VARIABLE-LENGTH ENCODING

By

S. Bende

Department of Mathematics, Technical University, Budapest

(Received June 24, 1969)

Presented by Prof. Dr. D. Králik

Introduction

This paper gives a theoretical treatment of several properties which describe certain variable-length encodings likely to lend themselves for the storage or transmission of information. An optimum encoding is sought for by which every possible information can be encoded with the minimum possible of symbols, that is, using shorter sequences (code-words) for the more frequent messages and longer sequences for the less frequent ones without separating them by commas. This kind of encoding is called variable-length comma-free encoding. The restriction that none of the sequence assigned to a code-word is allowed to serve as the initial sequence of another code-word, defines the encoding as to have the prefix property [1, 2].

All the encodings dealt with in the present paper are of the prefix type.

1. Fundamental concepts, terminology

Let be given a set $\chi = \{\chi_1, \chi_2, \ldots, \chi_q\}$ with a finite number $q \geq 2$ of elements, usually called alphabet. The sequences $\chi_i, \chi_{i_1} \ldots \chi_{i_2}$ constructed from the elements (letters) of χ are called words. The words are denoted by A, B, ... etc. The empty word without any letter is denoted by O, and the empty set by Θ.

The number $\lambda = \lambda(A)$ of letters in a word $A = \chi_{A_1} \chi_{A_2} \ldots \chi_{A_{\lambda(A)}}$ is to be understood as the length of A, its initial sequence of letters O; χ_{A_1}; ... ; A is called the prefix of A.

If A is a prefix of B, we write $A \preceq B$ or $A \prec B$. The symbol $\preceq$ indicates obviously a reflexive, antisymmetrical, transitive relation between the words.

The set of words forms a cancellative semigroup, its operation is the juxtaposition of the words.

A and B are words not necessarily of the same length, their distance $\varrho(A; B)$ is equal to the number of corresponding pairs χ_{A_i}, χ_{B_i}; $i = 1, \ldots, \mathrm{Min}\,\{\lambda(A), \lambda(B)\}$ for which $\chi_{A_i} \neq \chi_{B_i}$.

For the distance thus defined

$$\varrho(A; A) = 0$$
$$\varrho(A; B) = \varrho(B; A)$$

always hold for arbitrary A, B, since the triangle axiom

$$\varrho(A; B) + \varrho(B; C) \geq \varrho(A; C)$$

holds with the restriction that $\lambda(B) \geq \mathrm{Min}\,\{\lambda(A); \lambda(C)\}$. It is easy to see that $\varrho(A; B) = 0$ holds if and only if A and B are comparable with respect to the relation $\preceq$. If for A and B $\varrho(A; B) > 0$ holds they will be called disjoint.

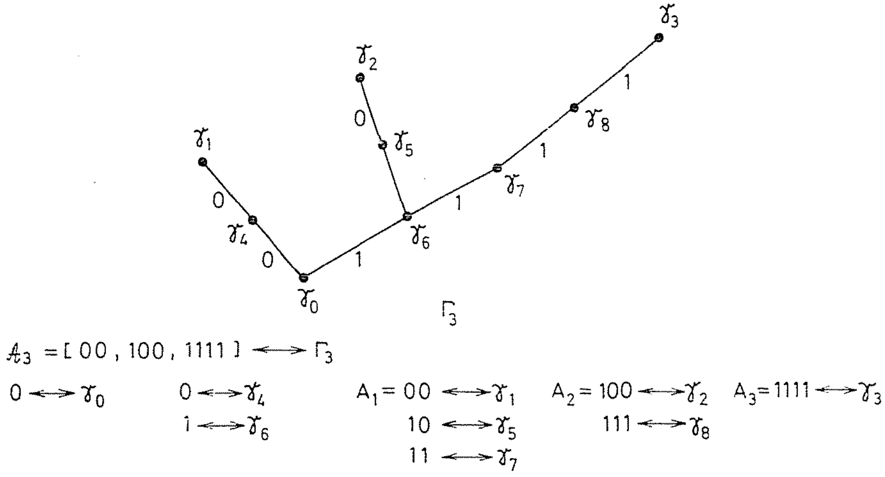


Fig. 1

An n-tuple of distinct words A_i $(i = 1, 2, \ldots, n)$ is called a code and it will be denoted by $\mathcal{A}_n = [A_1, \ldots, A_n]$. If the length of each code-word, with $i = 1, 2, \ldots, (n - 1)$ is such that $\lambda(A_i) \leq \lambda(A_{i+1})$ holds, the code (with this property) will be denoted by $\bar{\mathcal{A}}_n$.

The distance of an arbitrary word W from $\mathcal{A}_n$ is defined by $\mathrm{Min}_i\,\{\varrho(W; A_i); A_i \in \mathcal{A}_n\}$ and denoted by $\varrho(W; \mathcal{A}_n)$.

An arbitrary code $\mathcal{A}_n$ can be represented as a rooted tree with n end points and whose edges are labelled by the letters of alphabet χ.

There is a one-to-one correspondence between all prefixes of $\mathcal{A}_n$ and all the vertices of the tree Γ_n with a root γ_0.

The representation is illustrated by the following example; $\mathcal{A}_3 = [00, 100, 111]$ (Fig. 1).

It is obvious that the degree of $\gamma_0 \in \Gamma_n$ is at most q any other vertex is at most $q + 1$. It is easy to see that any Γ_n of the type given above with appropriately labelled edges represents a code $\mathcal{A}_n$.

2. Theorems and proofs

The following well-known theorem will be frequently used throughout this paper: A code $\mathcal{A}_n$ with the prefix property containing $n \geq 2$ words can be constructed from the letters of the alphabet $\chi = \{\chi_1, \ldots, \chi_q\}$, $q \geq 2$ if and only if the length of every code-word satisfy Szilárd's inequality

$$\sum_{A_i \in \mathcal{A}_n} q^{-\lambda(A_i)} \leq 1 .$$

If the equality

$$\sum_{A_i \in \mathcal{A}_n} q^{-\lambda(A_i)} = 1 \tag{1}$$

holds, $\mathcal{A}_n$ is called exhausted. By the next theorem it will be exhibited that the exhaustion of a code can be defined by its other properties.

In this paper an arbitrary code is to be understood with the prefix property.

Theorem 2.1. The following statements are equivalent

a) $$\sum_{A_i \in \mathcal{A}_n} q^{-\lambda(A_i)} = 1 .$$

b) No code $\mathcal{A}_m$ exists for which $\mathcal{A}_n \subset \mathcal{A}_m$, $(n < m)$ holds.

c) For arbitrary word w (whose letters are the elements of alphabet χ) $\varrho(w; \mathcal{A}_n) = 0$ holds.

Proof: Condition b) is a consequence of a). Suppose that a code $\mathcal{A}_m$ exists for which $\mathcal{A}_n \subset \mathcal{A}_m$. This implies that

$$\sum_{A_i \in \mathcal{A}_n} q^{-\lambda(A_i)} < \sum_{A_i \in \mathcal{A}_m} q^{-\lambda(A_i)} \leq 1$$

it contradicts to condition a). Condition c) is a consequence of b). Suppose that a word w exists, for which $\varrho(w; \mathcal{A}_n) > 0$. Then none of the A_i is a prefix of w and the union of $\mathcal{A}_n$ and w is a code $\mathcal{A}_{n+1} = \mathcal{A}_n \cup w$ with the property $\mathcal{A}_n \subset \subset \mathcal{A}_{n+1}$ which is a contradiction to condition b). Condition a) is a consequence of c). Suppose that

$$\sum_{A_i \in \mathcal{A}_n} \mathrm{q}^{-\lambda(A_i)} < 1.$$

Consider the set $\mathcal{V}$ consisting of all the words of length l, $l > \operatorname*{Max}_i \{\lambda(A_i); A_i \in \mathcal{A}_n\}$ whose letters are in χ (their number is q^l). All the elements of $\mathcal{V}$ whose prefix is A_i form a subset of $\mathcal{V}$ denoted by $\mathcal{C}(A_i)$. The number of elements in $\mathcal{C}(A_i)$ is $q^{l-\lambda(A_i)}$.

* The inequality of the form (1) has been published first by Leo Szilárd in his paper on the Maxwellian demon (L. Szilárd: Über die Entropieverminderung in einem thermodynamischen System bei Eingriff intelligenter Wesen. Z. Phys. 1929. 840—856.).

Since

$$\mathcal{C}(A_i) \cap \mathcal{C}(A_j) = \Theta; \quad i \neq j; \quad A_i, A_j \in \mathcal{A}_n$$

the number of elements in the set $\mathcal{C} = \bigcup_{i=1}^{n} C(A_i)$ is

$$\sum_{A_i \in \mathcal{A}_n} q^{l-\lambda(A_i)}. \text{ Now } \sum_{A_i \in \mathcal{A}_n} q^{-\lambda(A_i)} < 1 \text{ implies that } \sum_{A_i \in \mathcal{A}_n} q^{l-\lambda(A_i)} < q^l.$$

Hence $\mathcal{V} \setminus \mathcal{C}$ is not empty. For an arbitrary $W \in \mathcal{V} \setminus \mathcal{C}$ we have $\varrho(W; \mathcal{A}_n) > 0$ which contradicts to condition c).

Remarks The exhausted code with the minimum number of elements based on the alphabet χ is denoted by ${}_l\mathfrak{I}_q = [\chi_1, \ldots, \chi_q]$. Each code-word of $\mathfrak{I}_q$ is of length 1.

$\mathcal{V}_q = [V_1, \ldots, V_{q^l}]$ denotes the code with the maximum number of elements (based on the alphabet χ). In this code each code-word is of length l.

Theorem 2.2. If $\mathcal{A}_n$ is exhausted and $A_r \in \mathcal{A}_n$; $\lambda(A_r) = \operatorname{Max}_i \{\lambda(A_i); A_i \in \mathcal{A}_n\}$ is an element with the prefix A of length $\lambda(A_r) - 1$, then the words $A\,\chi_1, A\,\chi_2, \ldots, A\,\chi_q$ are the elements of $\mathcal{A}_n$.

Proof: Since $\lambda(A\,\chi_j) = \lambda(A_r)$ holds, $A\,\chi_j$ $(j = 1, \ldots, q)$ is not a prefix of any elements of $\mathcal{A}_n$. On the other hand there is not such A_i; $\lambda(A_i) < \lambda(A\,\chi_j) = \lambda(A_r)$ which is the prefix of $A\,\chi_j$ $(j = 1, \ldots, q)$. since it would imply that A_i were the prefix of A_r too, and that is impossible for code words being mutually disjoint. By theorem 2.1.c. $\varrho(A\,\chi_j; \mathcal{A}_n) = 0$ holds which implies $A\,\chi_j \in \mathcal{A}_n$, $(j = 1, \ldots, q)$.

Corollary. In an exhausted code the number of code-words with maximum length is a multiple of q.

Theorem 2.3. If $\mathcal{A}_n = [A_1, \ldots, A_n]$ and $\mathcal{B}_m = [B_1, \ldots, B_m]$ are codes, then $\mathcal{A}_n \times \mathcal{B}_m = [A_1, \ldots, A_{n-1}, A_nB_1, A_nB_2, \ldots, A_nB_m]$ is a code too.

The latter will be exhausted if $\mathcal{A}_n$ and $\mathcal{B}_m$ are exhausted.

Proof: For $i = 1, 2, \ldots, (n-1)$ and $j = 1, 2, \ldots, m$ we have $\varrho(A_i; A_nB_j) \geq \varrho(A_i; A_n) > 0$, and for $k \neq j$ we have $\varrho(A_nB_k; A_nB_j) = \varrho(A_n; A_n) + \varrho(B_k; B_j) > 0$, and so any pair of words of $\mathcal{A}_n \times \mathcal{B}_m$ is disjoint. If $\mathcal{A}_n$ and $\mathcal{B}_m$ are exhausted, we have

$$\sum_{i=1}^{n} q^{-\lambda(A_i)} = 1, \quad \sum_{i=1}^{m} q^{-\lambda(B_i)} = 1.$$

Hence, denoting $\mathcal{C}_{n+m-1} = \mathcal{A}_n \times \mathcal{B}_m$,

$$\sum_{C \in \mathcal{C}_{n+m-1}} q^{-\lambda(C)} = \sum_{i=1}^{n-1} q^{-\lambda(A_i)} + q^{-\lambda(A_n)} \cdot \sum_{i=1}^{m} q^{-\lambda(B_i)} = \sum_{i=1}^{n} q^{-\lambda(A_i)} = 1$$

indicating that $\mathcal{C}_{n+m-1} = \mathcal{A}_n \times \mathcal{B}_m$ is exhausted. The dual statement of theorem 2.3 is

Theorem 2.4. If $n > k \geq 2$, and all the code words of $\mathcal{A}_n$ with the common prefix A of maximum length $\lambda(A) \neq 0$ are given by the sequence

$$A_{n-k+1} = AB_1, \quad A_{n-k+2} = AB_2, \ldots, \quad A_n = AB_k,$$

then

$$\mathcal{A}_n = [A_1, A_2, \ldots, A_{n-k}, AB_1, AB_2, \ldots, AB_k] = \mathcal{A}_{n-k+1} \times \mathcal{B}_k.$$

If $\mathcal{A}_n$ is exhausted, both $\mathcal{A}_{n-k+1}$ and $\mathcal{B}_k$ are exhausted too.

Proof. By supposition, none of the words $A_1, A_2, \ldots, A_{n-k}$ has the prefix A, or is a prefix of A. By the transitivity of the relation $\preceq$, such a code word would be namely the prefix of the words $AB_1, AB_2, \ldots, AB_k$, too, which is impossible since each pair of the code words is disjoint. It follows that the pairs of words of $A_1, A_2, \ldots, A_{n-k}, A$ are disjoint and therefore form a code $\mathcal{A}_{n-k+1} = [A_1, \ldots, A_{n-k}, A]$.

It follows from the fact that each pair of the code-words of $\mathcal{A}_n$ is disjoint and by the identity

$$\varrho(A_{n-k+i}; A_{n-k+j}) = \varrho(AB_i; AB_j) = \varrho(B_i; B_j)$$

that the pairs of words $B_1, B_2, \ldots, B_k$ are disjoint and form a code $\mathcal{B}_k = [B_1, B_2, \ldots, B_k]$. If $\mathcal{A}_n$ is exhausted,

$$1 = \sum_{A_i \in \mathcal{A}_n} q^{-\lambda(A_i)} = \sum_{i=1}^{n-k} q^{-\lambda(A_i)} + q^{-\lambda(A)} \cdot \sum_{B_i \in \mathcal{B}_k} q^{-\lambda(B_i)} \leq \sum_{A_i \in \mathcal{A}_{n-k+1}} q^{-\lambda(A_i)} \leq 1$$

hence

$$\sum_{A_i \in \mathcal{A}_{n-k+1}} q^{-\lambda(A_i)} = 1$$

and also

$$\sum_{B_i \in \mathcal{B}_k} q^{-\lambda(B_i)} = 1\,,$$

which is sufficient for $\mathcal{A}_{n-k+1}$ and $\mathcal{B}_k$ to be exhausted.

By Theorem 2.2. we get:

Corollary. An exhausted code $\bar{\mathcal{A}}_n$ $(n > q)$ can be written in the form $\bar{\mathcal{A}}_n = \mathcal{A}_{n-q+1} \times \mathfrak{J}_q$, where $\mathcal{A}_{n-q+1}$ is an exhausted code.

As an example to theorem 2.4 let us consider an exhausted code represented by

$$\bar{\mathcal{A}}_6 = [00, 01, 10, 110, 1110, 1111]$$
$$\bar{\mathcal{A}}_6 = [00, 01, 1] \times [0, 10, 110, 111]$$
$$\bar{\mathcal{A}}_6 = [00, 01, 10, 11] \times [0, 10, 11]$$
$$\bar{\mathcal{A}}_6 = [00, 01, 10, 110, 111] \times [0, 1] = [00, 01, 10, 110, 111] \times \mathfrak{J}_2.$$

Theorem 2.5. If $\mathcal{A}_n$ is exhausted, the number of its different prefixes is $\dfrac{nq-1}{q-1}$.

Proof: It is clear that the number of the prefixes of $\mathcal{A}_n$ is equal to the number of vertices of the tree Γ_n representing $\mathcal{A}_n$. It can be easily seen that if $\mathcal{A}_n$ is exhausted, then except the n end-points, precisely q directed edges start from each vertex, and except the starting point γ_0 to which no edge is directed, just one edge runs to each vertex. If the number of vertices is σ the number of edges starting from the vertices of Γ_n is $(\sigma - n)\,q$. Since in each tree there is always one vertex more than edges, $(\sigma - n)\,q = \sigma - 1$, thus $\sigma = \dfrac{nq-1}{q-1}$ holds. In [1] the same result for the binary case ($q = 2$) is given. The following result is known (see e.g. [7]).

Theorem 2.6. The necessary and sufficient condition for the existence of an exhausted code with n words (constructed from the letters of the alphabet $\chi = \{\chi_1, \ldots, \chi_q\}$, $(q \geq 2)$) is that n is an integer of the form $r(q-1)+1$, $r \geq 1$.

Proof: The necessity of the condition follows from theorem 2.5.

For an exhausted code we have $nq - 1 \equiv 0 \pmod{q-1}$ and all positive solutions of this congruence are the integers $n_r = r(q-1)+1$, when $r = 0, 1, 2, \ldots$ The sufficiency may be proved by induction as follows. If $r = 1$ by remark 1 of Theorem 2.1 the code $\mathfrak{I}_q = \mathcal{A}_{n_1}$ is exhausted. Suppose that $\mathcal{A}_{n_{r-1}}$, $r \geq 1$ is exhausted, then, by Theorem 2.3, the code $\mathcal{A}_{n_r} = \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_q$ is exhausted too.

Corollary. If $q = 2$, for any natural number $n \geq 2$ there exists an exhausted code with n elements. In the following, n_r always denotes the integer $(rq-1)+1$.

If $q > 2$ (non-binary encoding) and v words $(1 \leq v \leq q-2)$ are omitted from the code-words of maximum length of the exhausted code $\mathcal{A}_{n_r}$ $(r \geq 1)$, the code $\mathcal{A}_{n_r - v}$ thus obtained having $n_r - v$ code words is called quasi-exhausted. This follows from the corollary of theorem 2.4.

Theorem 2.7. The quasi-exhausted code $\bar{\mathcal{A}}_{n_r - v}$ $(1 \leq v \leq q-2,\ r > 1)$ can be constructed in the form

$$\bar{\mathcal{A}}_{n_r - v} = [A_1, \ldots, A_{n_r - q}, A\chi_1, A\chi_2, \ldots, A\chi_{q-v}] =$$
$$= [A_1, \ldots, A_{n_r - q}, A] \times [\chi_1, \chi_2, \ldots, \chi_{q-v}] = \mathcal{A}_{n_{n-1}} \times \mathfrak{I}_{q-v}$$

where $\mathcal{A}_{n_{r-1}}$ is an exhausted code.

Remark. Since $q - v \geq 2$ and $\mathfrak{I}_{q-v} = [\chi_1, \ldots, \chi_{q-v}]$ is quasi-exhausted, for any integer $n \geq 2$ there exists an exhausted or quasi-exhausted code with n code-words (constructed from the letters of the alphabet χ).

Theorem 2.8. a) If $\mathcal{A}_n$ is quasi-exhausted, then for an arbitrary word W with $\lambda(W) < \operatorname*{Max}_i \{\lambda(A_i);\ A_i \in \mathcal{A}_n\}$ we have $\varrho(W; \mathcal{A}_n) = 0$.

b) If for a code $\mathcal{A}_n$ we have for every word W with $\lambda(W) < \operatorname*{Max}_i \{\lambda(A_i);$ $A_i \in \mathcal{A}_n\}$ that $\varrho(W; \mathcal{A}_n) = 0$, then $\mathcal{A}_n$ is exhausted or quasi-exhausted.

Proof: Both statements of theorem 2.8 are trivial for $n \leq q$. Consider $n > q$. Let us denote by $\bar{\mathcal{A}}_n$ the code obtained by arranging the word lengths of $\mathcal{A}_n$ into a monotonically non decreasing sequence. Assuming $\mathcal{A}_n$ to be quasi-exhausted, applying Theorem 2.7 with $n_r - \nu$, we get $\bar{\mathcal{A}}_n = \mathcal{A}_{n_{r-1}} \times$ $\times\, \mathfrak{J}_{q-\nu}$. Now we have for each word W with $\lambda(W) < \operatorname*{Max}_i \{\lambda(A_i);\ A_i \in \mathcal{A}_n\}$ the identity

$$\varrho(W; \mathcal{A}_n) = \varrho(W; \bar{\mathcal{A}}_n) = \varrho(W; \mathcal{A}_{n_{r-1}})$$

and since $\mathcal{A}_{n_{r-1}}$ is exhausted the statement a) follows by Theorem 2.1.

Let us assume statement b) to be proved i.e. for each word W, with $\lambda(W) < \operatorname*{Max}_i \{\lambda(A_i);\ A_i \in \mathcal{A}_n\}$ the distance $\varrho(W; \mathcal{A}_n) = 0$. Consequently, no word of shorter length exists than $\operatorname*{Max}_i \{\lambda(A_i);\ A_i \in \mathcal{A}_n\}$ which is disjoint from the code-words of $\mathcal{A}_n$. Thus $\mathcal{A}_n$ is either exhausted or such that maximum $q - 2$ words of length $\operatorname*{Max}_i \{\lambda(A_i);\ A_i \in \mathcal{A}_n\}$ with are disjoint from the code-words of $\mathcal{A}_n$, i.e. $\mathcal{A}_n$ is quasi-exhausted.

An algorithm for the construction of codes will be presented. Let be given $\lambda_1 < \lambda_2 < \ldots < \lambda_r$ the lengths of the elements of $\mathcal{A}_n$, and $s_l \geq 1$ $(l = 1, \ldots, r)$ the number of elements of length λ_l, obviously

$$\sum_{l=1}^{r} s_l = n \text{ holds.}$$

$$\sum_{l=1}^{r} s_l q^{-\lambda_l} \leq 1$$

is supposed to hold.

Let us give n rational numbers $\alpha(l; k)$ $l = 1, 2, \ldots, r$ and $k = 1, 2, \ldots, s_l$ as follows if $l = 1$, $\alpha(1; k) = (k - 1)\, q^{-\lambda_1}$ $(k = 1, \ldots, s_1)$ and if $l > 1$

$$\alpha(l; k) = (k - 1)\, q^{-\lambda_l} + \sum_{i=1}^{l-1} s_i\, q^{-\lambda_i}, \quad (k = 1, 2, \ldots, s_l)$$

By this definition it is obvious that

Lemma 2.1. (i) $\alpha(1; 1) = 0$

(ii) $\alpha(l; k + 1) = \alpha(l; k) + q^{-\lambda_l}, \quad k = 1, 2, \ldots, (s_l - 1)$

(iii) $\alpha(l + 1, 1) = \alpha(l; s_l) + q^{-\lambda_l}, \quad l = 1, 2, \ldots, (r - 1)$

(iv) $\alpha(l; k) < 1$

Let δ_i be the digits of the q-nary number system, then

Lemma 2.2. The q-nary fractional form of $\alpha(l; k)$ contains at most λ_l non-zero digits i.e.

$$\alpha(l; k) = \sum_{i=1}^{\lambda_l} \delta_i q^{-i} = 0, \delta_1 \delta_2 \ldots \delta_{\lambda_l}.$$

Proof: For $\alpha(1; 1) = 0$, the statement is trivial, for any other $\alpha(l; k)$ it is easy to see using the inequality $q^{-\lambda_l} \leq \alpha(l; k) < 1$ implied by (ii), (iii), (iv) of lemma 2.1.

Lemma 2 3. In the fractional forms of two different numbers, namely $\alpha(l; k) = 0, \delta_1\delta_2 \ldots \delta_{\lambda_l}$ and $\alpha(l'; k') = 0, \delta'_1\delta'_2 \ldots \delta'_{\lambda_{l'}}$, it does not hold for each $i = 1, 2, \ldots, \text{Min}\,\{\lambda_l; \lambda_{l'}\}$ that $\delta_i = \delta'_i$.

Proof: $\alpha(l; k)$ and $\alpha(l'; k')$ are different if at least either $l = l'$ or $k = k'$ does not hold. Thus, without loss of generality, let k, k' be arbitrary if $l > l'$ and let us assume, contrary to above statement, that for each $i = 1, 2, \ldots, \lambda_{l'}$ $\delta_i = \delta'_i$ holds.

Since $0 < \alpha(l; k) - \alpha(l'; k') < 1$,

$$\alpha(l; k) - \alpha(l'; k') = 0,\underbrace{00 \ldots 0}_{\lambda_{l'} \text{ digits}} \delta_{\lambda_{l'}+1} \delta_{\lambda_{l'}+2} \ldots \delta_{\lambda_l}$$

holds.

This is impossible because of the inequality

$$\alpha(l;k) - \alpha(l';k') = \sum_{i=l'}^{l-1} s_i q^{-\lambda_i} + (k-1) q^{-\lambda_l} (k'-1) q^{-\lambda_{l'}} \geq q^{-\lambda_{l'}}$$

where $l \geq l'$, $k > k'$ holds.

Theorem 2.9. Considering the digits $A_{l_k} = \delta, \delta_2 \ldots \delta_{\lambda_{l'}}, \delta_{\lambda_l}$ — including any possible digit 0 at the end of the fractions — being in fractional parts of the numbers $\alpha(l; k) = 0, \delta_1\delta_2 \ldots \delta_{\lambda_l}$ the sequences A_{l_k} form a code $\mathcal{A}_n$. $\mathcal{A}_n$ has the s_l prescribed number of elements of length λ_l.

Proof: Lemma 2.2 implies that by the definition of $\mathcal{A}_n$ it has exactly s_l elements of length λ_l, where $\sum_{l=1}^{r} s_l = n$ and $s_l \geq 1$, and by lemma 2.3 the sequences A_{l_k} consist of disjoint pairs of words. Thus, according to our statement $\mathcal{A}_n$ is a code.

Remark. For algorithmic construction of binary codes see [1], [2], [6].

For sake of illustration we present the binary code constructed by means of above algorithm over the letters of the English alphabet. This is an opportunity to compare it with the Huffmann type code which is also given below (Table 1).

It may be remarked that this code is exhausted.

Table 1

Letter	Word length	Code-word	Huffmann-type code-word
Space	3	000	000
E	3	001	101
T	4	0100	0010
A	4	0101	0100
O	4	0110	0110
I	4	0111	1000
N	4	1000	1001
S	4	1001	1100
R	4	1010	1101
H	4	1011	1110
L	5	11000	01010
D	5	11001	01011
U	5	11010	11110
C	5	11011	11111
F	6	111000	001100
M	6	111001	001101
W	6	111010	001110
Y	6	111011	001111
P	6	111100	011110
G	6	111101	011101
B	6	111110	011111
V	7	1111110	0111000
K	8	11111110	01110010
X	10	1111111100	0111001100
J	10	1111111101	0111001110
Q	10	1111111110	0111001101
Z	10	1111111111	0111001111

3. Minimum redundancy encoding

Let us assume the sequence of informations $\mathfrak{a}i \in \mathfrak{A}_n$ of the set $\mathfrak{A}_n = \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n\}$ with $n \geq 2$ elements to occur in the sequences $\mathfrak{a}_{i1}\mathfrak{a}_{i2}\ldots$ with the probability

$$p_i = p(\mathfrak{a}_1), p_2 = p(\mathfrak{a}_2), \ldots, p_n = p(\mathfrak{a}_n); \sum_{i=1}^{n} p_i = 1 .$$

The code $\mathcal{A}_n$ over the alphabet $\chi = \{\chi_1, \dots, \chi_q\}$ will be called a minimum redundancy code with respect to the probability distribution $P_n = \{p_1, p_2, \dots \dots, p_n\}$ briefly, P_n-minimized, if for any code $\mathcal{A}'_n$ over the alphabet χ we have

$$M[P_n; \mathcal{A}_n] = \sum_{A_i \in \mathcal{A}_n} p_i \lambda(A_i) \leq M[P_n; \mathcal{A}'_n] = \sum_{A'_i \in \mathcal{A}'_n} p_i \lambda(A'_i).$$

The necessary and sufficient condition of minimum redundancy encoding will be determined by six lemmas. In the non binary case let $n_r = r(q-1)+1$ and

$$n = \begin{cases} n_r, & \text{if } \mathcal{A}_n \text{ is exhausted} \\ n_r - \nu, & \text{if } \mathcal{A}_n \text{ is quasi-exhausted} \end{cases}$$

where $\mathcal{A}_n = \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_q$

$$q' = \begin{cases} q, & \text{if } \mathcal{A}_n \text{ is exhausted} \\ q - \nu, & \text{if } \mathcal{A}_n \text{ is quasi-exhausted.} \end{cases}$$

Using the former notations the corollary of theorems 2.4 and 2.7 implies

Lemma 3.1. The exhausted or quasi-exhausted code $\bar{\mathcal{A}}_n$ with $r > 1$ can be constructed in the form $\bar{\mathcal{A}}_n = \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_{q'}$, where $\mathcal{A}_{n_{r-1}}$ is the exhausted code and $\mathfrak{I}_{q'} = \{\chi_1, \dots, \chi_{q'}\}$ $(q' \geq 2)$.

Lemma 3.2. Let an $\mathcal{A}_n = \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_{q'}$ $(r > 1)$ be exhausted or quasi-exhausted code and $P_n = \{p_1, p_2, \dots, p_n\}$ the probability distribution. Then for

$$P_{n_{r-1}} = \left\{p_1, \dots, p_{n-q'}, \sum_{i=1}^{q'} p_{n-q'+i}\right\}$$

the identity

$$M[P_n; \mathcal{A}_n] = M[P_{n_{r-1}}, \mathcal{A}_{n_{r-1}}] + \sum_{i=1}^{q'} p_{n-q'+i}$$

holds.

Proof: Since

$$\begin{aligned} \mathcal{A}_n &= \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_{q'} = [A_1, \dots, A_{n_{r-1}}] \times \mathfrak{I}_{q'} = \\ &= [A_1, A_2, \dots, A_{n_{r-1}}, A_{n_{r-1}}\chi_1, A_{n_{r-1}}\chi_2, \dots, A_{n_{r-1}}\chi_{q'}] \end{aligned}$$

and $n - q' + 1 = n_{r-1}$ it is easy to see that

$$\begin{aligned} M[P_n; \mathcal{A}_n] &= \sum_{i=1}^{n-q'} p_i \lambda(A_i) + \{\lambda(A_{n_{r-1}}) + 1\} \cdot \sum_{i=1}^{q'} p_{n-q'+i} = \\ &= M[P_{n_{r-1}}; \mathcal{A}_{n_{r-1}}] + \sum_{i=1}^{q'} p_{n-q'+i} \end{aligned}$$

holds.

Lemma 3.3. If the code $\mathcal{A}_n$ is P_n-minimized, then it is exhausted or quasi-exhausted.

Proof: If, contrary to the above statement, the P_n-minimized code $\mathcal{A}_n$ is not exhausted or quasi-exhausted, by theorem 2.8 a word W; $\lambda(W) < \operatorname*{Max}_i \{\lambda(A_i); A_i \in \mathcal{A}_n\}$ exist for which $\varrho(W; \mathcal{A}_n) > 0$. If a code-word of maximum length in $\mathcal{A}_n$ is replaced by W, for the code obtained $\mathcal{A}'_n$, contrary to the fact that $\mathcal{A}_n$ is P_n-minimized,

$$M[P_n; \mathcal{A}'_n] < M[P_n; \mathcal{A}_n]$$

holds. $\bar{P}_n$ denotes a probability distribution P_n whose probabilities p_i $(i = 1, \ldots, n-1)$ are arranged into monotonically non-increasing sequence i.e. $p_i \geq p_{i+1}$.

Lemma 3.4. If $\mathcal{A}_n$ is $\bar{P}_n$-minimized, then with $A_i \in \mathcal{A}_n$ $\lambda(A_1) \leq \lambda(A_2) \leq \leq \ldots \leq \lambda(A_n)$.

Proof: Assume that contrary to our statement, there exist such A_i and A_j $(1 \leq i < j \leq n)$ that $\lambda(A_i) > \lambda(A_j)$ holds. By exchanging in $\mathcal{A}_n$ the word A_i and A_j, we get the code $\mathcal{A}'_n$ with $A'_i = A_j$; $A'_j = A_i$ $(A'_i, A'_j \in \mathcal{A}'_n)$ and because of the inequality $p_i\,\lambda(A'_i) + p_j\,\lambda(A'_j) = p_i\,\lambda(A_j) + p_j\,\lambda(A_i) < p_i\,\lambda(A_i) + p_j\,\lambda(A_j)$ holding for $p_i \geq p_j > 0$ and $\lambda(A_i) > \lambda(A_j) > 0$ we find, contrary to the fact that $\mathcal{A}_n$ is $\bar{P}_n$-minimized, that

$$M[\bar{P}_n; \mathcal{A}'_n] < M[\bar{P}_n; \mathcal{A}_n].$$

Lemma 3.5. If the code $\bar{\mathcal{A}}_n = \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_{q'}$, $(r > 1)$ is exhausted or quasi-exhausted and $\bar{P}_n$-minimized, then the exhausted code $\mathcal{A}_{n_{r-1}}$ is $P_{n_{r-1}}$-minimized with respect to the probability distribution

$$P_{n_{r-1}} = \left\{p_1, p_2, \ldots, p_{n-q'}, \sum_{i=1}^{q'} p_{n-q'+i}\right\}$$

which may be obtained by summing over the q' terms of $\bar{P}_n$.

Proof: Assume that, contrary to our statement, $\mathcal{A}_{n_{r-1}}$ is not $P_{n_{r-1}}$-minimized. Since for given n_{r-1} the equation $\sum\limits_{i=1}^{n_{r-1}} q^{-\lambda_i} = 1$ has only a finite number of solutions in the positive integers $\lambda_1, \lambda_2, \ldots, \lambda_{n_{r-1}}$ this implies that there is a finite number of exhausted codes consisting of a sequence of n_{r-1} words. Thus, by lemma 3.3, there exists an exhausted code $\mathfrak{B}_{n_{r-1}}$ which is $P_{n_{r-1}}$-minimized and for which by our indirect assumption

$$M[P_{n_{r-1}}; \mathfrak{B}_{n_{r-1}}] < M[P_{n_{r-1}}; \mathcal{A}_{n_{r-1}}]$$

holds (i).

Consider the code $\mathfrak{B}_n = \mathfrak{B}_{n_{r-1}} \times \mathfrak{I}_{q'}$; making use of Lemma 3.2, one can obtain by the inequality (i),

$$M[\bar{P}_n; \mathcal{B}_n] = M[P_{n_{r-1}}; \mathcal{B}_{n_{r-1}}] + \sum_{i=1}^{q'} p_{n-q'+i} <$$
$$< M[P_{n_{r-1}}; \mathcal{A}_{n_{r-1}}] + \sum_{i=1}^{q'} p_{n-q'+i} = M[\bar{P}_n; \mathcal{A}_n]$$

contrary to the fact that $\mathcal{A}_n$ is $\bar{P}_n$-minimized.

Lemma 3.6. Let be

$$\bar{P}_{n_{r-1}} = \{p_1 \geq \dots \geq p_{s-1} > p_s \geq {}_{s+1} \geq \dots \geq p_{n_{r-1}}\}$$

and $\mathcal{A}_{n_{r-1}} = [A_1, A_2, \dots, A_{n_{r-1}}]$ $\bar{P}_{n_{r-1}}$-minimized. Moreover be $p_s = p_{s_1} + p_{s_2} + \dots + p_{s_{q'}}$ such a partition of $p_s \in \bar{P}_{n_{r-1}} (p_{s-1} > p_s)$ for which

$$\bar{P}_n = \{p_1 \geq \dots \geq p_{s-1} > p_{s+1} \geq \dots \geq p_{n_{r-1}} \geq p_{s_1} \geq p_{s_2} \geq \dots \geq p_{s_{q'}}\}$$

then it holds for the code

$$\mathcal{A}_n = [A_1, \dots, A_{s-1}, A_{s+1}, \dots, A_{n_{r-1}}, A_s] \times \mathfrak{I}_{q'}; (A_i \in \mathcal{A}_{n_{r-1}})$$

that it is $\bar{P}_n$-minimized.

Proof: Assume, contrary to our statement, that $\mathcal{A}_n$ is not $\bar{P}_n$-minimized. In the proof of Lemma 3.5 it has been shown that for given n, the number of exhausted codes is finite, thus, for given n, the number of quasi-exhausted codes constructed over a set of $n - \nu$ words is finite. Hence, Lemmas 3.3 and 3.4 imply that a $\bar{\mathcal{B}}_n$ code exists which is $\bar{P}_n$-minimized and because of our indirect assumption, we have

$$M[\bar{P}_n; \bar{\mathcal{B}}_n] < M[\bar{P}_n; \mathcal{A}_n]. \qquad \text{(i)}$$

Considering the probability distribution

$$P_{n_{r-1}} = \{p_1, p_2, \dots p_{s-1}, p_{s+1}, \dots, p_{n_{r-1}}, p_s\} \qquad (p_i \in \bar{P}_{n_{r-1}})$$

and by Lemma 3.2 $\bar{\mathcal{B}}_n = \mathcal{B}_{n_{r-1}} \times \mathfrak{I}_{q'}$ and $\mathcal{A}_n = \mathcal{A}_{n_{r-1}} \times \mathfrak{I}_{q'}$ where $\mathcal{A}_{n_{r-1}} = [A_1, A_2, \dots, A_{s-1}, A_{s+1}, \dots, A_{n_{r-1}}, A_s]$ inequality (i) implies, that

$$\text{(ii)} \qquad M[P_{n_{r-1}}; \mathcal{B}_{n_{r-1}}] = M[\bar{P}_n; \bar{\mathcal{B}}_n] - p_s <$$
$$< M[\bar{P}_n, \mathcal{A}_n] - p_s = M[P_{n_{r-1}}; \mathcal{A}_{n_{r-1}}]$$

If by $\mathcal{B}_{n_{r-1}} = [B_1, \dots, B_{n_{r-1}}]$ where $B_i \in \mathcal{B}_{n_{r-1}}$ one obtains

$$\mathcal{B}'_{n_{r-1}} = [B_1, \dots, B_{s-1}, B_{n_{r-1}}, B_s, \dots, B_{n_{r-1}-1}]$$

then

$$M[P_{n-r_1}; \mathcal{B}_{n_{r-1}}] = M[\bar{P}_{n_{r-1}}; \mathcal{B}'_{n_{r-1}}]$$

hence, considering that

$$M\,[P_{n_{r-1}}; \mathcal{A}_{n_{r-1}}] = M\,[\overline{P}_{n_{r-1}}; \overline{\mathcal{A}}_{n_{r-1}}]$$

using (ii) one can obtain that contrary to the fact that $\overline{\mathcal{A}}_{n_{r-1}}$, is $\overline{P}_{n_{r-1}}$-minimized,

$$M\,[\overline{P}_{n_{r-1}}; \mathfrak{B}'_{n_{r-1}}] < M\,[\overline{P}_{n_{r-1}}; \overline{\mathcal{A}}_{n_{r-1}}]$$

holds.

Corollary. Lemma 3.4 implies $\mathcal{A}_n = \overline{\mathcal{A}}_n$.

Theorem 3.1. Let be $n_k = k(q-1) + 1 - \nu$ $(k > 1;\ 0 \leq \nu < q-1)$ and

$$\overline{P}_{n_k} = \{p_1^{(k)}, p_2^{(k)}, \ldots, p_{n_k}^{(k)}\}$$

the probability distribution. Let be

$$\overline{P}_{n_r} = \{p_1^{(r)} \geq p_2^{(r)} \geq \cdots \geq p_{n_r}^{(r)}\}$$

the probability distribution for $r = k-1, k-2, \ldots, 1$ where $n_r = r(q-1) + 1$ obtained by arranging the terms of the distribution

$$P_{n_r} = \left\{ p_1^{(r+1)}, \ldots, p_{n_{r+1}}^{(r+1)}{}_{-q'}, \sum_{i=1}^{q'} p_{n_{r+1}}^{(r+1)}{}_{-q'+i} \right\}$$

into a monotonically decreasing sequence where

$$q' = \begin{cases} q-\nu, & \text{if in } \overline{P}_{n_r} \quad r = k \\ \ \ q\ \ , & \text{if in } \overline{P}_{n_r} \quad r < k\,. \end{cases}$$

The necessary and sufficient condition for the exhausted or quasi-exhausted code $\overline{\mathcal{A}}_{n_k}$ to be $\overline{P}_{n_k}$-minimized, is that the equality:

$$\text{(A.)} \qquad M\,[\overline{P}_{n_k}; \overline{\mathcal{A}}_{n_k}] = \sum_{r=1}^{k} \sum_{i=1}^{q'} p_{n_r-q'+i}^{(r)}$$

holds, where $p_{n_r-q'+i}^{(r)} \in \overline{P}_{n_r}$ $(i = 1, 2, \ldots, q')$.

Proof: The following two statements are obvious.

(i) For any probability distribution $P_q = \{p_1, \ldots, p_q\}$ the code $\mathcal{A}_q$ is P_q-minimized if and only if $\lambda(A_i) = 1$; $A_i \in \mathcal{A}_q$ holds. This implies for $\mathcal{A}_{n_1}$ if P_{n_1}-minimized,

$$M\,[P_{n_1}; \mathcal{A}_{n_1}] = M\,[P_q; \mathfrak{I}_q] = \sum_{i=1}^{q} p_i^{(1)} = 1$$

since $n_1 = q$.

(ii) If the code $\mathcal{A}_{n_r}$ is P_{n_r}-minimized the code $\overline{\mathcal{A}}_{n_r}$ consisting of its codewords arranged into a sequence of monotonically non-increasing word lengths, is $\overline{P}_{n_r}$-minimized, where $\overline{P}_{n_r}$ is the monotonically non-increasing sequence of terms in P_{n_r}.

Assuming now $\mathcal{A}_{n_k}$ to be $\overline{P}_{n_k}$-minimized, by Lemma 3.5 in the case where $r = k, k - 1, \ldots, 2$ (by (i), (ii) and Lemma 3.2) make the validity of the equations

$$M[\overline{P}_{n_k};\ \mathcal{A}_{n_k}] = M[\overline{P}_{n_{k-1}},\ \mathcal{A}_{n_{k-1}}] + \sum_{i=1}^{q-\nu} p^{(k)}_{n_k-(q-\nu)+i}$$

$$M[\overline{P}_{n_{k-1}}; \mathcal{A}_{n_{k-1}}] = M[\overline{P}_{n_{k-2}}, \mathcal{A}_{n_{k-2}}] + \sum_{i=1}^{q} p^{(k-1)}_{n_{k-1}-q+i}$$

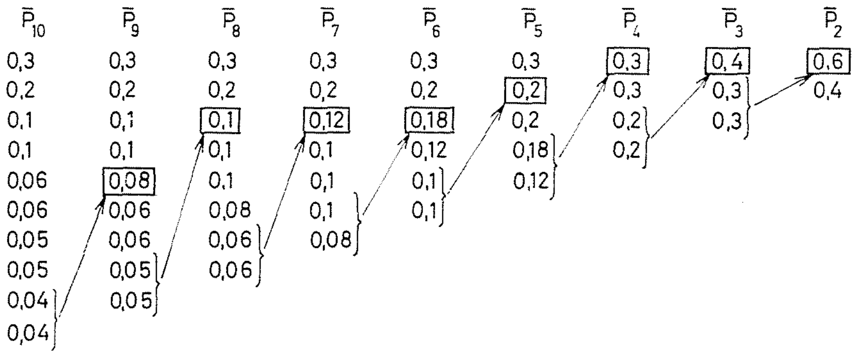
$$\vdots \qquad\qquad \vdots$$

$$M[\overline{P}_{n_2};\ \mathcal{A}_{n_2}] = M[\overline{P}_{n_1};\ \mathcal{A}_{n_1}] + \sum_{i=1}^{q} p_{n_2-q+i}$$

$$M[\overline{P}_{n_1};\ \mathcal{A}_{n_1}] = \sum_{i=1}^{q} p^{(1)}_i$$

obvious. (A) can be obtained by summing these equations.

The prove the sufficiency, let be given a probability distribution $\overline{P}_{n_k}$. One can construct from $\overline{P}_{n_k}$ the probability distributions $\overline{P}_{n_{k-1}}, \overline{P}_{n_{k-2}}, \ldots, \overline{P}_{n_1}$ for these distributions the equality (A) holds. Making use of (i) one can begin with the $\overline{P}_{n_1}$-minimized code $\mathfrak{J}_q$, to apply Lemma 3.6 and its corollary. The code $\mathcal{A}_{n_k}$ obtained by using the procedure $(k - 1)$ times is $\overline{P}_{n_k}$-minimized. Proof of the sufficiency of (A) of theorem 3.3 implies a method based on Lemma 3.6 for the construction of $\overline{P}_n$-minimized codes. The algorithm is illustrated by an example. The example is that of a binary code, the algorithm, however, works also when the code is qith q-nary alphabet. Let be given the probability distribution $\overline{P}_{10}$ and construct the table of the probability distributions $\overline{P}_9, \overline{P}_8, \ldots, \overline{P}_2$ as follows



$\overline{P}_{10}$	$\overline{P}_9$	$\overline{P}_8$	$\overline{P}_7$	$\overline{P}_6$	$\overline{P}_5$	$\overline{P}_4$	$\overline{P}_3$	$\overline{P}_2$
0,3	0,3	0,3	0,3	0,3	0,3	$\boxed{0{,}3}$	$\boxed{0{,}4}$	$\boxed{0{,}6}$
0,2	0,2	0,2	0,2	0,2	$\boxed{0{,}2}$	0,3	0,3	0,4
0,1	0,1	$\boxed{0{,}1}$	$\boxed{0{,}12}$	$\boxed{0{,}18}$	0,2	0,2	0,3	
0,1	0,1	0,1	0,1	0,12	0,18	0,2		
0,06	$\boxed{0{,}08}$	0,1	0,1	0,1	0,12			
0,06	0,06	0,08	0,1	0,1				
0,05	0,06	0,06	0,08					
0,05	0,05	0,06						
0,04	0,05							
0,04								

Beginning by the $\overline{P}_2$-minimized code $\mathcal{A}_2 = \mathfrak{J}_2 = [0, 1]$, the procedure to obtain $\mathcal{A}_{r+1}$ from $\mathcal{A}_r$ is to omit from $\mathcal{A}_r$ the word $A_i \in \mathcal{A}_r$ corresponding to p_i

in the encircled position of $\bar{P}_r$ and by putting the words $A_i\,0$, $A_i\,1$ after the remaining code words of $\bar{\mathcal{A}}_r$. By this procedure one can obtain the following $\bar{P}_r$-minimized $\bar{\mathcal{A}}_r$ codes ($r = 2, \ldots, 10$):

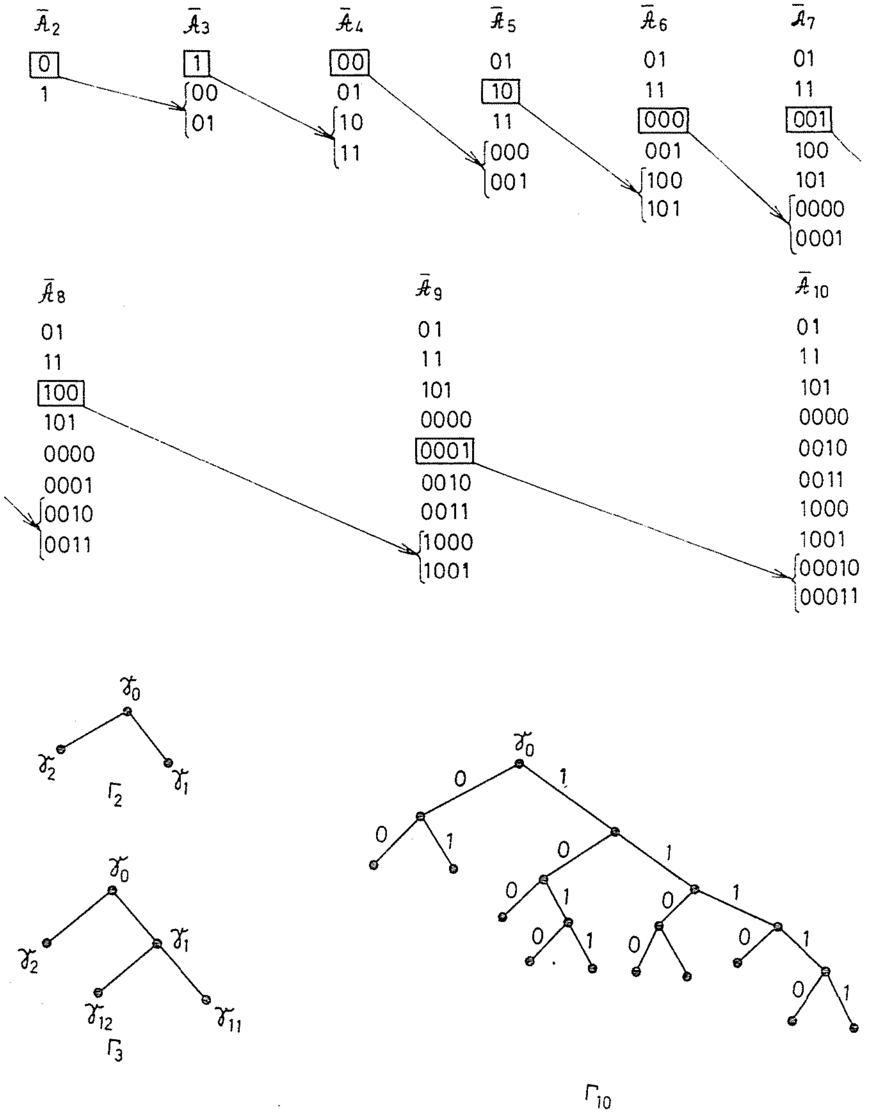

$\bar{\mathcal{A}}_2$: 0, 1
$\bar{\mathcal{A}}_3$: 1, 00, 01
$\bar{\mathcal{A}}_4$: 00, 01, 10, 11
$\bar{\mathcal{A}}_5$: 01, 10, 11, 000, 001
$\bar{\mathcal{A}}_6$: 01, 11, 000, 001, 100, 101
$\bar{\mathcal{A}}_7$: 01, 11, 001, 100, 101, 0000, 0001
$\bar{\mathcal{A}}_8$: 01, 11, 100, 101, 0000, 0001, 0010, 0011
$\bar{\mathcal{A}}_9$: 01, 11, 101, 0000, 0001, 0010, 0011, 1000, 1001
$\bar{\mathcal{A}}_{10}$: 01, 11, 101, 0000, 0010, 0011, 1000, 1001, 00010, 00011
γ_0
γ_2
γ_1
Γ_2
γ_0
γ_2
γ_1
γ_{12}
γ_{11}
Γ_3
γ_0
0
1
Γ_{10}

Fig. 2

In a graph representation, the $\bar{P}_{10}$-minimized code is obtained as follows. Let the tree Γ_2 correspond to $\bar{P}_2$ with two end points of Γ_2 corresponding to $\bar{P}_2 = \{p_1^{(2)}, p_2^{(2)}\}$. Tree Γ_3 corresponding to $\bar{P}_3$ is obtained by drawing two direct edges from the vertex $\gamma_1 \in \Gamma_2$ corresponding to the encircled element $p_1^{(2)}$ of $\bar{P}_2$. The end points of Γ_3 correspond to the elements of $\bar{P}_3$ by that the lengths of the paths running from γ_0 to the end points $\gamma_2; \gamma_{12}; \gamma_{11}$ corresponding to the elements $p_1^{(3)} \geq p_2^{(3)} \geq p_3^{(3)}$ of $\bar{P}_3$ yield a monotonically non-decreasing sequence. Iterating this procedure in a similar way, the tree Γ_{10} corresponding to $\bar{P}_{10}$ will be of the form in Fig. 2.

The edges of Γ_{10} are directed from the root γ_0 and are labelled by 0 and 1. The paths leading from γ_0 to the end points of Γ_{10}, when arranged into a monotonically decreasing sequence of lengths, correspond to the code-words of the $\bar{P}_{10}$-minimized code $\bar{\mathcal{A}}_{10}$. In our example the code-words of $\bar{\mathcal{A}}_{10}$ are

$$\begin{aligned}
A_1 &= 00\\
A_2 &= 01\\
A_3 &= 100\\
A_4 &= 1010\\
A_5 &= 1011\\
A_6 &= 1100\\
A_7 &= 1101\\
A_8 &= 1110\\
A_9 &= 11110\\
A_{10} &= 11111
\end{aligned}$$

One can observe that the algorithm of theorem 2.9 gives the same code for the parameters

$$\begin{array}{llll}
\lambda_1 = 2 & \lambda_2 = 3 & \lambda_3 = 4 & \lambda_4 = 5\\
s_1 = 2 & s_2 = 1 & s_3 = 5 & s_4 = 2
\end{array}$$

4. Suppression of noise effects

The method described below permits the error detecting and correcting procedures developed for binary $(n; k)$ — codes (block codes) to be applied to comma-free, variable-length binary encoding. For the description of basic notions of protection against noise effects see references [4] and [5].

Let us assume the sequence of information $\mathfrak{A}_n$ to be encoded by the words of the exhausted code, $\mathcal{A}_n$ and the distinct lengths of the code-words are given by the positive integers $\lambda_1 < \lambda_2 < \dots < \lambda_r$ and the number of words of length λ_ν $(\nu = 1, 2, \dots, r)$ is denoted by $s_\nu \geq 1$ where $\sum_{\nu=1}^{r} s_\nu = n$. Let $A_i = \delta_1\delta_2 \dots \delta_k$ where $A_i \in \mathcal{A}_n$; $\lambda(A_i) = \lambda_k$ and δ_j is either 0 or 1 and let the first subsequence $V_{i_1} \preceq A_i$; $V_{i_1} = \delta_1\delta_2 \dots \delta_{\lambda_1}$ of length λ_1 be termed the prefix of order one and the subsequence $V_{i_2} = \delta_{\lambda_1+1}\,\delta_{\lambda_1+2} \dots \delta_{\lambda_2}$ of length $\lambda_2 - \lambda_1$ the prefix of order two etc., finally the subsequence $V_{i_k} = \delta_{\lambda_{k-1}+1}\,\delta_{\lambda_{k-1}+2} \dots \delta_{\lambda_k}$ of length $\lambda_k - \lambda_{k-1}$ the prefix of order k of A_i. Denoting the set of all of the words of lengths $\lambda_1; \lambda_2 - \lambda_1; \ldots ; \lambda_r - \lambda_{r-1}$ formable from 0 and 1 by $\mathcal{V}_1; \mathcal{V}_2; \ldots , \mathcal{V}$ taking λ_0 to be zero. The sequence $\mathcal{V}_\nu$ $(\nu = 1, 2, \ldots , r)$ has $2^{\lambda_\nu - \lambda_{\nu-1}}$ elements. The $\mathcal{V}_\nu$ are exhausted codes and also $\lambda_\nu - \lambda_{\nu-1}$ dimensional vector fields over the residueclass-field Mod 2.

Considering the direct product $\mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_r$, it is obvious that any word A_i of length λ_k in the code $\mathcal{A}_n$ is an element of the direct product $\mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_k$. Conversely, the vectors of direct products $\mathcal{V}_1, \mathcal{V}_1 \otimes \otimes V_2, \ldots , \mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_r$ are usually not code-words. A weaker, but from practical point of view, an important theorem is

Theorem 4.1. If $\mathcal{A}_n$ is exhausted, there exists for each $V_{\nu_j} \in \mathcal{V}_\nu$ $(1 \leq \leq \nu \leq r;\ 1 \leq j \leq 2^{\lambda_\nu - \lambda_{\nu-1}})$ some $A_i \in \mathcal{A}_n$ whose prefix of order ν is V_{ν_j}.

Proof: When $\nu = 1$, the statement is trivial since $\mathcal{A}_n$ is exhausted. For $\nu \geq 2$ let us choose the code $\mathcal{A}' \subset \mathcal{A}_n$ obtained from $\mathcal{A}_n$ by omitting the elements longer than $\lambda_{\nu-1}$, a word W of length $\lambda_{\nu-1}$ for which $\varrho(W; \mathcal{A}') > 0$. Such W always exists, otherwise the elements of $\mathcal{A}_n$ with maximum length $\lambda_{\nu-1}$ would give an exhausted code; thus by theorem 2.1.b. $\mathcal{A}_n$ could not have any element of length λ_ν, whereas by definition $\mathcal{A}_n$ has $s_\nu \geq 1$ elements of length λ_ν. Let us consider the word WV_{ν_j}; by theorem 2.1.c. we have $\varrho(WV_{\nu_j}; \mathcal{A}_n) = 0$, hence $\lambda(WV_{\nu_j}) = \lambda_\nu \leq \lambda_r$ implies $WV_{\nu_j} \preceq A_i$, at least for one $A_i \in \mathcal{A}_n$.

Consider the block-codes $\mathcal{U}_1(l_1; \lambda_1), \mathcal{U}_2(l_2; \lambda_2 - \lambda_1), \ldots , \mathcal{U}_r(l_r; \lambda_r - \lambda_{r-1})$; it may be observed that $\mathcal{U}_\nu(l_\nu; \lambda_\nu - \lambda_{\nu-1})$ is of order $2^{\lambda_\nu - \lambda_{\nu-1}}$ thus, $V_{\nu_j} \in \mathcal{V}_\nu$, $U_{\nu_j} \in \mathcal{U}_\nu : V_{\nu_j} \leftrightarrow U_{\nu_j}$ $(1 \leq j \leq 2^{\lambda_\nu - \lambda_{-\nu 1}})$ can be used to construct a one-to-one correspondence $\mathcal{V}_\nu \leftrightarrow \mathcal{U}_\nu$ $(\nu = 1, 2, \ldots , r)$. The correspondence $V_{\nu_j} \longleftrightarrow U_\nu$ implies a similar one-to-one correspondence between the words $A_i = V_{i_1} V_{i_2} \ldots \ldots V_{i_k}$ $(A_i \in \mathcal{A}_n)$ and $A_i^* = U_{i_1}\ U_{i_2} \ldots U_{i_k}$. The A_i^* form a code $\mathcal{A}_n^*$ having n code-words for which $A_i \longleftrightarrow A_i^*$; $A_i \in \mathcal{A}_n$; $A_i^* \in \mathcal{A}_n^*$ $(i = 1, \ldots , n)$ holds. If the elements of the sequence of information $\mathfrak{A}_n$ are encoded by the words of $\mathcal{A}_n^*$, the erroneous bits occurring in the prefix of the code-word $A_i^* = = U_{i_1} U_{i_2} \ldots U_{i_k}$ of order ν can be detected or corrected by methods of error detection or correction applicable to the block code $\mathcal{U}_\nu$. If the noise effects do not appear uniformly but are more frequent in a sequence of code-words ranged in the interval of prefixes of order ν, a more effective error correction can be used for the prefix of order ν.

If the basic code $\mathcal{A}_n$ is P_n-minimized, the most frequently occurring code words of the corresponding code $\mathcal{A}_n^*$ have the property that the maximum order of their prefixes is at a minimum.

References

1. Gilbert, E. N.—Moore, E. F.: Variable-length binary encodings. The Bell System Technical Journal **38**, 933—968 (1969).
2. Huffmann, D. A.: A method for the construction of minimum redundancy codes. Proc. I.R.E. **40**, 1098—1101 (1952).

3. CALABI, L.: On error-correcting. Variable-length codes. Scientific Report No. 9, Contract AF **19** (604)—7493 December 1963. Applied Mathematics, Air Force Research Laboratories Office of Aerospace Research, United States Air Force Bedford Massachusetts.
4. PETERSON, W. W. Error-correcting codes. Massachusetts Institute of Technology, 1961.
5. DÉNES, J., RADA, T.: Véges struktúrák és digitális áramkörök kapcsolata. MTA Mat. Int. Közleményei **10** 679—732 (1965).
6. FRIED, E.: Vesszőmentes kódrendszer algoritmikus konstrukciója, NIM Számítástechnikai Közlemények **6,** 9—13 (1965).
7. FANO, R. M.: Transmission of information. A statistical theory of communications. New York, 1961.

Summary

Necessary and sufficient condition is given for a code to be minimized. An algorithm is presented to construct minimized codes. Error correcting variable-length encoding is illustrated by an example.

Dr. Sándor BENDE, Budapest XI., Stoczek u. 2—4, Hungary