PAPER *Special Issue on A Special issue of IEICE Transactions*

A Multilevel Construction of Permutation Codes*

Tadashi WADAYAMA[†], ***Member and*** **A.J.Han VINCK**[††], ***Nonmember***

SUMMARY A novel multilevel construction for permutation codes is presented. A permutation code of length n is a subset of all the vectors obtained from coordinate permutations on the vector $(0, 1, \ldots, n-1)$. We would like to construct a permutation code with cardinality as large as possible for a given code length n and a minimum distance. The proposed construction is available when $n = 2^m$ (m is a positive integer). We exploit m-constant weight binary codes as component codes and combine them in a multilevel way. We can construct permutation codes with various parameters by selecting appropriate combination of component codes. Moreover, the multilevel structure enable us to use a multi-stage decoding algorithm.

key words: *permutation code, multilevel code, multi-stage decoding*

1. Introduction

A permutation code of length n is originally defined by the action of a permutation group G on the initial vector $\boldsymbol{a} \triangleq (0, 1, 2, \ldots, n-1)$[1]. In other words, a permutation code P is given by $P \triangleq \{\sigma(\boldsymbol{a}) : \sigma \in G\}$.

We here use the term "permutation code" in wider sense than one defined above. Let S be the set of all the vectors obtained from a coordinate permutation on $\boldsymbol{a}$: $S \triangleq \{\sigma(\boldsymbol{a}) : \sigma \in G_S\}$, where G_S is the symmetric group on n-elements. The cardinality of the set S is equal to $n!$. Consider a subset $P \subset S$ which has the cardinality M and the minimum Hamming distance d. We call P a *permutation code* and it is also denoted by (n, M, d)-permutation code. This change gives us more freedom on code construction without sacrificing the advantages of the permutation codes[4].

The most principal problem on permutation codes is the code construction problem: we would like to construct a permutation code with cardinality M as large as possible for a given code length n and a minimum distance d. Several works have been made to construct good permutation codes.

Blake[1] presented a construction of the permutation codes based on the k-transitive groups. He showed the construction of an $(n, n!, 3)$-code based on the alternating group. He also constructed $(n, n(n-1), n-1)$, $(n, n(n-1)(n-2), n-2)$-codes from sharply doubly and triply transitive permutation group, and (11,7920,8), (12,371392,8), (12,95040,8)-codes from the Mathieu group.

It is known that the cardinality M is upper bounded in such a way[2]:

$$M \leq \frac{n!}{(d-1)!}. \qquad (1)$$

For $n \leq 5$, the codes with the cardinality satisfying (1) with equality have been found by computer search[4]. When $n = 6$ and $d = 5$, the equality in (1) cannot be satisfied (The pair $n = 6$ and $d = 5$ is the smallest pairs which do not satisfy the equality). In [5], Kløve classified the permutation codes with $n = 6$ and $d = 5$ and proved that $M = 18$ is maximal.

In spite of the above works, the code parameters which is available are still limited. There is plenty of room for further research on this topic. In this paper, we present a novel construction for permutation codes. The construction presented here is based on the idea of the multilevel coded-modulation proposed by Imai and Hirakawa[6]. In the proposed construction, several binary constant weight binary codes are exploited as multilevel component codes. The multilevel structure gives flexibility on parameter selection. We can construct permutation codes with various parameters by selecting appropriate combination of component codes.

Due to the multilevel structure of the proposed codes, we can also use the multi-stage decoding algorithm which significantly reduces the decoding complexity. The lack of efficient decoding algorithm for a long permutation code is a serious problem for practical applications of permutation codes. The combination of M-FSK modulation and permutation codes has been considered as candidate codes for power line communications[3][4]. Moreover, permutation codes can be used as hopping patterns for frequency hop spread spectrum communications.

2. Constructions

2.1 Basic construction

Let C be a binary constant weight code with the length n, the cardinality M', the minimum distance d' and

[†] The author is with Faculty of Computer Science and System Engineering, Okayama Prefectural University, 111 Kuboki, Soja, Okayama,719–1197, Japan

[††] The author is with Institute for Experimental Mathematics, University of Essen, Germany

[*] This paper was presented at Symposium of Information Theory and Its Applications 2000 at Aso, Japan (Oct. 2000)

weight w. We denote the code C as an $[n, M', d', w]$-constant weight code. Let ϕ_p be the binary to integer conversion mapping defined by

$$\phi_p(x_{p-1}, \dots, x_1, x_0) \stackrel{\triangle}{=} \sum_{i=0}^{p-1} 2^i x_i, \tag{2}$$

where p is a positive integer and $x_i \in \{0,1\}$ for $0 \le i \le p-1$.

Assume that $n = 2^m$, where m is a positive integer. Let $C_i (i \in [0, m-1])$ be an $[n/2^i, M_i, d_i, n/2^{i+1}]$-constant weight code. The set of nonnegative integers from a to b is denoted by $[a,b]$. For example, $[0,4] = \{0,1,2,3,4\}$. We denote the set of codes as $\boldsymbol{C} = (C_0, C_1, \dots, C_{m-1})$. For any set of codewords

$$\boldsymbol{c}_0 = (c_0^{(0)}, c_1^{(0)}, \dots, c_{n-1}^{(0)}) \in C_0, \tag{3}$$

$$\boldsymbol{c}_1 = (c_0^{(1)}, c_1^{(1)}, \dots, c_{n/2-1}^{(1)}) \in C_1, \tag{4}$$

$$\cdots$$

$$\boldsymbol{c}_{m-1} = (c_0^{(m-1)}, c_1^{(m-1)}) \in C_{m-1}, \tag{5}$$

we here define an $m \times n$-matrix A. The (i,j)-element of A is denoted by $a(i,j)$ for $i \in [0, m-1]$ and $j \in [0, n-1]$. The first row of A, $(a(0,0), a(0,1), \dots, a(0,n-1))$, is determined in such a way:

$$a(0,t) = c_t^{(0)}, \quad t \in [0, n-1]. \tag{6}$$

The i-th row$(i \in [1, m-1])$ of A is given by

$$a(i, g_t^{(s)}) = c_t^{(i)}, \quad t \in [0, 2^{m-i}-1], s \in [0, 2^i-1]. \tag{7}$$

The $g_t^{(s)}$'s in the above equation are defined by

$$\{g_0^{(s)}, g_1^{(s)}, \dots, g_{2^{m-i}-1}^{(s)}\} \tag{8}$$
$$= \{j : \phi_i(a(0,j), a(1,j), \dots, a(i-1,j)) = s\},$$

where $g_0^{(s)} < g_1^{(s)} < \dots < g_{2^{m-i}-1}^{(s)}$. Let $\boldsymbol{\alpha}_j$ be the j-th column vectors$(j \in [0, n-1])$ of A. The mapping $\Phi_m(A)$ is defined by

$$\Phi_m(A) \stackrel{\triangle}{=} (\phi_m(\boldsymbol{\alpha}_0), \dots, \phi_m(\boldsymbol{\alpha}_{n-1})). \tag{9}$$

The above construction of an n-tuple over $[0, 2^m - 1]$ is refereed to as the *basic construction*.

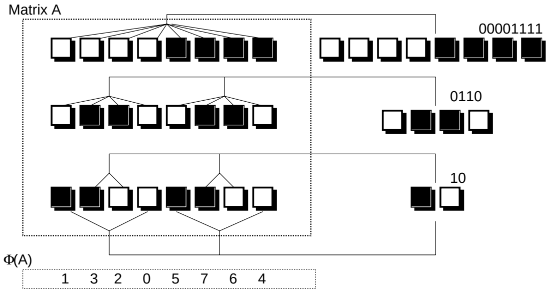

Fig. 1 Example of basic construction

Example 1: Consider the case where $m = 3, n = 2^3 = 8$. We take $[8,2,8,4]$-constant weight code $\{00001111, 11110000\}$ as C_0, $[4,2,4,2]$-constant weight code $\{0110, 1001\}$ as C_1 and $[2,2,2,1]$-constant weight code $\{01, 10\}$ as C_2. Suppose that $\boldsymbol{c}_0 = 00001111, \boldsymbol{c}_1 = 0110$, and $\boldsymbol{c}_2 = 10$. We then have

$$A = \begin{pmatrix} 00001111 \\ 01100110 \\ 11001100 \end{pmatrix}. \tag{10}$$

and $\Phi_3(A) = (1,3,2,0,5,7,6,4)$(See.Fig.1).

If $\boldsymbol{c}_0 = 00001111, \boldsymbol{c}_1 = 0110, \boldsymbol{c}_2 = 01$, then we have

$$A = \begin{pmatrix} 00001111 \\ 01100110 \\ 00110011 \end{pmatrix}. \tag{11}$$

In this case, we obtain $\Phi_3(A) = (0,2,3,1,4,6,7,5)$. □

As we have observed in the example, $\Phi_m(A)$ becomes a permuted vector of $(0,1,2,\dots,n-1)$. In order to prove $\Phi_m(A) \in S$ for any A, we need the following lemma.

Lemma 1: Every binary m-tuple appears only once as a column vector in A.

(Proof) Consider a binary r-tuple obtained from A:

$$\boldsymbol{z}_j^{(r)} \stackrel{\triangle}{=} (a(0,j), a(1,j), \dots, a(r-1,j))^t. \tag{12}$$

In order to prove the claim of the lemma, we shall prove the following more general claim: every binary r-tuple appears exactly 2^{m-r}-times in $\{\boldsymbol{z}_j^{(r)} : j \in [0, n-1]\}$. For $r = 1$, the claim holds because a codeword of the first level code C_0 has 2^{m-1}-zeros and 2^{m-1}-ones. Next, we assume that the claim holds for $r = r'$. Consider an arbitrary column index set $\{h_0, h_1, \dots, h_{2^{m-r'}-1}\}$ which satisfies

$$\boldsymbol{z} \stackrel{\triangle}{=} \boldsymbol{z}_{h_0}^{(r')} = \boldsymbol{z}_{h_1}^{(r')} = \dots = \boldsymbol{z}_{h_{2^{m-r'}-1}}^{(r')} \tag{13}$$

and $h_0 < h_1 < \dots < h_{2^{m-r'}-1}$. From the basic construction described above, we have

$$a(r', h_t) = c_t^{(r')}, \quad t \in [0, 2^{m-r'}-1]. \tag{14}$$

Since $\boldsymbol{c}^{(r')}$ has the same number of zeros and ones, the half of $\{\boldsymbol{z}_{h_t}^{(r'+1)} : t = 0, 1, \dots 2^{m-r'} - 1\}$ takes the value $(\boldsymbol{z}, 0)^t$ and the remaining takes the value $(\boldsymbol{z}, 1)^t$. It means that every binary $(r'+1)$-tuple appears exactly $2^{m-r'-1}$-times in $\{\boldsymbol{z}_j^{(r'+1)} : j = 0, 1, \dots, n-1\}$. □

For a given set of codes $\boldsymbol{C} = (C_0, C_1, \dots, C_{m-1})$, the set of all the possible matrices obtained by the basic construction is denoted by $\mathcal{A}(\boldsymbol{C})$. The cardinality $|\mathcal{A}(\boldsymbol{C})|$ is equal to $M_0 \times M_1 \times \dots \times M_{m-1}$. Consider $A \in \mathcal{A}(\boldsymbol{C})$ and let $\boldsymbol{\alpha}_j$ be the j-th column vectors$(j \in [0, n-1])$ of A. The set $\mathcal{P}(\boldsymbol{C})$ is defined by

$$\mathcal{P}(\boldsymbol{C}) \stackrel{\triangle}{=} \{\Phi_m(A) : A \in \mathcal{A}(\boldsymbol{C})\}. \tag{15}$$

From Lemma 1, we know that every binary m-tuple appears only once as a column vector in A. Since ϕ_m is one-to-one mapping from $\{0,1\}^m$ to $[0, 2^m-1]$, every number in $[0, 2^m-1]$ appears only once in $\Phi_m(A)$. It implies that $\mathcal{P}(\boldsymbol{C})$ is a permutation code of length n and the number of codewords of $\mathcal{P}(\boldsymbol{C})$ coincides with the cardinality of $\mathcal{A}(\boldsymbol{C})$.

We next discuss the minimum distance property of the permutation codes. Consider arbitrary two matrices $A_1, A_2 \in \mathcal{A}(\boldsymbol{C})$. Let $\boldsymbol{\alpha}_j^{(1)}$ and $\boldsymbol{\alpha}_j^{(2)}$ be the j-th column vectors($j \in [0, n-1]$) of A_1 and A_2, respectively. The distance between A_1 and A_2 is defined by

$$d_\alpha(A_1, A_2) \overset{\triangle}{=} |\{j : \boldsymbol{\alpha}_j^{(1)} \neq \boldsymbol{\alpha}_j^{(2)}, j \in [0, n-1]\}|.(16)$$

The minimum distance of $\mathcal{A}(\boldsymbol{C})$, d_{min}, is defined by

$$d_{min} \overset{\triangle}{=} \min\{d_\alpha(A_1, A_2) : A_1, A_2 \in \mathcal{A}(\boldsymbol{C}), A_1 \neq A_2\}.$$

Lemma 2: The minimum distance of $\mathcal{A}(\boldsymbol{C})$ is lower bounded by

$$d_{min} \geq \min\{d_0, 2d_1, 4d_2, \ldots, 2^{m-1}d_{m-1}\}. \qquad (17)$$

(Proof) Consider arbitrary two matrices $A_1, A_2 (A_1 \neq A_2) \in \mathcal{A}(\boldsymbol{C})$. Let $\boldsymbol{\beta}_i^{(1)}$ and $\boldsymbol{\beta}_i^{(2)}$ be the i-th row vectors($i \in [0, m-1]$) of A_1 and A_2, respectively. If the first rows $\boldsymbol{\beta}_0^{(1)} \neq \boldsymbol{\beta}_0^{(2)}$, then $d_\alpha(A_1, A_2) \geq d_0$ holds. The reason is the following. The both $\boldsymbol{\beta}_0^{(1)}$ and $\boldsymbol{\beta}_0^{(2)}$ belong to C_0. Thus, $d_h(\boldsymbol{\beta}_0^{(1)}, \boldsymbol{\beta}_0^{(2)}) \geq d_0$, where $d_h(\cdot,\cdot)$ is the Hamming distance function. Namely, the first rows differs at least d_0-coordinate positions. Next, we consider the case where

$$\boldsymbol{\beta}_i^{(1)} = \boldsymbol{\beta}_i^{(2)} \quad \text{for} \quad i \in [0, i^*-1], \qquad (18)$$

$$\boldsymbol{\beta}_{i^*}^{(1)} \neq \boldsymbol{\beta}_{i^*}^{(2)}, \qquad (19)$$

for $i^* \in [1, m-1]$. In this case, the Hamming distance between $\boldsymbol{\beta}_{i^*}^{(1)}$ and $\boldsymbol{\beta}_{i^*}^{(2)}$ satisfies $d_h(\boldsymbol{\beta}_{i^*}^{(1)}, \boldsymbol{\beta}_{i^*}^{(2)}) \geq 2^{i^*} d_{i^*}$ because $\boldsymbol{\beta}_{i^*}^{(1)}, \boldsymbol{\beta}_{i^*}^{(2)}$ are codewords of the 2^{i^*}-times repetition code of C_{i^*}. This implies that the i^*-th rows differs at least $2^{i^*} d_{i^*}$-coordinate positions. From the assumption $A_1 \neq A_2$ and the above argument, we have the claim of the lemma. □

The above discussion leads to the following theorem on the parameters of the permutation codes constructed by the basic construction.

Theorem 1: The code $\mathcal{P}(\boldsymbol{C})$ constructed by the basic construction is an (n, M, d)-permutation code with the following parameters:

$$\begin{aligned} n &= 2^m, \\ M &= M_0 \times M_1 \times \cdots \times M_{m-1}, \\ d &\geq \min\{d_0, 2d_1, 4d_2, \ldots, 2^{m-1}d_{m-1}\}. \end{aligned}$$

□

Example 2: Consider the case where $m = 2, n = 2^2 = 4$. We take $[4,2,4,2]$-constant weight code $\{1001, 1001\}$ as C_0 and $[2,2,2,1]$-constant weight code $\{01, 10\}$ as C_1. In this case, we have

$$\mathcal{A}(\boldsymbol{C}) = \left\{ \begin{pmatrix} 1001 \\ 0011 \end{pmatrix} \begin{pmatrix} 1001 \\ 1100 \end{pmatrix} \begin{pmatrix} 0110 \\ 0011 \end{pmatrix} \begin{pmatrix} 0110 \\ 1100 \end{pmatrix} \right\}$$

and

$$\mathcal{P}(\boldsymbol{C}) = \{(2013)(3102)(0231)(1320)\}.$$

It is easy to confirm that the code $\mathcal{P}(\boldsymbol{C})$ is a $(4,4,4)$-permutation code. In this case, the minimum distance bound by Theorem 1 ($d \geq \min\{4, 2 \times 2\}$) holds with equality. □

The following corollary is a simple application of Theorem 1.

Corollary 1: There exists an (n, M, d)-permutation code with the following parameters:

$$\begin{aligned} n &= 2^m, \\ M &= (2^{m+1}-2) \times (2^m - 2) \times \cdots \times (2^2 - 2), \\ d &\geq 2^{m-1}, \end{aligned}$$

where m is an arbitrary positive integer.

(Proof) Getting rid of $(0,0,\ldots,0)$ and $(1,1,\ldots,1)$ from the first order Reed-Muller code of degree m, we can obtain a $[2^m, 2^{m+1}-2, 2^{m-1}, 2^{m-1}]$-constant weight code. By using the $[2^{m-i}, 2^{m+1-i}-2, 2^{m-1-i}, 2^{m-1-i}]$-constant weight code as $C_i (i \in [0, \ldots, m-1])$, we have the permutation codes with the above parameters. □

Example 3: For $m = 3,4,5$, we can obtain $(8, 168, \geq 4)$, $(16, 5040, \geq 8)$, $(32, 312480, \geq 16)$-permutation codes, respectively. □

2.2 Extended construction

The basic construction described in the previous subsection is most efficient when the component codes have the minimum distances satisfying the equality $d_0 = 2d_1 = 4d_2 = \cdots = 2^{m-1}d_{m-1}$. When the above equality does not hold, we can improve the basic construction. We here present the *extended construction* for such a case.

Let B_i be a subset of $C_i (i \in [0, m-1])$. The cardinality of B_i is denoted by $q_i (q_i \leq |C_i|)$. Let Q_i be an alphabet with the cardinality q_i. Suppose that the functions $f_i (i \in [0, m-1])$ is a one-to-one mapping such that $f_i : Q_i \to B_i$.

Consider the set of codes $\boldsymbol{L} = (L_0, L_1, \ldots, L_{m-1})$ where L_i is a block code over the alphabet Q_i and the code L_i has the length 2^i, μ_i-codewords, the minimum distance δ_i $(i \in [0, m-1])$. The code is denoted by a $(2^i, \mu_i, \delta_i)_{q_i}$-code. For a given vector

$$(w_0, w_1, \ldots, w_{2^i-1}) \in L_i, \qquad (20)$$

the value $c_t^{(i,s)}$ is given by

$$(c_0^{(i,s)}, c_1^{(i,s)}, \ldots, c_{2^{m-i}-1}^{(i,s)}) = f_i(w_s) \in C_i, \tag{21}$$

where $i \in [0, m-1]$, $s \in [0, 2^i - 1]$, $t \in [0, 2^{m-i} - 1]$. An $m \times n$-matrix A can be defined as follows. The first row of A is determined in such a way:

$$a(0,t) = c_t^{(0,0)}, \quad t \in [0, n-1], \tag{22}$$

The i-th row($i \in [1, m-1]$) of A is given by

$$a(i, g_t^{(s)}) = c_t^{(i,s)}, \quad t \in [0, 2^{m-i} - 1] \tag{23}$$

for $s \in [0, 2^i - 1]$. The value $g_t^{(s)}$ is given by (8). Namely, the code L_i is used for selecting 2^i-codewords of C_i and each codeword is assigned to the positions corresponding to the same value in terms of s. This construction is called the extended construction.

The set $\mathcal{A}(\boldsymbol{C}, \boldsymbol{L})$ is the set of all the possible matrices obtained by the extended construction. The set $\mathcal{P}(\boldsymbol{C}, \boldsymbol{L})$ is defined by

$$\mathcal{P}(\boldsymbol{C}, \boldsymbol{L}) \overset{\triangle}{=} \{\Phi_m(A) : A \in \mathcal{A}(\boldsymbol{C}, \boldsymbol{L})\}. \tag{24}$$

Theorem 2: The code $\mathcal{P}(\boldsymbol{C}, \boldsymbol{L})$ is an (n, M, d)-permutation code whose parameters are given by

$$n = 2^m, \tag{25}$$

$$M = \mu_0 \times \mu_1 \times \cdots \times \mu_{m-1}, \tag{26}$$

$$d \geq \min\{\delta_0 d_0, \delta_1 d_1, \ldots, \delta_{m-1} d_{m-1}\}. \tag{27}$$

(Proof) Lemma 1 holds for $\mathcal{A}(\boldsymbol{C}, \boldsymbol{L})$ as well. For $\mathcal{A}(\boldsymbol{C}, \boldsymbol{L})$, the minimum distance bound (corresponding to Lemma 2) is given by

$$d_{min} \geq \min\{\delta_0 d_0, \delta_1 d_1, \ldots, \delta_{m-1} d_{m-1}\}. \tag{28}$$

The proof of the bound is almost the same as the proof of Lemma 2. The only difference is that the Hamming distance between $\boldsymbol{\beta}_{i^*}^{(1)}$ and $\boldsymbol{\beta}_{i^*}^{(2)}$ satisfies $d_h(\boldsymbol{\beta}_{i^*}^{(1)}, \boldsymbol{\beta}_{i^*}^{(2)}) \geq \delta_{i^*} d_{i^*}$. □

Example 4: Assume the following set of constant weight codes: $C_0 : [16, 1170, 4, 8]$, $C_1 : [8, 70, 2, 4]$, $C_2 : [4, 6, 2, 2]$, $C_3 : [2, 2, 2, 1]$. By using the basic construction, we have a $(16, 1170 \times 70 \times 6 \times 2 = 982800, \geq 4)$-permutation code. Consider the following block codes $L_0 : (1, 1170, 1)_{1170}$, $L_1 : (2, 70, 2)_{70}$, $L_2 : (4, 6^3, 2)_6$, $L_3 : (8, 2^7, 2)_2$. By using the extended construction, we can obtain a $(16, 1170 \times 70 \times 6^3 \times 2^7 = 2264371200 \simeq 2^{31}, \geq 4)$-permutation code. The cardinality of the code obtained from the extended construction is much larger than the one obtained from the basic construction in this case. □

The basic construction can be regarded as a special case of the extended construction. Namely, let $L_i = (2^i, M_i, 2^i)_{M_i}$. This code is the repetition code over M_i-ary alphabet. It is easy to see that the extended construction yields the same results obtained from the basic construction.

3. Multi-stage decoding algorithm for permutation codes

The multilevel structure of the permutation codes introduced in the previous section naturally leads to a multi-stage decoding algorithm for this class of codes. Although the proposed decoding algorithm is suboptimal, it gives significant reduction on decoding complexity of the permutation codes. The algorithm is based on the idea of the multi-stage decoding algorithm proposed by Imai and Hirakawa[6].

Throughout the section, we assume that the vector $\boldsymbol{x} \in \mathcal{P}(\boldsymbol{C})$ (a code obtained from the basic construction) is the transmitted vector and $\boldsymbol{y}$ is the received vector. The distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ is denoted by $d(\boldsymbol{x}, \boldsymbol{y})$. We here do not assume a specific channel. The distance measure $d(\cdot, \cdot)$ should be chosen appropriately depending on the channel statistics. For example, we should use the squared Euclidean distance as the distance measure for an additive white Gaussian channel.

3.1 Decoding algorithm

The outline of the multi-stage decoding algorithm is the following. Firstly, the first(0-th) row $\boldsymbol{r}_0$ in A is decoded with a decoder for C_0 based on the assumption that the other rows $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_{m-1}$ take values from $\{0,1\}^n$. In this decoding process, we have $\hat{\boldsymbol{r}}_0$ as the estimate of the first row of the transmitted word. Next, the repetition code of C_1 is decoded as well based on the assumption $\boldsymbol{r}_0 = \hat{\boldsymbol{r}}_0, \boldsymbol{r}_2 \in \{0,1\}^n, \ldots, \boldsymbol{r}_{m-1} \in \{0,1\}^n$. In a similar way, at the i-th row, the repetition code of C_i is decoded based on the decoding result of $\boldsymbol{r}_0$ to $\boldsymbol{r}_{i-1}$ and the assumption $\boldsymbol{r}_{i+1} \in \{0,1\}^n, \ldots, \boldsymbol{r}_{m-1} \in \{0,1\}^n$. The procedure is repeated until all the rows has been decoded.

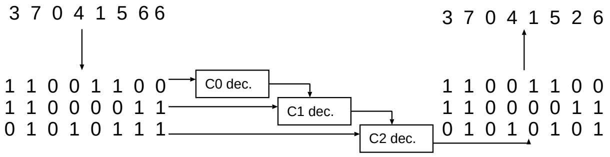

Fig. 2 Procedure of multi-stage decoding

The detail of the multi-stage decoding algorithm is described as follows:

[Multi-stage decoding algorithm for $\mathcal{P}(\boldsymbol{C})$]

Step 1 Compute the estimate of the first row codeword.

$$\hat{\boldsymbol{r}}_0 = \arg\min_{\boldsymbol{r}_0}\{d(\boldsymbol{y}, \Phi_m(R)) : \boldsymbol{r}_0 \in C_0,$$
$$\boldsymbol{r}_1 \in \{0,1\}^n, \ldots, \boldsymbol{r}_{m-1} \in \{0,1\}^n\}, \tag{29}$$

where the matrix R is the matrix with the rows $(\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_{m-1})$.

Step 2 Set $i = 1$.

Step 3 Compute the estimate of the i-th row codeword.

$$\hat{\boldsymbol{r}}_i = \arg\min_{\boldsymbol{r}_i}\{d(\boldsymbol{y}, \Phi_m(R)) : \boldsymbol{r}_0 = \hat{\boldsymbol{r}}_0, \ldots, \boldsymbol{r}_{i-1} = \hat{\boldsymbol{r}}_{i-1}, \boldsymbol{r}_i \in C_i^*, \boldsymbol{r}_{i+1} \in \{0,1\}^n, \ldots, \boldsymbol{r}_{m-1} \in \{0,1\}^n\}, \quad (30)$$

where C_i^* denotes the 2^i-times repetition code of C_i.

Step 4 If $i < m-1$, then set $i \leftarrow i+1$ and go to Step 3.

Step 5 Output the decoding result $(\hat{\boldsymbol{r}}_0, \hat{\boldsymbol{r}}_1, \ldots, \hat{\boldsymbol{r}}_{m-1})$ and quit the algorithm.

Example 5: From Corollary 1, we can obtain a $(256, 5100311059200 \simeq 2^{42}, \geq 128)$-permutation code. Consider the decoding algorithm based on exhaustive codeword generation. In this case, we have to generate approximately 2^{42}-codewords. On the other hand, if we exploit the multi-stage decoding algorithm presented here, we need to evaluate only $(2^9-2)+(2^8-2)+\cdots+(2^2-2) = 1004$ -codewords of $C_0, C_1, \ldots, C_{m-1}$. □

Tadashi Wadayama was born in Kyoto, Japan on May 9, 1968. He received the B.E., the M.E., and the D.E. degrees from Kyoto Institute of Technology in 1991, 1993 and 1997, respectively. Since 1995, he has been with Faculty of Computer Science and System Engineering, Okayama Prefectural University as a research associate. From April 1999 to March 2000, he stayed in Institute of experimental mathematics, University of Essen (Germany) as a visiting researcher. His research interests are in digital communication systems, especially in coding theory. He is a member of SITA and IEEE.

A. J. Han Vinck is a full professor in Digital Communications at the University of Essen, Essen, Germany, since 1990. He studied electrical engineering at the University of Eindhoven, The Netherlands, where he obtained his Ph.D. in 1980. His interest is in Information and Communication theory, Coding and Network aspects in digital communications. From 1991-1993 and 1998-2000 he was the director of the Institute for Experimental Mathematics in Essen. Professor Vinck was the director (1997-1999) of the Post-Graduate School on Networking, "CINEMA". Professor Vinck serves on the Board of Governors of the IEEE Information Theory Society since 1997 (until 2003). In 2000 he was elected 2nd vice president of the IEEE Information theory Society. In 1999 he was the Program Chairman for the IEEE IT workshop in Kruger Park, South Africa and in 1997 he acted as Co-chairman for the 1997 IEEE Information Theory symposium in Ulm, Germany (704 participants). Professor Vinck was founding Chairman (1995-1998) of the IEEE German Information Theory chapter. In 1990 he organized the IEEE Information Theory workshop in Veldhoven, the Netherlands.

Professor Vinck is the initiator of the Japanese-Benelux workshops on Information theory and the International wintermeeting on Coding, Cryptography and Information theory. He started (Essen, 1997) and still supports the organization of the series of conferences on Power Line Communications and its Applications. He is co-founder and president of the Shannon and the Gaus foundations. These foundations stimulate research and help young scientists in the field of Information theory and Digital Communications. In 1998 he was elected chairman of the Benelux Information and Communication Theory Society.

References

[1] I.F.Blake, "Permutation codes for discrete channels," *IEEE Trans. Information Theory*, IT-20, pp.138–140 (1974).

[2] M.Deza and S.A.Vanstone, "Bounds for permutation arrays," J.Stat. Plann.Infer.,vol.2,pp.197–209 (1978).

[3] A.J.Han Vinck, J. Häring, "Coding and modulation for power-line communications," in Proceeding of International Symposium on Power Line Communications 2000 (2000).

[4] A.J.Han Vinck, J. Häring, T. Wadayama, "Coded M-FSK for power line communications," in Proceeding of International Symposium on Information Theory 2000, June, Italy (2000).

[5] T. Kløve, "Classification of permutation codes of length 6 and minimum distance 5," in Proceeding of International Symposium on Information Theory and Its Applications 2000, Nov., Hawaii (2000).

[6] H.Imai, S.Hirakawa,"A new multilevel coding method using error-correcting codes," *IEEE Trans. Information Theory*, IT-23, pp.371–377 (1977).