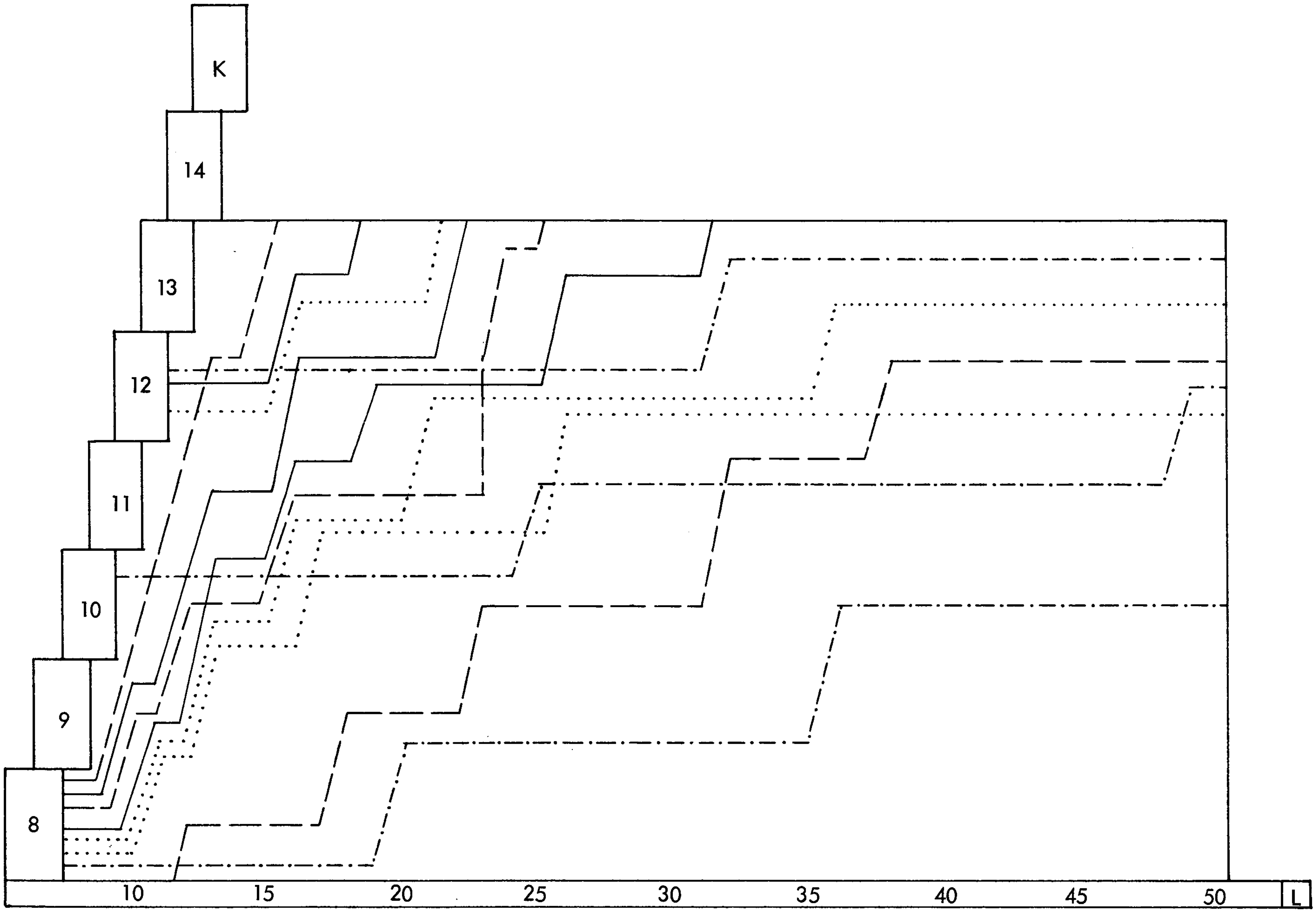


Fig. 10

Type of error-patterns	Maximum message length	Minimum redundancy cyclic code	Number of equi-valent solutions
Problem 1	15	6,3,2,1,0	2
b = 3	27	7,4,1,0	2
	63	8,5,2,1,0	4
	121	9,6,1,0	2
	255	10,7,4,2,0	10
	487	11,9,7,6,5,4,3,2,1,0	2
	1023	12,5,4,3,0	40
	1999	13,12,11,9,8,7,6,5,4,3,2,0	2
Problem 1			
b = 4	19	8,6,4,1,0	2
	35	9,6,4,3,0	2
	82	10,7,5,3,2,0	2
	164	11,10,7,5,3,2,0	2
	511	12,8,5,3,0	2
	1023	13,12,6,3,1,0	10
	1647	14,13,10,9,8,6,5,4,3,0	2
Problem 1			
b = 5	24	10,7,6,5,3,2,0	2
	47	11,9,7,5,4,3,2,1,0	2
	127	12,11,8,7,6,3,1,0	2
	290	13,10,7,6,5,2,0	2
	765	14,9,8,2,0	2

FIG: 11

Type of error-patterns	Maximum message length	Minimum redundancy cyclic code	Number of equivalent solutions
Problem 1 b = 6	31	12,11,9,6,5,4,3,1,0	2
	64	13,11,8,7,6,3,1,0	2
	165	14,12,11,10,9,8,7,5,3,0	2
	363	15,14,13,12,8,7,6,5,4,2,1,0	2
	819	16,15,14,12,11,10,9,7,4,3,2,0	2
Problem 1 b = 7	34	14,11,9,8,7,3,0	2
	99	15,11,10,9,8,4,3,0	2
	144	16,15,14,13,12,11,10,9,8,7,4,2,1,0	2
Problem 1 b = 8	50	16,13,11,8,6,4,3,0	2
Problem 2 e = 2	5	4,3,2,1,0	1
	6	5,3,2,1,0	5
	8	6,4,2,1,0	6
	11	7,5,2,1,0	2
	17	8,5,4,3,0	2
	22	9,8,3,1,0	2
	31	10,6,5,4,0	15
	37	11,9,8,7,5,3,2,1,0	2
	65	12,8,7,6,5,4,0	4
	65	13,12,9,4,1,0	2

FIG: 12

Type of error-patterns	Maximum message length	Minimum redundancy cyclic code	Number of equivalent solutions
Problem 2			
e = 3	9	8,5,4,3,2,1,0	29
	11	9,4,5,3,2,1,0	20
	15	10,8,5,4,2,1,0	2
	23	11,9,7,6,5,1,0	2
	23	12,10,7,4,3,2,1,0	2
	25	13,10,8,6,3,1,0	2
Problem 2			
e = 4	10	9,7,6,5,4,3,2,1,0	9
	11	10,7,6,5,4,3,2,1,0	46
	12	11,7,6,5,4,3,2,1,0	176
	14	12,11,9,7,5,3,2,1,0	35
	15	13,10,8,6,4,3,2,1,0	225
Problem 3			
b = 2	10	8,6,4,2,0	5
	12	9,6,4,3,2,0	10
	15	10,6,4,2,1,0	5
	18	11,7,4,2,1,0	14
	25	12,10,9,8,3,1,0	2
	31	13,10,9,7,5,4,1,0	4
Problem 3			
b = 3	15	12,9,6,3,0	19
	18	13,10,9,8,7,5,4,3,1,0	2
Problem 3			
$b_1 = 1$	11	9,7,6,4,3,1,0	4

FIG: 13

Type of error-patterns	Maximum message length	Minimum redundancy cyclic code	Number of equivalent solutions
Problem 3			
$b_2 = 3$	12	10,7,6,4,3,1,0	39
	15	11,8,7,5,3,2,1,0	4
	21	12,10,9,6,4,1,0	4
	22	13,9,6,5,4,3,2,0	2
Problem 4			
B = 8	12	9,6,4,3,2,0	10
b = 2	16	10,7,4,2,1,0	4
	31	11,9,5,3,1,0	2
	56	12,8,6,2,1,0	4
	120	13,9,7,6,5,2,1,0	2
Problem 4			
B = 11			
b = 2	58	13,11,8,7,6,5,4,1,0	2
	15	10,6,4,2,1,0	8
	20	11,7,5,4,3,2,0	6
	35	12,11,7,6,5,3,1,0	2
	58	13,11,8,7,6,5,4,1,0	2
Problem 4			
B = 15	38	13,10,9,8,6,5,3,2,1,0	2
b = 2	15	10,6,4,2,1,0	8
	18	11,7,4,2,1,0	14
	25	12,10,9,8,3,1,0	2
	38	13,10,9,8,6,5,3,2,1,0	2

FIG: 14

Type of error-patterns	Maximum message length	Minimum redundancy cyclic code	Number of equivalent solutions
Problem 4	15	12,9,6,3,0	22
B = 9			
b = 3	21	13,10,9,8,7,5,4,2,0	3

FIG: 15