Electronic Preprint for Journal of Information Processing Vol.25

Regular Paper

A New Construction Method of Gray Maps for Groups and its Application to the Groups of Order 16

Ko Sakai[1,a)] Yutaka Sato[2,b)]

Received: October 27, 2016, Accepted: February 9, 2017

Abstract: In this paper we propose a new construction method of Gray maps for groups. In a earlier paper, we succeeded the Type 1 construction for all groups of order 16 and confirmed that we can construct Type 2 maps for several groups of order 16, but failed to construct such maps for other groups. Therefore, in this paper we try to apply the new construction method to them.

Keywords: new construction method, Gray map, affine transformation

1. Introduction

Reza Sobhani [1] designed two classes of Gray maps called Type 1 Gray map and Type 2 Gray map, for finite p-groups. Both are constructed as extensions of a Gray map for a smaller group. Type 1 method constructs a code for the target group from a code for its maximal subgroup naturally, but it doubles the length of the resulting code.

The Type 2 method in contrast generally construct a shorter code than Type 1 that is just 1 bit longer than that for the based maximal subgroup. However, in our trial [8], among all the groups of order 16, only 6 groups allow Type 2 extension from 3-bit Gray codes for groups of order 8.

Marcel Wild [2] gave complete classification of the groups of order 16 based on several elementary facts. He examined them as the semidirect product of groups of order 8 by the cyclic group C_2 of order 2.

Based on Wild's work, we examined Type 1 Gray maps and Type 2 Gray maps for groups of order 16 [8] in the same way as Sobhani. First, we summarize Sobhani's approach in Section 2. Next, we propose a new construction method of Gray maps for an arbitrary finite group (not even necessary to be a p-group) in Section 3. In later sections, we try to apply it to several groups of order 16, among which there are some groups for which we failed to apply Type 2 method.

We believe the method can also contribute to constructing non-binary codes. However, in order to concentrate on binary codes here, we assume that the information is encoded in $\mathbb{Z}_2^n$, throughout this paper.

1 Faculty of Pure and Applied Sciences, University of Tsukuba, Tsukuba, Ibaraki 305–8571, Japan
2 Graduate School of Pure and Applied Sciences, University of Tsukuba, Tsukuba, Ibaraki 305–8571, Japan
a) ksakai@math.tsukuba.ac.jp
b) yutaka.okuhara@gmail.com

2. Preliminaries

2.1 Hamming-distance, Hamming-weight and Gray Map

In this section we assume that G is a finite 2-group of order 2^m. We review some key definitions and a lemma on Gray maps in Refs. [1], [5].

Definition 1 For any two elements $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{Z}_2^n$, the *Hamming-distance* between $\mathbf{u}$ and $\mathbf{v}$ is defined by

$$d_H(\mathbf{u}, \mathbf{v}) \stackrel{\text{def.}}{=} |\{i \mid 1 \le i \le n,\, u_i \ne v_i\}|.$$

The Hamming-distance is indeed a distance on $\mathbb{Z}_2^n$ [5].

Definition 2 The *Hamming-weight* of an element $\mathbf{u} \in \mathbb{Z}_2^n$ is defined by

$$w_H(\mathbf{u}) \stackrel{\text{def.}}{=} |\{i \mid 1 \le i \le n,\, u_i \ne 0\}|.$$

Definition 3 A map $\phi : G \to \mathbb{Z}_2^n$ is said to be a *Gray map*, if it is an injection and

$$w_H(\phi(a^{-1}b)) = d_H(\phi(a), \phi(b))$$

holds for all a, b in G. [*1]

Lemma 1 Let $\phi : G \to \mathbb{Z}_2^n$ be a Gray map. Then,

(1) For $g \in G$ we have $w_H(\phi(g)) = 0$ iff $g = e$, where e stands for the identity of G,

(2) For all g in G we have $w_H(\phi(g)) = w_H(\phi(g^{-1}))$,

(3) For all x, y in G we have $w_H(\phi(xy)) \le w_H(\phi(x)) + w_H(\phi(y))$.

proof: Assume that ϕ is a Gray map.

(1) $0 = w_H(\phi(g)) = w_H(\phi(e^{-1}g)) = d_H(\phi(e), \phi(g)) \iff \phi(g) = \phi(e) \iff g = e$,

(2) $w_H(\phi(g)) = w_H(\phi(e^{-1}g)) = d_H(\phi(e), \phi(g)) = d_H(\phi(g), \phi(e)) = w_H(\phi(g^{-1}e)) = w_H(\phi(g^{-1}))$,

(3) $w_H(\phi(g)) + w_H(\phi(h)) = d_H(\phi(g^{-1}), \phi(e)) + d_H(\phi(e), \phi(h)) \ge$

*1 In Sobhani's definion of the Gray map [1], function d_ϕ is defined by $d_\phi(a, b) = w_H(\phi(ab^{-1}))$ and is required to be indeed a distance on G. For simplicity in our definition, map ϕ is required just to be an injection, accepting suggestion of a referee.

Table 1 Aut(C_4) and Aut(C_8) $\simeq K_4$.

Aut(C_4)	effect on x	Aut(C_8)	effect on x
φ_1	x	σ_1	x
φ_2	x^3	σ_2	x^3
		σ_3	x^5
		σ_4	x^7

Table 2 Aut(K_8) $\simeq D_8$.

Aut(K_8)	effect on x	effect on y	order of automorphism
ψ_1	x	y	1
ψ_2	x^3y	x^2y	4
ψ_3	x^3	y	2
ψ_4	xy	x^2y	4
ψ_5	xy	y	2
ψ_6	x^3	x^2y	2
ψ_7	x^3y	y	2
ψ_8	x	x^2y	2

$$d_H(\phi(g^{-1}), \phi(h)) = w_H(\phi(gh)).$$

We define map $d_\phi : G \times G \to \mathbb{N} \cup \{0\}$ by $d_\phi(a, b) = d_H(\phi(a), \phi(b))$. Then, d_ϕ is a distance on G clearly.

2.2 Cyclic Extensions

For notational convenience, we use the standard presentation $\langle X \mid \Delta \rangle$ of groups by generator X and relation Δ [4].

For example, the cyclic group C_n of order n is represented as $\langle x \mid x^n = e \rangle$ and the *Klein four group* $K_4 = C_2 \times C_2$ as $\langle x, y \mid x^2 = y^2 = e, xy = yx \rangle$.

The direct product of C_4 and C_2 is represented as $\langle x, y \mid x^4 = y^2 = e, yx = xy \rangle$. Since this group appears frequently in this paper we denote it by K_8 as in Ref. [2]. Similarly, we denote the dihedral group $\langle x, y \mid x^4 = y^2 = e, yx = x^3y \rangle$ of order 8 by D_8, and the quaternion group $\langle x, y \mid x^4 = e, y^2 = x^2, yx = x^3y \rangle$ of order 8 by Q_8.

We follow Wild's fashion [2] for the classification of groups of order 16. Let N be a normal subgroup of G (in symbol $N \lhd G$). We denote by t_a the inner automorphism of N defined by an element $a \in G$ (namely $t_a(x) \overset{\text{def.}}{=} axa^{-1}$ for any element $x \in N$).

Suppose that $G/N \simeq C_n$ and pick any a in G such that the coset Na has order n in G/N. If we put $v = a^n$ and $\tau = t_a$, then $v \in N$, $\tau(v) = t_a(v) = aa^na^{-1} = a^n = v$, and $\tau^n = t_a^n = t_{a^n} = t_v$.

Definition 4 A quadruple (N, n, τ, v) is said to be an *extension type* if N is a group and if v in N and τ in Aut(N) are such that $\tau(v) = v$ and $\tau^n = t_v$.

Remark 1 An extension type determines the structure of group $G = \langle N, a \rangle$ uniquely.

Definition 5 The extension types (N, n, τ, v) and (N', n, σ, w) are *equivalent* if there is an isomorphism $\phi : N \to N'$ such that $\sigma = \phi \circ \tau \circ \phi^{-1}$ and $w = \phi(v)$.

Remark 2 The set Aut(G) of all automorphisms of a group G forms a group under composition of mappings. Let X generate G. Each $\theta : G \to G$ in Aut(G) is determined by its values on X. In particular Aut(C_4), Aut(C_8), Aut(K_8) and Aut(D_8) consist of the functions in **Tables 1–3**.

Remark 3 In Ref. [2], Marcel Wild denote the 14 groups of order 16 (besides the outsider $G_0 = C_2 \times C_2 \times C_2 \times C_2$) as follows (the last column shows an extension type of each group.):

$G_1 = C_2 \times C_8$	$(C_8, 2, \sigma_1, e)$
$G_2 = C_2 \ltimes_3 C_8$	$(C_8, 2, \sigma_2, e)$
$G_3 = C_2 \ltimes_5 C_8$	$(C_8, 2, \sigma_3, e)$
$G_4 = C_2 \ltimes_7 C_8$	$(C_8, 2, \sigma_4, e)$
$G_5 = Q_{16}$	$(C_8, 2, \sigma_4, x^4)$
$G_6 = C_{16}$	$(C_8, 2, \sigma_1, x)$
$G_7 = K_4 \times C_4$	$(K_8, 2, \psi_1, e)$
$G_8 = D_8 \times C_2$	$(K_8, 2, \psi_3, e)$
$G_9 = C_4 \ltimes_\tau K_4$	$(K_8, 2, \psi_5, e)$
$G_{10} = C_2 \ltimes_\tau Q_8$	$(K_8, 2, \psi_6, e)$
$G_{11} = C_2 \times Q_8$	$(K_8, 2, \psi_3, x^2)$
$G_{12} = C_4 \ltimes_\tau C_4$	$(K_8, 2, \psi_5, x^2)$
$G_{13} = C_4 \times C_4$	$(K_8, 2, \psi_1, y)$

Table 3 Aut(D_8) $\simeq D_8$.

Aut(D_8)	effect on x	effect on y	order of automorphism
α_1	x	y	1
α_2	x	xy	4
α_3	x	x^2y	2
α_4	x	x^3y	4
α_5	x^3	y	2
α_6	x^3	xy	2
α_7	x^3	x^2y	2
α_8	x^3	x^3y	2

2.3 Type 1 Gray Maps

In this subsection, we assume that H is a maximal subgroup of G with $[G : H] = 2$, and x is an arbitrary element in $G \setminus H$ and h is an arbitrary element in H. Type 1 Gray map for G is constructed as follows based on a Gray map for H.

Let us denote by $\mathbf{0}$ and $\mathbf{1}$ the vectors in $\mathbb{Z}_2^n$ whose components are all 0 and 1, respectively. Also we denote the usual concatenation of vectors by (|). Suppose $\phi : H \to \mathbb{Z}_2^n$ is a Gray map and define the map $\hat{\phi} : G \to \mathbb{Z}_2^{2n}$ by $\hat{\phi}(h) = (\phi(h) \mid \phi(h))$ and $\hat{\phi}(xh) = (\phi(h) \mid \phi(h) + \mathbf{1})$ [1]. We can easily see that $w_H(\hat{\phi}(g)) = 2w_H(\phi(g))$ for $g \in H$ and $w_H(\hat{\phi}(g)) = n$ for $g \notin H$. So the proofs of the following lemmas and theorem are routines.

Lemma 2 For all $g \in G$ we have $w_H(\hat{\phi}(g)) = w_H(\hat{\phi}(g^{-1}))$.

Lemma 3 For all $a, b \in G$ we have $w_H(\hat{\phi}(ab)) \le w_H(\hat{\phi}(a)) + w_H(\hat{\phi}(b))$.

Theorem 1 With notation as above, the map $\hat{\phi}$ is a Gray map.

Refer to Ref. [1] for the details [*2].

Remark 4 In [8], we constructed Type 1 Gray maps for all groups $G_0, G_1, \ldots, G_{12}$ and G_{13} of order 16.

2.4 Type 2 Gray Maps

In this subsection, we assume that G is isomorphic to the semidirect product of two finite 2-groups H of order 2^a and K of order 2^b, i.e. $G = H \ltimes_\psi K$ where $\psi : H \to \text{Aut}(K)$ is a group homomorphism. Suppose further that both H and K accept Gray maps $\theta_1 : H \to \mathbb{Z}_2^{n_1}$ and $\theta_2 : K \to \mathbb{Z}_2^{n_2}$, where θ_2 is compatible with ψ in the sense that for all $h \in H$

$$w_H(\theta_2(k)) = w_H(\theta_2(\psi_h(k))).$$

Then Type 2 Gray map θ for G is constructed as $\theta(hk) = (\theta_1(h) \mid \theta_2(k))$.

Theorem 2 With notation as above, the map θ is a Gray map.

Refer to [1] for the proof of Theorem 2.

*2 The proof of Theorem 1 written in Ref. [1] contains a small error caused by the definition of distance d_ϕ, but it is not essential.

Remark 5 In [8], we constructed Type 2 Gray maps for G_0, G_7, G_8, G_9, G_{12} and G_{13}.

3. New Construction Method for Gray Maps

In this section, we assume that G is an arbitrary finite group (not even necessary to be a p-group). Cayley's theorem says that every finite group can be embedded in the symmetric group of degree $|G|$ as a subgroup.

Define the mapping $g : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ as $g(u) = uP+c$ for all u in $\mathbb{Z}_2^n$, where c is a fixed element in $\mathbb{Z}_2^n$ and P is a fixed permutation matrix of order n. (A permutation matrix of order n is a $n \times n$-matrix which has exactly one 1 in each row and column and whose other entries are all 0. As is well known, a permutation matrix represents just a replacement of coordinates of vectors.) Since the mapping g above is an affine transformation over $\mathbb{Z}_2^n$, we call a mapping of this form an *affine permutation* [5] of degree n.

Our ideas to construct a Gray map for an arbitrary group is realizing Cayley's theorem over the group of affine permutations, instead of the symmetric group. The key points are that the set of all the affine permutations forms a group with respect to composition as a transformation from $\mathbb{Z}_2^n$ to itself and every affine permutation is an isometry with respect to Hamming distance.

In fact, let $g(u) = uP + c$ and $h(u) = uQ + d$ (we denote them by $[P, c]$ and $[Q, d]$, respectively) be two affine permutations. Since

$$(h \circ g)u = (uP + c)Q + d = uPQ + cQ + d,$$

the composition $h \circ g = [Q, d] \circ [P, c]$ is denoted by $[PQ, cQ + d]$ and is itself an affine permutation since PQ is a permutation matrix again.

Moreover, it is easily verified that the identity permutation is $[E, \mathbf{0}]$ and the inverse permutation of $[P, c]$ is $[P^{-1}, cP^{-1}]$. Thus, the set of all the affine permutations form a group, which we denote by $\mathcal{AP}$.

Next, let us confirm that every affine permutation $g = [P, c]$ is an isometry. Since P is a permutation matrix and c is a constant vector, clearly from definition of Hamming-distance, for any u and v in $\mathbb{Z}_2^n$

$$d_H(g(u), g(v)) = d_H(uP + c, vP + c) = d_H(uP, vP) = d_H(u, v)$$

holds.

Suppose that G is isomorphic to a subgroup G' of $\mathcal{AP}$. For simplicity, in what follows, we regard G as identical with G'. Therefore, an element $g \in G$ can be written in form $[P, c]$ by a permutation matrix P and a constant $c \in \mathbb{Z}_2^n$. We call c the *code-part* of an affine permutation $[P, c]$. The idea is that we employ the code-part c as the codeword for element $[P, c]$ in G.

Theorem 3 Let G be a subgroup of $\mathcal{AP}$ and consider the function $\phi : G \to \mathbb{Z}_2^n$ that maps each element $[P, c] \in G$ to its code-part c. Then, ϕ is a Gray map, if and only if it is an injection.

proof. Let $a = [P, c]$, $b = [Q, d]$. Then,

$$\begin{aligned} w_H(\phi(a^{-1}b)) &= w_H(\phi([P^{-1}, cP^{-1}][Q, d])) \\ &= w_H(\phi[QP^{-1}, dP^{-1} + cP^{-1}]) \\ &= w_H(dP^{-1} + cP^{-1}) = w_H(d + c) \\ &= d_H(c, d) = d_H(\phi(a), \phi(b)). \end{aligned}$$

Thus, in order to construct an n-bit Gray code for group G, we only need to search in the group of affine permutation of degree n for a subgroup isomorphic to G such that map ϕ is injective. This method is different from both Type 1 and Type 2. As examples we show how to construct some known Gray codes by this method in the rest of this section, and try to construct ones for more complicated groups in the later sections.

Since our matrices work only on binary vectors, all the vectors are denoted simply as bit strings (without commas or parentheses) in the examples.

Example 1 Let $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $c = 01$. Then, $\langle [P, c] \rangle \simeq C_4 = \langle x \mid x^4 = e \rangle$. Therefore C_4 has the following Gray map:

$$\begin{aligned} &\phi(e) &&= \phi[E, \mathbf{0}] &&= \phi[E, 00] &&= 00 \\ &\phi(x) &&= \phi[P, c] &&= \phi[P, 01] &&= 01 \\ &\phi(x^2) &&= \phi[P^2, cP + c] &&= \phi[P^2, 11] &&= 11 \\ &\phi(x^3) &&= \phi[P^3, cP^2 + cP + c] &&= \phi[P^3, 10] &&= 10 \end{aligned}$$

Example 2 Let $P_1 = P_2 = E$, $c_1 = 01$ and $c_2 = 10$. Then $\langle [P_1, c], [P_2, c_2] \rangle \simeq K_4 = \langle x, y \mid x^2 = y^2 = e, xy = yx \rangle$. Therefore K_4 has the following Gray map:

$$\begin{aligned} &\phi(e) &&= \phi[E, \mathbf{0}] &&= \phi[E, 00] &&= 00 \\ &\phi(x) &&= \phi[P_1, c_1] &&= \phi[E, 01] &&= 01 \\ &\phi(y) &&= \phi[P_2, c_2] &&= \phi[E, 10] &&= 10 \\ &\phi(xy) &&= \phi[P_2P_1, c_2P_1 + c_1] &&= \phi[E, 11] &&= 11 \end{aligned}$$

4. New Construction Method for Gray Maps for a Group of Order 8

In the literature a permutation matrix is denoted by symbol P_π, where π is a permutation of n elements, namely P_π is the matrix in which the $(i, \pi(i))$ entries are 1 and all the other entries are 0. Henceforth, we mainly employs this notation for permutation matrices. Note that multiplying a row vector by P_π permutes the components of the vector in the following way:

$$(a_1, a_2, \ldots, a_n)P_\pi = (a_{\pi^{-1}(1)}, a_{\pi^{-1}(2)}, \ldots, a_{\pi^{-1}(n)}),$$

and that $P_\pi^T = P_\pi^{-1} = P_{\pi^{-1}}$, so $(a_1, a_2, \ldots, a_n)P_\pi^T = (a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)})$.

(1) $C_8 = \langle x \mid x^8 = e \rangle \cong \langle [P_\pi^T, c] \rangle$, where $c = 0001$ and $\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)$.

(2) $K_8 = \langle x, y \mid x^4 = y^2 = e \rangle \cong \langle [P_{\pi_1}^T, c_1], [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 100$, $c_2 = 001$, $\pi_1 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$, and π_2 is the identity permutation.

(3) $D_8 = \langle x, y \mid x^4 = y^2 = e,\ xy = yx^3 \rangle \cong \langle [P_\pi^T, c_1], [P_\pi^T, c_2] \rangle$, where $c_1 = 100$, $c_2 = 001$, and $\pi_1 = \pi_2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$.

(4) $Q_8 = \langle x, y \mid x^4 = e,\ x^2 = y^2,\ xy = yx^3 \rangle \cong \langle [P_{\pi_1}^T, c_1], [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 1100$, $c_2 = 0110$, $\pi_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right)$, and $\pi_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right)$.

The cyclic group C_8 and the quaternion group Q_8 need 4 bits for their Gray codes.

5. New Type Gray Maps for a Group of Order 16

(1) $G_2 = \langle x, a \mid x^8 = a^2 = e,\ ax = x^3a \rangle \cong \langle [P_{\pi_1}^T, c_1], [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 0001$, $c_2 = 0010$, $\pi_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)$, and $\pi_2 =$

$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$.

(2) $G_3 = \langle x, a \mid x^8 = a^2 = e,\ ax = x^5 a\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2]\rangle$, where $c_1 = 0001$, $c_2 = 0101$, $\pi_1 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$, and π_2 is the identity permutation.

(3) $G_7 = \langle x, y, a \mid x^4 = y^2 = a^2 = e,\ xy = yx,\ xa = ax,\ ya = ay\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2], [P^T_{\pi_3}, c_3]\rangle$, where $c_1 = 1000$, $c_2 = 0010$, $c_3 = 0001$, $\pi_1 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$, and $\pi_2 = \pi_3$ is the identity permutation.

(4) $G_8 = \langle x, y, a \mid x^4 = y^2 = a^2 = e,\ xy = yx^3,\ xa = ax,\ ya = ay\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2], [P^T_{\pi_3}, c_3]\rangle$, where $c_1 = 1000$, $c_2 = 0010$, $c_3 = 0001$, $\pi_1 = \pi_2 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$, and π_3 is the identity permutation.

(5) $G_9 = \langle a, y, x \mid a^2 = y^2 = x^4 = e,\ ax = xya,\ ay = ya,\ xy = yx\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2], [P^T_{\pi_3}, c_3]\rangle$, where $c_1 = 1100$, $c_2 = 1111$, $c_3 = 0001$, $\pi_1 = \pi_2$ is the identity permutation, and $\pi_3 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$.

(6) $G_{12} = \langle a, x \mid a^4 = x^4 = e,\ ax = xa^3\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2]\rangle$, where $c_1 = 0100$, $c_2 = 0010$, $\pi_1 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$, and $\pi_2 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$.

(7) $G_{13} = \langle a, x \mid a^4 = x^4 = e,\ ax = xa\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2]\rangle$, where $c_1 = 0100$, $c_2 = 0110$, $\pi_1 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$, and $\pi_2 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$.

6. New Type Gray Maps for General Groups

In this section we show that our method can also construct Gray maps for several non-p-groups.

(1) $C_3 = \langle x \mid x^3 = e\rangle \cong \langle [P^T_\pi, c]\rangle$, where $c = 011$ and $\pi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.

(2) $C_5 = \langle x \mid x^5 = e\rangle \cong \langle [P^T_\pi, c]\rangle$, where $c = 00011$ and $\pi = \begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}$.

(3) $C_6 = \langle x \mid x^6 = e\rangle \cong \langle [P^T_\pi, c]\rangle$, where $c = 001$ and $\pi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.

(4) For $n \in \mathbb{N}$, $C_{2n} = \langle x \mid x^{2n} = e\rangle \cong \langle [P^T_\pi, c]\rangle$, where $c = 0\ldots01$, and $\pi = \begin{pmatrix}1&2&\ldots&n-1&n\\2&3&\ldots&n&1\end{pmatrix}$.

(5) For $n \in \mathbb{N}$, $C_{2n+1} = \langle x \mid x^{2n+1} = e\rangle \cong \langle [P^T_\pi, c]\rangle$, where $c = 0\ldots011$ and $\pi = \begin{pmatrix}1&2&\ldots&2n-1&2n&2n+1\\3&4&\ldots&2n+1&1&2\end{pmatrix}$.

(6) $D_6 = \langle x, y \mid x^3 = y^2 = e,\ xy = yx^2\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2]\rangle$, where $c_1 = 011$, $c_2 = 010$, $\pi_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, and π_2 is the identity permutation.

(7) $D_{10} = \langle x, y \mid x^5 = y^2 = e,\ xy = yx^4\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2]\rangle$, where $c_1 = 00101$, $c_2 = 01101$, $\pi_1 = \begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$, and π_2 is the identity permutation.

(8) $D_{12} = \langle x, y \mid x^6 = y^2 = e,\ xy = yx^5\rangle \cong \langle [P^T_{\pi_1}, c_1], [P^T_{\pi_2}, c_2]\rangle$, where $c_1 = 0010$, $c_2 = 0111$, $\pi_1 = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$, and π_2 is the identity permutation.

7. Summary

In Ref. [8], we constructed a Type 1 Gray map for C_8, K_8, D_8 and Q_8 over $\mathbb{Z}_2^4$, and we constructed a Type 2 Gray map for K_8 and D_8 over $\mathbb{Z}_2^3$ and showed that neither C_8 nor Q_8 can have 3-bit Gray maps. Similarly we constructed Type 1 Gray maps for all groups $G_1, G_2, \ldots, G_{13}$ of order 16 over $\mathbb{Z}_2^8$, and Type 2 Gray maps for G_7, G_8, G_9, G_{12}, G_{13} over $\mathbb{Z}_2^4$, but failed to construct 4-bit Gray maps for the other eight groups of order 16.

In this paper we showed that our method can reconstruct 3-bit Gray maps for K_8 and D_8, and can construct 4-bit Gray maps for C_8, Q_8. Similarly, the method can reconstruct 4-bit Gray maps for G_7, G_8, G_9, G_{12}, G_{13}, and such ones also for G_2, G_3.

Finally, we showed that our method is effective to several non-p-groups of simple type, namely, C_{2n}, C_{2n+1}, D_6, D_{10} and D_{12}.

Since our method is not constructive, we are trying to find a constructive method.

References

[1] Sobhani, R.: Gray isometries for finite p-groups, *Trans. Combinatorics*, Vol.2, No.1, pp.17–26 (2013).

[2] Wild, M.: The groups of order sixteen made easy, *The Mathematical Association of America*, January (2005).

[3] Hammons, A.R., Kummar, P.V., Calderbank, A.R., Sloane, N.J.A. and Sole, P.: The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, Vol.40, pp.301–319 (1994).

[4] Rotman, J.J.: *An Introduction to the Theory of Groups*, Springer (1995).

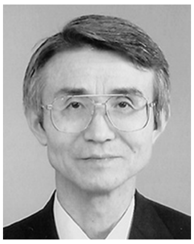
[5] Van Lint, J.H.: *Introduction to Coding Theory*, Third Edition, Springer (1999).

[6] Thomas, A.D. and Wood, G.V.: *Group Tables*, Mathematics Series 2, Shiva Publishing Limited, Kent, UK (1980).

[7] Macwilliams, F.J. and Sloane, N.J.A.: *The theory of error-correcting codes*, North-Holland, Amsterdam (1977).

[8] Sakai, K. and Sato, Y.: Construction of Gray maps for groups of order 16, available from ⟨http://www.arXiv.org/1609.03690v1/cs.IT/13Sep2016⟩.

Ko Sakai was born in 1953. He recieved his Ph.D. from Tokyo Institute of Technology in 1990. He has been an associate professor at University of Tsukuba since 1995. He has been interested in applied algebra and logic for more than 30 years.



Yutaka Sato was bone in 1949. He is a student of Graduate School of Pure and Applied Sciences, University of Tsukuba. His current research interest is algebraic coding theory.