Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®
Discrete Mathematics 277 (2004) 87–100

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

On the hardness of counting problems of complete mappings

Jieh Hsiang[a,1], D. Frank Hsu[b], Yuh-Pyng Shieh[a,1]

[a] *Department of Computer Science and Information Engineering, National Taiwan University, Taipei 106, Taiwan*

[b] *Department of Computer and Information Science, Fordham University, LL813, 113 West 60th Street, New York, NY 10023, USA*

Received 2 May 2002; received in revised form 2 May 2003; accepted 19 May 2003

Abstract

A *complete mapping* of an algebraic structure $(G, +)$ is a bijection $f(x)$ of G over G such that $f(x)=x+h(x)$ for some bijection $h(x)$. A question often raised is, given an algebraic structure G, how many complete mappings of G there are. In this paper we investigate a somewhat different problem. That is, how difficult it is to count the number of complete mappings of G. We show that for a *closed structure*, the counting problem is #P-complete. For a closed structure with a *left-identity* and *left-cancellation law*, the counting problem is also #P-complete. For an *abelian group*, on the other hand, the counting problem is beyond the #P-class. Furthermore, the famous counting problems of n-queen and toroidal n-queen problems are both beyond the #P-class.
© 2003 Elsevier B.V. All rights reserved.

Keywords: #P-completeness; Counting problem; Complete mapping; n-Queen problem

1. Overview

A *complete mapping* of an algebraic structure $(G, +)$ is a bijection $f(x)$ of G over G such that $f(x) = x + h(x)$ for some bijection $h(x)$. For example, $(1, 2, 4)(3, 6, 5)$ is a complete mapping of $(Z_7, +)$.

[1] Research supported in part by Grant NSC 90-2213-E-002-110 and Grant NSC 90-2811-E-002-044 of the National Science Council of the Republic of China.

E-mail addresses: hsiang@csie.ntu.edu.tw (J. Hsiang), hsu@trill.cis.fordham.edu (D.F. Hsu), arping@turing.csie.ntu.edu.tw (Y.-P. Shieh).

doi:10.1016/S0012-365X(03)00176-6

x	0	1	2	3	4	5	6	Cycle structure
$f(x)=x+h(x)$	0	2	4	6	1	3	5	(1,2,4)(3,6,5)
$h(x)$	0	1	2	3	4	5	6	

This concept for groups was first introduced by Mann [10], who used it to construct orthogonal Latin squares. We note that the mapping $f(x)$ so defined here was called *orthomorphism* by Johnson et al. [9] in 1961 and the mapping $h(x)$ was defined as complete mapping by Paige [11] in 1952. While other terminologies have been used, the most common alternative for complete mapping has been *orthogonal mapping*, a term first used by Bose et al. [3] in 1960. We also note that in this context, complete mapping and orthomorphism are sort of dual to each other. If $f(x)$ is an orthomorphism of a group G, then $h(x) = -x + f(x)$ is a complete mapping (in the sense of Paige). Conversely, if $f(x)$ is a complete mapping, then $g(x) = x + f(x)$ is an orthomorphism. Because of this tight relationship, the studies of complete mappings or orthomorphisms bear strong similarities and the choice to pick complete mapping or orthomorphism depends heavily on its applications.

Due to the importance of a complete mapping of a group $(G,+)$ in constructing algebraic structures, such as left neofields, and combinatorial and experimental configurations, such as Mendelsohn designs, the enumeration problems have been studied. Johnson et al. [9] in 1961 studied orthomorphisms and their relations to the constructions of mutually orthogonal Latin squares and finite projection planes. They obtained criteria using orthomorphisms that enable them to say whether a given set of mutually orthogonal Latin squares may be extended. They also derived properties that make computation faster. They have successfully obtained a new set of 5 mutually orthogonal Latin squares of order 12.

In 1980, Hsu [5] studied cyclic neofields (an algebraic structure $(N,+,*)$ so that $(N,+)$ is a quasigroup and $(N\setminus\{0\},*)$ is a cyclic group) and used complete mappings of a group G ($|G|=n$) to construct cyclic neofields N of order $n+1$. By identifying each cyclic neofield as the exponents of its presentation function, Hsu [5] successfully enumerated all cyclic neofields of orders $v \leqslant 10$ (hence all complete mappings of a cyclic group G of odd order $|G|=n\leqslant 9$). In 1991, Hsu [6] used a group of operators (from the set of complete mappings to itself) to classify the set of complete mappings on a cyclic group Z_n. In particular, the list of all complete mappings was exhibited for the cyclic group of order $\leqslant 9$.

For a group $(G,+)$, if $f(x)$ is a complete mapping then for all $c\in G$, $c+f(x)$ is also a complete mapping. Therefore without loss of generality, we may assume $f(0)=0$ (where 0 is the identity of G) and call f a *standard* complete mapping. Thus, the number of complete mappings of a group G is a multiple of $|G|$. In 2000, Hsiang et al. [16] presented #(CM(G)) (the number of standard complete mappings in a group G) for all group G with $|G|\leqslant 19$. Recently, Shieh [15] computed #(CM(G)) for all group G with $|G|\leqslant 23$ and obtained #(CM(Z_{23}))$=19,686,730,313,955$. The following is a list of all known non-zero #(CM(Z_n)):

n	1	3	5	7
$\#(CM(Z_n))$	1	1	3	19
n	9	11	13	15
$\#(CM(Z_n))$	225	3,441	79,259	2,424,195
n	17	19	21	23
$\#(CM(Z_n))$	94,417,089	4,613,520,889	275,148,653,115	19,686,730,313,955

A *strong complete mapping* is a complete mapping $f(x)$ such that $x + f(x)$ is also a permutation. This term was first used by Hsu and Keedwell [7], in which they gave a construction for strong complete mappings of odd order elementary abelian groups. Anderson [2] called them *strong orthomorphisms* and used them in the construction of strong partial starters, and Horton [4] called these strong permutations and used them in the construction of strong starters. A strong complete mapping can be seen as a solution to the *modulo* n-queen problem which is also called *toroidal* n-queen problem by Rivin et al. [14].

In this paper, we focus on the counting problems of complete mappings of various closed structures. Instead of finding the actual numbers of complete mappings, we focus on the hardness of the counting problems in terms of complexity classes, in particular the #P-classes, and present some of our findings here.

(1) The counting problem of complete mappings of a *closed structure* is #P-complete.
(2) The counting problem of complete mappings of a closed structure with an *identity* is also #P-complete.
(3) The counting problem of complete mappings of a closed structure with a *left-identity* and *left-cancellation law* is still #P-complete.
(4) The counting problem of complete mappings of a *cyclic group* is beyond the #P-class.
(5) The counting problem of complete mappings of an *abelian group* is also beyond the #P-class.
(6) The counting problems of the n-queen problems and the toroidal n-queen problems are both beyond the #P-class.

2. Variants of complete mappings

Definition 1. Let G be a finite set and $+$ be a function from $G \times G$ to G.

(1) Then $(G, +)$ is called a *closed structure*.
(2) If for any $x, y \in G$, there exist unique z and w such that $z + x = x + w = y$, then $(G, +)$ is called a *quasigroup*.

(3) If $(G,+)$ is a quasigroup and there exists an $e \in G$ such that $\forall x \in G, e+x=x+e=x$, then $(G,+)$ is called a *loop*.
(4) If $(G,+)$ is a loop and $\forall x,y,z \in G$, we have $(x+y)+z=x+(y+z)$, then $(G,+)$ is called a *group*.

Definition 2. Let $(G,+)$ be a closed structure. A permutation $f(x)$ of G is a *complete mapping* if there exists a permutation $h(x)$ of G such that $f(x)=x+h(x)$. We also call $h(x)$ a *transversal* of G. A complete mapping (and a transversal) of a quasigroup, loop, or group can be defined similarly.

Definition 3. Let $(G,+)$ be a closed structure. A permutation $f(x)$ of G is a *strong complete mapping* if $f(x)$ is both a complete mapping and a transversal of G.

Definition 4. For a loop or a group $(G,+)$, a complete mapping $f(x)$ is called *standard* if f maps the identity 0 of G to 0. We use $\#(\mathrm{CM}(G))$ to denote the number of standard complete mappings and $\#(\mathrm{SCM}(G))$ the number of standard strong complete mappings.

3. Hardness of the counting problems of complete mappings

Let $M=\{1,2,3,\ldots,n\}$ and $\mathrm{Perm}(M)=\{\pi|\pi \textit{ is a permutation of } M\}$. Given an $n \times n$ matrix A, the *permanent* of A is defined as $\sum_{\pi\in\mathrm{Perm}(M)}\prod_{i=1}^{n} A_{i,\pi(i)}$. In 1979, Valiant [17] proved that the evaluation of the permanent of an $n\times n$ matrix of 0's and 1's is #P-complete. We will use this fact to prove our results.

Definition 5. Let Q be a binary relation.

- Q is *polynomially balanced* if there exists a polynomial $p(x)$ such that for any $(x,y)\in Q$, we have $|x| \leqslant p(|y|)$ and $|y| \leqslant p(|x|)$.
- Q is *polynomial-time decidable* if given x,y, we can decide whether $(x,y)\in Q$ in polynomial time.

Definition 6.

- *#P-class*
  Let Q be a polynomially balanced, polynomial-time decidable binary relation. The *counting problem associated with* Q, denoted by C_{Q}, is the following: Given x, how many y's are there such that $(x,y)\in Q$? (The output is assumed to be an integer in binary). We denote by *#P* the class of all counting problems associated with polynomially balanced polynomial-time decidable binary relations.
- *Z-reduction*
  Let C_{P} and C_{Q} be two problems in the #P-class. A *Z-reduction* from C_{P} to C_{Q} is a pair of polynomial time computable functions (R,S) such that R maps an

instance x of C_{P} to an instance $R(x)$ of C_{Q}, and S maps $C_{\mathrm{Q}}(R(x))$ back to $C_{\mathrm{P}}(x)$.

- *#P-completeness*
  A counting problem C_{Q} is #P-*complete* if C_{Q} is in the #P-class and every #P problem C_{P} can be reduced to C_{Q}.

Valiant defined #P-completeness using Turing reductions [17]. The definition we adopted here (Z-reduction) was given by Zankó [18], who used it to prove that (0,1)-permanent is #P-complete.

Lemma 1. *The counting problems of transversals and complete mappings of a closed structure* $(G,+)$ *are both in the #P-class.*

Proof. (1) Let $Q=\{((G,+),h(x))|(G,+)$ is a closed structure and $h(x)$ is a transversal of $(G,+)\}$. It is easy to check that Q is polynomially balanced. Given a permutation $h(x)$ of G. It can also be checked in polynomial time whether $\{x+h(x)|x\in G\}=G$. Thus Q is polynomial time decidable, and the counting problem of transversals is in the #P-class.

(2) Let $Q=\{((G,+),f(x))|(G,+)$ is a closed structure and $f(x)$ is a complete mapping of $(G,+)\}$. It is easy to check that Q is polynomially balanced. Given a permutation $f(x)$ of G, let $A=\{a_{i,j}\}$ be an $n\times n$ matrix such that $a_{i,j}=1$ if and only if $i+j=f(i)$. Then a transversal $h(x)$ that makes $f(x)$ a complete mapping is a permutation such that $a_{i,h(i)}=1$ for all i. We construct a bipartite graph $B=(U,V,E)$ where $U=\{u_1,\dots u_n\}$ and $V=\{v_1,\dots v_n\}$ are two sets of nodes, and $E\subset U\times V$ is a set of edges defined as $(u_i,v_j)\in E$ if $a_{i,j}=1$. A *perfect matching* in a bipartite graph is a set $M\subset E$ of n edges, such that for any two edges $(u,v),(u',v')\in M$, $u\neq u'$ and $v\neq v'$. Thus, the existence problem for a transversal $h(x)$ that makes $f(x)$ a complete mapping is the same as the existence problem of a perfect matching. Since it is well-known that the existence of a perfect matching can be decided in $\mathrm{O}(n^3)$ [12], the existence problem for h can also be checked in polynomial time. Thus Q is polynomial time decidable, and the counting problem for complete mappings is in the #P-class. □

Theorem 2. *The counting problems for transversals and complete mappings of a closed structure with identity are both #P-complete.*

Proof. For convenience, we define $C_{\mathrm{P}}, C_{\mathrm{T}}$, and C_{C}.

(1) Let C_{P} be the evaluation problem of the *permanent* of an $n\times n$ matrix of 0’s and 1’s.

(2) Let C_{T} be the counting problem of *transversals* of a closed structure with identity.

(3) Let C_{C} be the counting problem of *complete mappings* of a closed structure with identity.

We will first reduce C_{P} to C_{T} by a Z-reduction (R,S). Then with the same (R,S), we reduce C_{P} to C_{C}.

Given an $n \times n$ matrix $A_{i,j}$ of 0's and 1's, we construct $R(A) = (G,+)$ as follows. Let $M = \{1,2,3,\ldots,n\}$ and $G = \{0,1,2,3,\ldots,n,\triangle\}$. For all $a,b \in M$, we define

(1) $a+b=b$ if $A_{a,b}=1$,
(2) $a+b=\triangle$ if $A_{a,b}=0$,
(3) $a+\triangle=\triangle+a=\triangle$,
(4) $\triangle+\triangle=\triangle$,
(5) $0+0=0$,
(6) $0+a=a+0=a$,
(7) $0+\triangle=\triangle+0=\triangle$.

By the above definition, 0 is the identity of $(G,+)$. By the definition of the permanent (permanent$(A) = \sum_{\pi} \prod_{i=1}^{n} A_{i,\pi(i)}$), we have that the permanent of A is the number of all permutations π of M such that $A_{i,\pi(i)}=1$ for all $i \in M$. For any permutation π of M, we define h_π as a transversal of G by $h_\pi(0)=0$, $h_\pi(\triangle)=\triangle$ and $h_\pi(x)=\pi(x)$ for $x \neq 0,\triangle$. For example, given

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

we construct $G=\{0,1,2,3,4,\triangle\}$ and

$$(G,+) = \begin{array}{|c|c|cccc|c|}
\hline
+ & 0 & 1 & 2 & 3 & 4 & \triangle \\
\hline
0 & 0 & 1 & 2 & 3 & 4 & \triangle \\
\hline
1 & 1 & 1 & 2 & \triangle & \triangle & \triangle \\
2 & 2 & \triangle & 2 & \triangle & 4 & \triangle \\
3 & 3 & 1 & \triangle & 3 & 4 & \triangle \\
4 & 4 & \triangle & 2 & \triangle & \triangle & \triangle \\
\hline
\triangle & \triangle & \triangle & \triangle & \triangle & \triangle & \triangle \\
\hline
\end{array}.$$

Take $\pi = (2,4)$ (in cycle structure) for example. We construct h_π and f_π

$+$	0	1	2	3	4	△
0	⓪	1	2	3	4	△
1	1	①	2	△	△	△
2	2	△	2	△	④	△
3	3	1	△	③	4	△
4	4	△	②	△	△	△
△	△	△	△	△	△	△⃝

,

x	$\pi(x)$	$x + h_\pi(x) = f_\pi(x)$
0		$0 + 0 = 0$
1	1	$1 + 1 = 1$
2	4	$2 + 4 = 4$
3	3	$3 + 3 = 3$
4	2	$4 + 2 = 2$
△		$\triangle + \triangle = \triangle$

.

Given a transversal $h(x)$ of $R(A) = (G,+)$, it is easy to check that $h(0) = 0$ and $h(\triangle) = \triangle$. If π is a permutation of M such that $A_{i,\pi(i)} = 1$ $(\forall i \in M)$ then there exists a unique transversal h of G such that $h = h_\pi$. Conversely, if $h(x)$ is a transversal of G, then there exists a unique permutation π of M with $A_{i,\pi(i)} = 1$ $(\forall i \in M)$ such that $h = h_\pi$. Thus the permanent of A equals the number of transversals of $(G,+)$. Let S simply be the identity function. It is easy to verify that both R and S are polynomial time computable. We thus complete the Z-reduction (R,S) from C_P to C_T.

Furthermore, given a matrix A and $R(A) = (G,+)$, we have the following properties:

(1) For any complete mapping f of $R(A) = (G,+)$, we have $f(0) = 0$ and $f(\triangle) = \triangle$.
(2) Every complete mapping $f(x)$ of $R(A) = (G,+)$ is also its own transversal. That is, $f(x) = x + f(x)$. The same is true with transversals.

Therefore the number of transversals of $(G,+)$ is the same as the number of complete mappings of $(G,+)$. Using the same Z-reduction (R,S), we can also reduce C_P to C_C. □

Corollary 2.1. *The counting problems of transversals and complete mappings of a closed structure are both #P-complete.*

Theorem 3. *The counting problems of transversals and complete mappings of a closed structure with a left-identity and the left-cancellation law are both #P-complete.*

Proof. For convenience, we define C_P, C_T, C_T1, C_C, and C_C1.

(1) Let C_P be the problem evaluating the *permanent* of an $n \times n$ matrix of 0's and 1's.
(2) Let C_T be the counting problem of *transversals* of a closed structure with left-cancellation law.

(3) Let C_{T1} be the counting problem of transversals of a closed structure with left-cancellation law and a left-identity.
(4) Let C_{C} be the counting problem of *complete mappings* of a closed structure with left-cancellation law.
(5) Let C_{C1} be the counting problem of complete mappings of a closed structure with left-cancellation law and a left-identity.

We will first construct a Z-reduction (R,S) and use it to both reduce C_{P} to C_{T} and from C_{P} to C_{C}. We will then construct a (R',S') to reduce C_{P} to both C_{T1} and C_{C1}.

Let $A_{i,j}$ be an $n \times n$ matrix of 0's and 1's. We assume that the number of 1's in each row or column of A is not n. (Otherwise, we can construct an $(n+1)\times(n+1)$ matrix $B_{i,j}$ where $B_{i,j}=A_{i,j}$, $B_{i,n+1}=B_{n+1,j}=0$, and $B_{n+1,n+1}=1$ for $1 \leqslant i,j \leqslant n$. Since the permanent of B equals the permanent of A, B will satisfy our assumption.) We take $G=\{1,2,3,\dots,2n\}$, and construct $R(A)=(G,\oplus)$ defined below. Let $a,b \in M=\{1,2,3,\dots,n\}$ and $+$ be the addition of natural number. We define

(1) $a \oplus b = b,\ a \oplus (n+b) = (n+b)$ if $A_{a,b}=1$,
(2) $a \oplus b = (n+b),\ a \oplus (n+b) = b$ if $A_{a,b}=0$,
(3) $(n+a) \oplus b = (a+1)(\operatorname{mod} n)$ (here we take $n \bmod n$ to be n), and
(4) $(n+a) \oplus (n+b) = (n+b)$ for $a,b \in \{1,2,3,\dots,n\}$.

For example, given

$$A=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

we construct $G=\{1,2,3,4,5,6,7,8\}$, and

$$(G,\oplus)=\begin{array}{|c|cccc|cccc|}
\hline
\oplus & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
1 & 1 & 2 & 7 & 8 & 5 & 6 & 3 & 4 \\
2 & 5 & 2 & 7 & 4 & 1 & 6 & 3 & 8 \\
3 & 1 & 6 & 3 & 4 & 5 & 2 & 7 & 8 \\
4 & 5 & 2 & 7 & 8 & 1 & 6 & 3 & 4 \\
\hline
5 & 2 & 3 & 4 & 1 & 5 & 6 & 7 & 8 \\
6 & 2 & 3 & 4 & 1 & 5 & 6 & 7 & 8 \\
7 & 2 & 3 & 4 & 1 & 5 & 6 & 7 & 8 \\
8 & 2 & 3 & 4 & 1 & 5 & 6 & 7 & 8 \\
\hline
\end{array}.$$

Then $(G, \oplus)$ satisfies the left-cancellation law. For convenience, we split the additive table into four parts UL, UR, DL, DR, where

$$UL = M \times M,$$

$$UR = M \times (n + M),$$

$$DL = (n + M) \times M \quad \text{and}$$

$$DR = (n + M) \times (n + M).$$

Let $L = UL \cup DL$, $R = UR \cup DR$, $U = UL \cup UR$ and $D = DL \cup DR$.

$\oplus$	M	$n+M$
M	UL	UR
$n+M$	DL	DR

$\oplus$	M	$n+M$
M	U	
$n+M$	D	

$\oplus$	M	$n+M$
M	L	R
$n+M$		

Because $(G, \oplus)$ has left-cancellation law and $x \oplus h(x) = f(x)$, the number of transversals is the same as the number of complete mappings. Considering a complete mapping $f(x)$ such that $x \oplus h(x) = f(x)$, we define place$(f(x)) = (x, h(x))$. Finding a complete mapping $f(x)$ is finding the values of place(1), place(2), place(3), …, place($2n$) such that the function $h(x)$ (defined as $h(x) = y$ if place$(z) = (x, y)$ for some z) is a well-defined permutation. For example,

$\oplus$	1	2	3	4	5	6	7	8	$x \oplus h(x) = f(x)$	place$(f(x)) = (x, h(x))$
1	①	2	7	8	5	6	3	4	$1 \oplus 1 = 1$	place$(1) = (1, 1)$
2	5	2	7	④	1	6	3	8	$2 \oplus 4 = 4$	place$(4) = (2, 4)$
3	1	6	③	4	5	2	7	8	$3 \oplus 3 = 3$	place$(3) = (3, 3)$
4	5	②	7	8	1	6	3	4	$4 \oplus 2 = 2$	place$(2) = (4, 2)$
5	2	3	4	1	⑤	6	7	8	$5 \oplus 5 = 5$	place$(5) = (5, 5)$
6	2	3	4	1	5	⑥	7	8	$6 \oplus 6 = 6$	place$(6) = (6, 6)$
7	2	3	4	1	5	6	⑦	8	$7 \oplus 7 = 7$	place$(7) = (7, 7)$
8	2	3	4	1	5	6	7	⑧	$8 \oplus 8 = 8$	place$(8) = (8, 8)$

.

We claim that

$$\forall m \in M \;\; \text{place}(m) \in L \text{ and}$$

$$\forall m \in M \;\; \text{place}(n + m) \in R.$$

The reason is as follows. Let $m \in M$.

(1) $\text{place}(m) \in R \Rightarrow \text{place}(m) \in UR$.
(2) $\text{place}(n+m) \in L \Rightarrow \text{place}(n+m) \in UL$.
(3) $\text{place}(m) \in UL \Rightarrow \text{place}((m+1) \bmod n) \in U$.
(4) $\text{place}(m) \in UR \Rightarrow \text{place}(n+m) \in UL \Rightarrow \text{place}((m+1) \bmod n) \in U$.
(5) $\text{place}(m) \in U \Rightarrow \text{place}((m+1) \bmod n) \in U$ (By 3 and 4.)

$\text{place}(m) \in R$ $\Rightarrow_1$ $\text{place}(m) \in UR$ $\Rightarrow_2$ $\text{place}(m+n) \in UL$ $\Rightarrow_3$ $\text{place}((m+1) \bmod n) \in U$ $\Rightarrow_4$ $\text{place}((m+2) \bmod n) \in U$ $\Rightarrow_5$ $\text{place}((m+3) \bmod n) \in U$ $\Rightarrow_5$ $\dots$ $\Rightarrow_5$ $\text{place}((m+n) \bmod n)$ $=\text{place}(m) \in U$	$\text{place}(m+n) \in L$ $\Rightarrow_2$ $\text{place}(m+n) \in UL$ $\Rightarrow_4$ $\text{place}((m+1) \bmod n) \in U$ $\Rightarrow_5$ $\text{place}((m+2) \bmod n) \in U$ $\Rightarrow_5$ $\text{place}((m+3) \bmod n) \in U$ $\Rightarrow_5$ $\dots$ $\Rightarrow_5$ $\text{place}((m+n) \bmod n)$ $=\text{place}(m) \in U$

Now if $\text{place}(m) \in R$ for some m, then by the above arguments, all the $n+1$ elements in the set $\{\text{place}(m), \text{place}((m+1) \bmod n), \dots, \text{place}((m+n-1) \bmod n), \text{place}(m+n)\}$ will be in U. Since h is a permutation, $|h(M)| = n$ and there should be only n elements $x \in G$ such that $\text{place}(x) \in U$. Thus $\text{place}(m)$ cannot be in R. By the same reasoning, $\text{place}(m+n)$ is not in L. Therefore $\text{place}(m) \in L$ and $\text{place}(m+n) \in R$.

As a consequence, we have the following results:

(1) $\text{place}(m) \in UL \Rightarrow \text{place}((m+1) \bmod n) \in UL$.
(2) $\text{place}(m) \in DL \Rightarrow \text{place}((m+1) \bmod n) \in DL$.

This implies that either $\text{place}(m) \in UL$ for all $m \in M$ or $\text{place}(m) \in DL$ for all $m \in M$. The number of transversals of G is, therefore, $\text{permanent}(A) \times n! + n! \times \text{permanent}(A) = 2 \times n! \times \text{permanent}(A)$. Let $S(y) = y/(2 \times n!)$. It is easy to verify that both R and S are polynomial time computable. We complete the Z-reduction (R, S) from C_P to C_T. Since the number of transversals of G is the same as the number of complete mappings of complete mappings of G, (R, S) is also a Z-reduction from C_P to C_C.

We now construct $R'(A) = (G', \otimes)$ as follows. Let $G' = \{0\} \cup G$, $m \in M$, and $a \in G$. Define

(1) $a \otimes m = a \oplus ((m-1) \bmod n)$.
(2) $a \otimes (n+m) = a \oplus (n+m)$.
(3) $0 \otimes x = x$ and $x \otimes 0 = 0$ for all $x \in G'$.

For example, let

$$(G',\otimes)=\begin{array}{|c|cccc|c|cccc|}
\hline
\otimes & 2 & 3 & 4 & 1 & 0 & 5 & 6 & 7 & 8\\
\hline
1 & 1 & 2 & 7 & 8 & 0 & 5 & 6 & 3 & 4\\
2 & 5 & 2 & 7 & 4 & 0 & 1 & 6 & 3 & 8\\
3 & 1 & 6 & 3 & 4 & 0 & 5 & 2 & 7 & 8\\
4 & 5 & 2 & 7 & 8 & 0 & 1 & 6 & 3 & 4\\
\hline
0 & 2 & 3 & 4 & 1 & 0 & 5 & 6 & 7 & 8\\
\hline
5 & 2 & 3 & 4 & 1 & 0 & 5 & 6 & 7 & 8\\
6 & 2 & 3 & 4 & 1 & 0 & 5 & 6 & 7 & 8\\
7 & 2 & 3 & 4 & 1 & 0 & 5 & 6 & 7 & 8\\
8 & 2 & 3 & 4 & 1 & 0 & 5 & 6 & 7 & 8\\
\hline
\end{array}.$$

Then $(G',\otimes)$ is a closed structure with left-identity and left-cancellation law. By a deduction similar to the previous case, we can show that the number of transversals of G' is $2\times(n+1)!\times\text{permanent}(A)$. Let $S'(y)=y/(2\times(n+1)!)$. It is easy to verify that both R' and S' are polynomial time computable. Therefore (R',S') is a Z-reduction from C_{P} to C_{T1}. Note that (R',S') is also a Z-reduction from C_{P} to C_{C1}, we thus complete the proof. □

We now turn our attention to some problems that are beyond the #P class. We first present a lemma that establishes a relationship (an upper-bound) between the number of solutions for a counting problem and the size of the input.

Lemma 4. *Let Q be a $p(|x|)$-polynomially balanced, polynomial-time decidable binary relation. Given x, the number $C_{\mathrm{Q}}(x)$ of y's such that $(x,y)\in Q$ is less than or equals to $2^{p(|x|)}$. Furthermore, the length of $C_{\mathrm{Q}}(x)$ is $\mathrm{O}(p(|x|))$.*

Proof. We assume that x, y, and the number $C_{\mathrm{Q}}(x)$ are represented as integers in binary. Since Q is $p(|x|)$-polynomially balanced, for any y, $(x,y)\in Q$ we have $|y|\leqslant p(|x|)$. Therefore $C_{\mathrm{Q}}(x)$ is less then or equals to $2^{p(|x|)}$, and the output length of $C_{\mathrm{Q}}(x)$ is $\mathrm{O}(p(|x|))$. □

Theorem 5. *The counting problem of (strong) complete mappings for cyclic groups Z_n is beyond the #P-class.*

Proof. Recall that in Definition 4, we let $\#(\mathrm{CM}(G))$ denote the number of standard complete mappings of a group G, and $\#(\mathrm{SCM}(G))$ denote the number of standard strong complete mappings of a group G. Let p be a prime, and n be p^m for some nature number m. Hsiang et al. [16] showed that $\#(\mathrm{CM}(Z_n))\geqslant\#(\mathrm{SCM}(Z_n))\geqslant p^{n/p}/n$. If we take n as the input (with length $t=\log(n)$), then the output length is $\Omega(2^t\log(p)/p-t)$.

By Lemma 4, the counting problems of (strong) complete mappings for cyclic groups Z_n are not #P problems. □

We should remark that at the first glance Theorem 5 seems to contradict Theorem 3. This is not the case because in Theorem 3 the entire structure needs to be considered as the input (which may be of size n^2) while in Theorem 5, the input size is only $\log(n)$ (the number of bits needed to encode n). Theorem 5 gives rise to another set of results concerning the n-queen problems.

Definition 7 (n-queen problem). Let $Z_n = 0, 1, 2, \ldots, n-1$. A solution of the n-queen problem is a permutation $f(x)$ from Z_n to Z_n such that $\forall_{i \neq j \in Z_n} i + f(i) \neq j + f(j)$ and $\forall_{i \neq j \in Z_n} - i + f(i) \neq -j + f(j)$ under the natural number addition. We use $Q(n)$ to denote the number of solutions of the n-queen problem.

Considering a modular chessboard, i.e. chessboards where the diagonals continue on the other side, there is another variant of the n-queen problem called the *modular* n*-queen problem*. The concept of modular chessboards were introduced by Pólya [13]. There are different names for the modular n-queen problem such as the toroidal n-queen problem [14], which we adopt here, or the n-super-queen problem [8].

Definition 8 (toroidal n-queen problem). A solution of the toroidal n-queen problem is a permutation $f(x)$ from Z_n to Z_n such that (under the cyclic group $(Z_n, +)$), $x + f(x)$ and $-x + f(x)$ are both permutations. We use $TQ(n)$ to denote the number of solutions of the toroidal n-queen problem.

Lemma 6. *Given a cyclic group* Z_n,

(1) *a solution* $f(x)$ *to the toroidal n-queen problem is a* standard *strong complete mapping if and only if* $f(0) = 0$,
(2) $TQ(n) = n \times \#(\mathrm{SCM}(Z_n))$,
(3) $\#(\mathrm{SCM}(Z_n)) \leqslant TQ(n) \leqslant Q(n)$.

By the Theorem 5 and the Lemma 6, we have the following corollary.

Corollary 6.1. *The counting problems of the n-queen and the toroidal n-queen problem are both beyond the #P-class.*

Proof. Because (the number of solutions of n-queen) $\geqslant$ (the number of solutions of the toroidal n-queen problem) $\geqslant$ (the number of standard strong complete mappings of cyclic group Z_n), and the input lengthes of three problems are all $\log(n)$ size, the counting problems of the (toroidal) n-queen problem are both beyond the #P-class. □

Theorem 7. *The counting problem of complete mappings for finite abelian groups G is beyond the #P-class.*

Proof. By the fundamental theorem of finite abelian groups, every finite abelian group G is the direct product of cyclic groups of prime power order. We can take G as

Table 1

Structure	CS			QG	LP	G	AG	CG
Closed	√	√	√	√	√	√	√	√
Left-cancellation			√	√	√	√	√	√
Cancellation				√	√	√	√	√
Left-identity		√	√		√	√	√	√
Identity		√			√	√	√	√
Association						√	√	√
Commutation							√	√
Cyclic								√
#P-complete	Yes	Yes	Yes	?	?	?	No	No
#P-complete? (conjecture)				Yes	Yes	No		

Note: CS: closed structure, QG: quasigroup, LP: loop, G: group, AG: abelian group, and CG: cyclic groups.

$G = Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times Z_{p_3^{\alpha_3}} \times \ldots \times Z_{p_k^{\alpha_k}}$ where $p_1 \leqslant p_2 \leqslant p_3 \leqslant \ldots \leqslant p_k$ are primes and if $i \leqslant j, p_i = p_j$ then $\alpha_i \leqslant \alpha_j$. So we can use $(p_1, \alpha_1, p_2, \alpha_2, p_3, \alpha_3, \ldots, p_k, \alpha_k)$ to encode the abelian group G. Let $n = |G|$. We have $\alpha_i \leqslant \log_2 n$, $k \leqslant \log_2 n$, and $p \leqslant n$. So the space required to encode G is less than $(\log_2 n + \log_2(\log_2 n)) \times k \leqslant 2 \times (\log_2 n)^2 = \mathrm{O}((\log_2 n)^2)$. So we can encode any finite abelian group G using $\mathrm{O}((\log_2 |G|)^2)$ space. Let $t = \log(n)^2$. Since cyclic groups are abelian, by the proof of Theorem 5 the output length is $\Omega(2^{\sqrt{t}} \log(p)/p - \sqrt{t})$. By Lemma 4, the counting problem of complete mappings for abelian groups is not in the #P-class. □

4. Discussion

We summarize the above theorems in Table 1. We conjecture that the counting problem of complete mappings for a group is beyond the #P-class. This is because the growth rate of the number of groups with respect to the size of groups is very small [1] (A000001) (open the url in [1], and see the sequence numbered A000001). And we think there may be an encoding method to describe a group with a very short length. However we guess that for a loop [1] (A057997) or a quasigroup [1] (A002860) the counting problems of complete mappings are both #P-complete.

References

[1] http://www.research.att.com/∼njas/sequences/.

[2] B.A. Anderson, Sequencings and houses, Congr. Numer. 43 (1984) 23–43.

[3] R.C. Bose, I.M. Chakravarti, D.E. Knuth, On methods of constructing sets of mutually orthogonal Latin squares using a computer I, Technometrics 2 (1960) 507–516.

[4] J.D. Horton, Orthogonal starters in finite Abelian groups, Discrete Math. 79 (1990) 265–278.

[5] D.F. Hsu, Cyclic neofields and combinatorial designs, Lecture Notes in Mathematics Vol. 824, Springer, Berlin, 1980.

[6] D.F. Hsu, Orthomorphisms and near orthomorphisms, in: Y. Alavi (Ed.), Graph Theory, Combinatorics, and Applications, Wiley, New York, 1991, pp. 667–679.

[7] D.F. Hsu, A.D. Keedwell, Generalized complete mappings, neofields, sequenceable groups and block designs II, Pacific J. Math. 117 (1985) 291–312.

[8] F.K. Hwang, K.-W. Lih, Latin squares and superqueens, Combin. Theory Ser. A 34 (1983) 110–114.

[9] D.M. Johnson, A.L. Dulmage, N.S. Mendelsohn, Orthomorphisms of groups and orthogonal Latin squares I, Canad. J. Math. 13 (1961) 356–372.

[10] H.B. Mann, The construction of orthogonal Latin squares, Ann. Math. Statist. 13 (1942) 418–423.

[11] L.J. Paige, Complete mappings of finite groups, Pacific J. Math. 1 (1951) 111–116.

[12] C.H. Papadimitriou, Computational Complexity, Addison-Wesley, Reading, MA, 1994.

[13] G. Pólya, Über die ‘doppelt-periodischen’ Lösungen des n-Damen-Problems, Mathematische Unterhaltungen und Spiele II, W. Ahrens, 1918, pp. 364–374.

[14] I. Rivin, I. Vardi, P. Zimmermann, The n-queens problem, Amer. Math. Monthly 101 (1994) 629–639.

[15] Y.-P. Shieh, Partition strategies for #P-complete problem with applications to enumerative combinatorics, Ph.D. Thesis, National Taiwan University, 2001.

[16] Y.-P. Shieh, J. Hsiang, D.F. Hsu, On the enumeration of abelian k-complete mappings, Congressus Numerantium 144 (2000) 67–88.

[17] L.G. Valiant, The complexity of computing the permanent, Theoret. Comput. Sci. 8 (1979) 189–201.

[18] V. Zankó, #p-completeness via many-one reductions, Internat. J. Foundations Comput. Sci. 2 (1991) 77–82.