Journal of Information Processing Vol.26 345–349 (Apr. 2018)

[DOI: 10.2197/ipsjjip.26.345]

Regular Paper

A Method for Constructing a Gray Map for a Group Based on Its Semidirect-product Structure

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

Received: June 11, 2017, Accepted: January 15, 2018

Abstract: In this paper we propose a method for constructing a Gray map for a group. In an earlier paper, we suggested a new design principle of Gray maps for groups and tried to apply it to several concrete groups. Though the trial had some success, the method is not very constructive. In this paper we try to design a more constructive method based on the semidirect-product structure of the target group.

Keywords: Gray map, semidirect product of groups

1. Introduction

Reza Sobhani [1] designed two methods for constructing Gray maps for finite p-groups and called them Type 1 and Type 2. Both methods construct a Gray map as an extension of one for a smaller group. Type 1 method constructs a Gray map from one for a maximal subgroup of the target group naturally, but it doubles the length of the resulting code. Type 2 method in contrast, generally constructs a shorter code than Type 1. However, the application of Type 2 is limited to groups with specific structure, and indeed our trial [8] on Type 2 construction succeeded for only 6 groups among all the groups of order 16.

So, we proposed a new design policy for an arbitrary finite group (not necessary to be a p-group) in Ref. [9]. Our idea for constructing an n-bit Gray code for group G is to search in the group of affine permutation of degree n for a subgroup isomorphic to G with a suitable property. This method is different from both Type 1 and Type 2.

In Ref. [9], we showed that our method can reconstruct 4-bit Gray maps for G_2, G_3, G_7, G_8, G_9, G_{12} and G_{13} [*1]. Also we showed that our method is effective for several non-p-groups of simple type, namely, C_{2n}, C_{2n+1}, D_6, D_{10} and D_{12}. However, since our construction in Ref. [9] is somewhat ad hoc, we propose a more constructive method in this paper. After mathematical preparation in Section 2, we give a rough idea of the method theoretically in Section 3 and a systematic procedure in Section 4. We try to apply it to several groups of order 16 in Section 5.

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 a Gray map 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

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

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

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

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

$$w(\phi(a^{-1}b)) = d(\phi(a), \phi(b))$$

holds for all a, b in G.

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

(1) For $g \in G$ we have $w(\phi(g)) = 0$ iff $g = e$, where e stands for the identity of G,
(2) For all g in G we have $w(\phi(g)) = w(\phi(g^{-1}))$,
(3) For all x, y in G we have $w(\phi(xy)) \le w(\phi(x)) + w(\phi(y))$.

Refer to Ref. [9] for the proof of Lemma 1.

We define a map $d_\phi : G \times G \to \mathbb{N} \cup \{0\}$ by $d_\phi(a, b) = d(\phi(a), \phi(b))$. 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 $\langle x \mid x^n = e \rangle$, the *Klein four group* $K_4 = C_2 \times C_2$ as $\langle x, y \mid x^2 = y^2 = e, xy = yx \rangle$, and $C_2^3 = C_2 \times C_2 \times C_2$ is represented as $\langle x, y, z \mid x^2 = y^2 = z^2 = e, yx = xy, zx = xz, yz = zy \rangle$. 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 group $C_4 \times C_2$ appears frequently in this paper we denote it by K_8 as in Ref. [2].

Similarly, we denote the dihedral group $\langle x, y \mid x^n = y^2 =$

[1] Faculty of Pure and Applied Sciences, University of Tsukuba, Tsukuba, Ibaraki 305–8577, Japan
[2] Graduate School of Pure and Applied Sciences, University of Tsukuba, Tsukuba, Ibaraki 305–8577, Japan
[a)] ksakai@math.tsukuba.ac.jp
[b)] yutaka.kinjiro@gmail.com

[*1] We follow Wild [2] for the name of groups of order 16. Refer to Remark 3 for each group G_i.

$e,\ yx = x^{n-1}y\rangle$ of order $2n$ by D_{2n}, 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.

Let N be a normal subgroup of G (in symbol $N \lhd G$). We denote by ψ_a the conjugation automorphism of N defined by element $a \in G$ (namely $\psi_a(x) \stackrel{\text{def.}}{=} axa^{-1}$ for 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 $\tau = \psi_a$, then $v \in N, \tau(v) = \psi_a(v) = aa^n a^{-1} = a^n = v$, and $\tau^n = {\psi_a}^n = \psi_{a^n} = \psi_v$.

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

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

Remark 2 The set $\mathrm{Aut}(G)$ of all automorphisms of a group G forms a group under composition of mappings. Let X generate G. Then each $\theta : G \to G$ in $\mathrm{Aut}(G)$ is determined by its values on X. In particular $\mathrm{Aut}(C_4)$, $\mathrm{Aut}(C_8)$, $\mathrm{Aut}(K_8)$ and $\mathrm{Aut}(D_8)$ consist of the following respective functions [2], [9]:

$\mathrm{Aut}(C_4)$ and $\mathrm{Aut}(C_8) \simeq K_4$

$\mathrm{Aut}(C_4)$	effect on x	$\mathrm{Aut}(C_8)$	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

$\mathrm{Aut}(K_8) \simeq D_8$

$\mathrm{Aut}(K_8)$	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

$\mathrm{Aut}(D_8) \simeq D_8$

$\mathrm{Aut}(D_8)$	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

The group $\mathrm{Aut}(Q_8)$ is isomorphic to symmetric group S_4 and the group $\mathrm{Aut}(C_2^3)$ consists of $7 \times 6 \times 4 = 168$ elements.

Remark 3 In Ref. [2], Marcel Wild denotes the 14 groups of order 16 (besides the outsider $G_0 = C_2 \times C_2 \times C_2 \times C_2$) as follows (we add the last column to show extension types [*2] of each group.):

[*2] An extension type determines the group structure, but a group can have several extension types even if the base group is fixed. We select a few of the specific extension types for the reason described later.

$G_1 = C_8 \times C_2$ $(C_8, 2, \sigma_1, e),\ (K_8, 2, \psi_1, x)$

$G_2 = C_8 \rtimes_{\sigma_2} C_2$ $(C_8, 2, \sigma_2, e),\ (D_8, 2, \alpha_8, x^2),\ (Q_8, 2, \beta_1, e)$

$G_3 = C_8 \rtimes_{\sigma_3} C_2$ $(C_8, 2, \sigma_3, e),\ (K_8, 2, \psi_8, x)$

$G_4 = C_8 \rtimes_{\sigma_4} C_2$ $(C_8, 2, \sigma_4, e),\ (D_8, 2, \alpha_6, e)$

$G_5 = Q_{16}$ $(C_8, 2, \sigma_4, x^4),\ (Q_8, 2, \beta_1, x^2)$

$G_6 = C_{16}$ $(C_8, 2, \sigma_1, x)$

$G_7 = C_4 \times K_4$ $(K_8, 2, \psi_1, e),\ (C_2^3, 2, \gamma_1, z),\ (C_4, 4, \varphi_1, e)$

$G_8 = D_8 \times C_2$ $(K_8, 2, \psi_3, e),\ (D_8, 2, \alpha_1, e),\ (C_2^3, 2, \gamma_2, e)$

$G_9 = K_4 \rtimes_{\sigma} C_4$ $(K_8, 2, \psi_7, e),\ (C_2^3, 2, \gamma_3, yz),\ (K_4, 4, \sigma, e)$

$G_{10} = Q_8 \rtimes_{\tau_6} C_2$ $(K_8, 2, \psi_6, e),\ (D_8, 2, \alpha_3, e),\ (Q_8, 2, \beta_2, e)$

$G_{11} = Q_8 \times C_2$ $(K_8, 2, \psi_3, x^2),\ (Q_8, 2, \beta_3, e)$

$G_{12} = C_4 \rtimes_{\varphi_2} C_4$ $(K_8, 2, \psi_5, x^2),\ (C_4, 4, \varphi_2, e)$

$G_{13} = C_4 \times C_4$ $(K_8, 2, \psi_1, y),\ (C_4, 4, \varphi_1, e),$

where the automorphisms of Q_8 and C_2^3 in the table above are as follows:

$\beta_1 : Q_8 \to Q_8$ $(x \mapsto x^3,\ y \mapsto xy),$

$\beta_2 : Q_8 \to Q_8$ $(x \mapsto x,\ y \mapsto x^2y),$

$\beta_3 : Q_8 \to Q_8$ $(x \mapsto x,\ y \mapsto y),$

$\gamma_1 : C_2^3 \to C_2^3$ $(x \mapsto x,\ y \mapsto y,\ z \mapsto z),$

$\gamma_2 : C_2^3 \to C_2^3$ $(x \mapsto x,\ y \mapsto xy,\ z \mapsto z),$

$\gamma_3 : C_2^3 \to C_2^3$ $(x \mapsto x,\ y \mapsto xy,\ z \mapsto xz).$

2.3 Type 2 Gray Maps

In this subsection, we assume that G is isomorphic to the semidirect product $K \rtimes_\psi H$ of two finite 2-groups K and H where $\psi : H \to \mathrm{Aut}(K)$ is the conjugation homomorphism, i.e., ψ_h is the automorphism on K defined by $\psi_h(k) = hkh^{-1}$. 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 $h \in H$ and $k \in K$

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

Every element $g \in G$ can be written uniquely in form kh by an element $k \in K$ and an element $h \in H$. Then, define a map θ from G to $\mathbb{Z}_2^{n_1+n_2}$ as

$$\theta(g) = \theta(kh) = (\theta_2(k) \mid \theta_1(h)),$$

where we denote the usual concatenation of vectors by $(\ |\ )$.

Theorem 1 (Sobhani [1]) The map θ defined above is a Gray map.

Proof: Let $a = kh$, $b = k'h'$ be elements of G. Then

$$\begin{aligned} w(\theta(a^{-1}b)) &= w(\theta(h^{-1}k^{-1}k'h')) = w(\theta(\psi_{h^{-1}}(k^{-1}k')h^{-1}h')) \\ &= w(\theta_2(\psi_{h^{-1}}(k^{-1}k')) \mid \theta_1(h^{-1}h')) \\ &= w(\theta_2(\psi_{h^{-1}}(k^{-1}k'))) + w(\theta_1(h^{-1}h')) \\ &= w(\theta_2(k^{-1}k')) + w(\theta_1(h^{-1}h')) \\ &= d(\theta_2(k), \theta_2(k')) + d(\theta_1(h), \theta_1(h')) \\ &= d((\theta_2(k) \mid \theta_1(h)), (\theta_2(k') \mid \theta_1(h'))) \\ &= d(\theta(kh), \theta(k'h')) = d(\theta(a), \theta(b)). \end{aligned}$$

Since θ_1 and θ_2 are injections, θ is clearly an injection.

Remark 4 In Ref. [8], we constructed Type 2 Gray maps for G_0, G_7, G_8, G_9, G_{12} and G_{13}.

However, compatible map θ_2 may not exist and, even if one exists, it is not very easy to find.

2.4 Embedding to the Group of Affine Permutations and the Induced Gray Map

In this subsection, we assume that G is an arbitrary finite group (not necessary to be a p-group).

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 degree n. (A permutation matrix of degree 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 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 for constructing a Gray map for an arbitrary group are to embed the target group in the group of affine permutations. The key points are that the set of all affine permutations forms a group with respect to the composition as a transformation from $\mathbb{Z}_2^n$ to itself and that every affine permutation is an isometry with respect to the 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 of degree n. Then, the composition $h \circ g = [Q, d] \circ [P, c]$ is denoted by $[PQ, cQ + d]$ and is itself an affine permutation. Moreover, the identity permutation is $[E, \mathbf{0}]$, where we denote by $\mathbf{0}$ the vector whose components are all 0, and the inverse permutation of $[P, c]$ is $[P^{-1}, cP^{-1}]$. Thus, the set of all affine permutations of degree n forms a group, which we denote by $\mathcal{AP}(n)$.

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 the definition of the Hamming-distance, for any u and v in $\mathbb{Z}_2^n$

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

holds.

Suppose that G is isomorphic to a subgroup G' of $\mathcal{AP}(n)$. 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 2 Let G be a subgroup of $\mathcal{AP}(n)$ 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.

Refer to Ref. [9] for the proof of Theorem 2.

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.

Remark 5 A permutation matrix is denoted by the 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 employ 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

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

3. Extension of Embedding Based on Semidirect-product Structures

In this section we assume that G is isomorphic to the semidirect product $G \simeq K \rtimes_\psi H$ of a normal subgroup K and a subgroup H where ψ is the conjugation homomorphism. Suppose further that both K and H can be embedded to the group of affine permutations (described in Section 2.4), namely, there exist embeddings $\phi_K : K \to \mathcal{AP}(m)$, $\phi_H : H \to \mathcal{AP}(n)$. Assuming that $\phi_K(k) = [P_k, c_k]$ for $k \in K$ and $\phi_H(h) = [Q_h, d_h]$ for $h \in H$, we try to define an embedding $\phi_G : G \to \mathcal{AP}(m + n)$.

Any element g in G can be written in form kh by an element $k \in K$ and an element $h \in H$ uniquely. We want to embed $g = kh$ in form $\phi_G(kh) = \left[\begin{pmatrix} P_{kh} & O \\ O & Q_h \end{pmatrix}, (c_{kh} \mid d_h)\right]$, where P_{kh} is some permutation matrix of degree m. In particular, assume that $k \in K$ is embedded in form $\phi_G(ke) = \left[\begin{pmatrix} P_k & O \\ O & E \end{pmatrix}, (c_k \mid \mathbf{0})\right]$ as an element ke in G. Select an element $a \in G \setminus K$ and let us embed it in form $\phi_G(a) = \left[\begin{pmatrix} P_a & O \\ O & Q_h \end{pmatrix}, (c_a \mid d_h)\right]$ where a is written as kh by $k \in K$ and $h \in H$. Then, the element $\psi_a(k) = aka^{-1}$ is embedded to

$$\left[\begin{pmatrix} P_a^{-1}P_kP_a & O \\ O & E \end{pmatrix}, (c_aP_a^{-1}P_kP_a + c_kP_a + c_a \mid \mathbf{0})\right].$$

So, in order for such an embedding to be successful, it is necessary that

$$P_a^{-1}P_kP_a = P_{aka^{-1}}, \tag{A}$$

$$c_aP_a^{-1}P_kP_a + c_kP_a + c_a = c_{aka^{-1}}. \tag{B}$$

If we put $c_a = \mathbf{0}$, then the latter condition (B) reduces to

$$c_kP_a = c_{aka^{-1}}. \tag{B'}$$

In this case, since P_a is a permutation, we have $w(c_k) = w(c_{aka^{-1}})$ and Theorem 1 guarantees that the embedding induces a Gray map. Therefore, a promising candidate for $\phi_G(a)$ is $\left[\begin{pmatrix} P_a & O \\ O & Q_h \end{pmatrix}, (\mathbf{0} \mid d_h)\right]$ with P_a satisfying conditions (A) and (B'). Moreover, if an element $g \in G$ has a code-part of form $(\mathbf{0} \mid d_h)$ and the coset Ka has order n in $H \simeq G/K$, then $\phi_G(a^n)$ is written as $\left[\begin{pmatrix} {P_a}^n & O \\ O & E \end{pmatrix}, (\mathbf{0} \mid \mathbf{0})\right]$. So, in order the code part to be injective, a must have order n also in G and ${P_a}^n$ must be E. Therefore, if we want to give a code of form $(\mathbf{0} \mid d_h)$ to element a, we can further limit the candidate a and P_a as described above.

4. A Recipe of Semidirect-product Construction of Gray Maps for Groups of Order 16

Guided by the previous section, here we describe a design method of Gray maps for groups of order 16 based on the semidirect-product structure. Our recipe is as follows:

(1) If G has extension type $(K, 2, \tau, e)$ and K is embedded in $\mathcal{AP}(n)$ by ϕ_K, then:
  (1-1) For any $k \in K$ define $\phi_G(k) = \left[\begin{pmatrix} P_k & O \\ O & 1 \end{pmatrix}, (c_k \mid 0)\right]$, where $\phi_K(k) = [P_k, c_k]$.
  (1-2) Select an element a of order 2 in $G \setminus K$.
  (1-3) Search for a permutation matrix P_a of degree n satisfying ${P_a}^2 = E$, (A), (B') and define $\phi_G(a) = \left[\begin{pmatrix} P_a & O \\ O & 1 \end{pmatrix}, (\mathbf{0} \mid 1)\right]$,
  (1-4) Since the other values of ϕ_G are automatically determined, check if ϕ_G successfully embeds G to $\mathcal{AP}(n+1)$.

(2) If G has extension type $(K, 4, \tau, e)$ and K is embedded in $\mathcal{AP}(n)$ by ϕ_K, then:
  (2-1) For any $k \in K$ define $\phi_G(k) = \left[\begin{pmatrix} P_k & O \\ O & E \end{pmatrix}, (c_k \mid 00)\right]$, where $\phi_K(k) = [P_k, c_k]$.
  (2-2) Select an arbitrary element a of order 4 in $G \setminus K$.
  (2-3) Search for a permutation matrix P_a of degree n satisfying ${P_a}^4 = E$, (A), (B') and define $\phi_G(a) = \left[\begin{pmatrix} P_a & O \\ O & P \end{pmatrix}, (\mathbf{0} \mid 10)\right]$, where P is the permutation matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
  (2-4) Since the other values of ϕ_G are automatically determined, check if ϕ_G successfully embeds G to $\mathcal{AP}(n+2)$.

5. Construction Examples of Gray Maps for Groups of Order 16

(1) $G_1 = \langle x, a \mid x^8 = a^2 = e,\ xa = ax \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 10000$, $c_2 = 00001$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 4&1&2&3&5 \end{smallmatrix}\right)$ and π_2 is the identity permutation.

(2) $G_4 = \langle x, a \mid x^8 = a^2 = e,\ xa = ax^7 \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 10000$, $c_2 = 00001$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 4&1&2&3&5 \end{smallmatrix}\right)$ and $\pi_2 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 4&3&2&1&5 \end{smallmatrix}\right)$.

(3) $G_7 = \langle x, y, a \mid x^4 = y^2 = a^2 = e,\ xy = yx,\ xa = ax,\ ya = ay \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2],\ [P_{\pi_3}^T, c_3] \rangle$, where $c_1 = 1000$, $c_2 = 0010$, $c_3 = 0001$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&1&3&4 \end{smallmatrix}\right)$ and π_2, π_3 are the identity permutations.

(4) $G_8 = \langle x, y, a \mid x^4 = y^2 = a^2 = e,\ xy = yx,\ xa = ax^3,\ ya = ay \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2],\ [P_{\pi_3}^T, c_3] \rangle$, where $c_1 = 1000$, $c_2 = 0010$, $c_3 = 0001$, $\pi_1 = \pi_3 = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&1&3&4 \end{smallmatrix}\right)$ and π_2 is the identity permutation.

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

(6) $G_9 = \langle x, y, a \mid x^2 = y^2 = a^4 = e,\ xy = yx,\ ax = ya,\ ay = xa \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2],\ [P_{\pi_3}^T, c_3] \rangle$, where $c_1 = 1000$, $c_2 = 0100$, $c_3 = 0010$, $\pi_3 = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&1&4&3 \end{smallmatrix}\right)$ and π_1, π_2 are the identity permutations.

(7) $G_{10} = \langle x, y, a \mid x^4 = e,\ y^2 = x^2,\ xy = yx^3,\ xa = ax,\ ay = x^2ya \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2],\ [P_{\pi_3}^T, c_3] \rangle$, where $c_1 = 11000$, $c_2 = 01100$, $c_3 = 00001$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 3&4&1&2&5 \end{smallmatrix}\right)$ and $\pi_2 = \pi_3 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 2&1&4&3&5 \end{smallmatrix}\right)$.

(8) $G_{11} = \langle x, y, a \mid x^4 = e,\ y^2 = x^2,\ xy = yx^3,\ xa = ax,\ ay = ya \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2],\ [P_{\pi_3}^T, c_3] \rangle$, where $c_1 = 11000$, $c_2 = 01100$, $c_3 = 00001$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 3&4&1&2&5 \end{smallmatrix}\right), \pi_2 = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 2&1&4&3&5 \end{smallmatrix}\right)$ and π_3 is the identity permutation.

(9) $G_{12} = \langle x, a \mid x^4 = a^4 = e,\ xa = ax^3 \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 1000$, $c_2 = 0010$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&1&3&4 \end{smallmatrix}\right)$, and $\pi_2 = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&1&4&3 \end{smallmatrix}\right)$.

(10) $G_{13} = \langle x, a \mid x^4 = a^4 = e,\ xa = ax \rangle \simeq \langle [P_{\pi_1}^T, c_1],\ [P_{\pi_2}^T, c_2] \rangle$, where $c_1 = 1000$, $c_2 = 0010$, $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&1&3&4 \end{smallmatrix}\right)$, and $\pi_2 = \left(\begin{smallmatrix} 1&2&3&4 \\ 1&2&4&3 \end{smallmatrix}\right)$.

6. Summary

We propose a constructive method to design Gray maps for groups of order 16 in this paper.

We have shown that our method can construct Gray maps for several groups of order 16, namely, G_1, G_4, G_7, G_8, G_9, G_{10}, G_{11}, G_{12} and G_{13}. This method required less time and effort to design a Gray map than that in the previous paper [9].

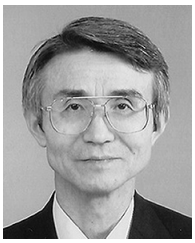
However, our recipe failed to construct Gray maps for $G_5 = Q_{16}$ and $G_6 = C_{16}$ because the groups do not have an extension type of form $(K, 2, \tau, e)$ and so does it for $G_2 = (C_8, 2, \sigma_2, e)$ and $G_3 = (C_8, 2, \sigma_3, e)$ because $w(c_x) \neq w(c_{\sigma_2(x)})$ and $w(c_x) \neq w(c_{\sigma_3(x)})$.

Our next theme is to find a new recipe effective for the failed groups.

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*, Vol.112, No.1, pp.20–31 (Jan. 2005).
[3] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. and Solé, 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*, 3rd ed., 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⟩.
[9] Sakai, K. and Sato, Y.: A New Construction Method of Gray Maps for Groups and its Application to the Groups of Order 16, *IPSJ Digital Courier*, Vol.58, No.8 (2017) (online), available from ⟨https://ipsj.ixsq.nii.ac.jp/ej/⟩.

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 recieved his Ph.D. from University of Tsukuba in 2017. He has been a visiting researcher at University of Tsukuba since 2018. His current research interest is algebraic coding theory.