Discrete Applied Mathematics 162 (2014) 149–158

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Hardness of learning loops, monoids, and semirings

Ching-Lueh Chang *

Department of Computer Science and Engineering, Yuan Ze University, Taoyuan, Taiwan

ARTICLE INFO

Article history:
Received 13 December 2011
Received in revised form 5 August 2013
Accepted 14 August 2013
Available online 8 September 2013

Keywords:
Query complexity
Loop
Monoid
Semiring

ABSTRACT

We show that each randomized $o(|G|^2)$-query algorithm can recover only an expected $o(1)$ fraction of the Cayley table of some finite Abelian loop $(G, \cdot)$, where both multiplication and inversion queries are allowed. Furthermore, each randomized $o(|R|^2)$-query algorithm can recover only an expected $o(1)$ fraction of any of the Cayley tables of some finite commutative semiring $(R, +, \cdot)$, with $(R, +)$ being a commutative aperiodic monoid, where each query may ask for $x + y$ or $x \cdot y$ for any $x, y \in R$.

1. Introduction

Zumbrägel et al. [15] consider the problem of learning the Cayley table (i.e., multiplication table) of a groupoid $(G, \cdot)$ by making the minimum number of queries, each for a product $a \cdot b$, with $a, b \in G$. They give a deterministic $|G|$-query algorithm for the exact recovery of the Cayley table of any finite Abelian group $(G, \cdot)$. The bound of $|G|$ is optimal up to an additive factor of $|G|/\ln|G| - 1/2 + \lg|G|$ [15, Corollary 9]. Note that $|G|^2$ rather than $O(|G|)$ queries are needed to exhaust the Cayley table. When $(G, \cdot)$ is taken uniformly at random from a set $\mathcal{X}$ of groupoids with groundset G, the expected number of queries for any algorithm to exactly recover the Cayley table of $(G, \cdot)$ is at least $\log_{|G|}|\mathcal{X}|$ [15, Lemma 6]. Zumbrägel et al. [15, Proposition 16] also give a deterministic $(|R| + (\lg|R|)^2)$-query algorithm for recovering the two Cayley tables of any finite ring $(R, +, \cdot)$, where each query may ask for $x + y$ or $x \cdot y$ on any choice of $x, y \in R$.

Given the results of Zumbrägel et al. [15], we are motivated by whether all the axioms of finite Abelian groups are necessary for recovering the Cayley table with only $o(|G|^2)$ queries. First of all, commutativity is not necessary, because existing results can be easily modified to give a deterministic $O(|G|\log|G|)$-query algorithm for the exact recovery of any finite group $(G, \cdot)$. See, e.g., [9]. The present paper shows that all the other axioms of finite Abelian groups are necessary for recovering the Cayley table with $o(|G|^2)$ queries even if only a small constant (in expectation) fraction of the entries need to be recovered. In particular, we show that any randomized $o(|G|^2)$-query algorithm can recover only an expected $o(1)$ fraction of the Cayley table of some finite Abelian loop even if the algorithm is furthermore allowed to query for the inverse of any element (note that each Abelian loop does have a unique inverse for any of its elements). Our proof composes Abelian groups in a manner belonging to a general class of crossed products [14, Eq. (2)]. Furthermore, we show that any randomized $o(|R|^2)$-query algorithm can recover only an expected $o(1)$ fraction of any of the Cayley tables of some finite commutative semiring $(R, +, \cdot)$, with $(R, +)$ being a commutative aperiodic monoid. As a corollary, any randomized $o(|G|^2)$-query algorithm can recover only an expected $o(1)$ fraction of the Cayley table of some finite commutative aperiodic monoid. It is well known that Abelian loops and commutative monoids satisfy all the axioms of groups except for associativity and existence of inverses, respectively; so all the axioms of groups are essential for $o(|G|^2)$-query recovery of any constant fraction of a Cayley table.

* Tel.: +886 3 4638800; fax: +886 3 4638850.
E-mail address: clchang@saturn.yzu.edu.tw.

0166-218X/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dam.2013.08.012

There are related works concerning quasigroups. A Latin square of order n refers to the Cayley table of a quasigroup of size n. A partially filled n-by-n table that can be uniquely completed to a Latin square is called a critical set if deleting any of its entries prevents unique completion to a Latin square [4,13]. Ghandehari et al. [10, Theorem 4] prove the existence of a Latin square of order n whose smallest critical sets have size at least $n^2 - (e + o(1))n^{5/3}$. Therefore, recovering exactly the Cayley table of a quasigroup of size n requires $n^2 - (e + o(1))n^{5/3}$ queries in the worst case. Furthermore, the minimum size of critical sets in any Latin square of order n is at least $n\lfloor(\log^{1/3} n)/2\rfloor$ [3]. There exists a Latin square of order n having a critical set of size s if $\lfloor n^2/4\rfloor \le s \le (n^2 - n)/2$ [5,1] or, for $n = 2^m$, $4^{m-1} \le s \le 4^m - 3^m$ [6]. No critical sets in any Latin square of order $n \ge 7$ can have size greater than $n^2 - \lfloor(7n - \sqrt{n} - 20)/2\rfloor$ [2,11].

The paper is organized as follows. Section 2 defines the basic terms. Section 3 shows that any randomized $o(|G|^2)$-query algorithm can recover only an expected $o(1)$ fraction of the Cayley table of some finite Abelian loop. Section 4 proves that any randomized $o(|R|^2)$-query algorithm can recover only an expected $o(1)$ fraction of the Cayley tables of some commutative semiring whose addition induces a commutative aperiodic monoid. The Appendix proves that any finite group can be recovered with $O(|G| \log |G|)$ multiplication queries, a result that is not hard to see from the existing literature.

2. Preliminaries

We begin with some basic definitions in algebra [7].

Definition 1. A *groupoid* $(G, \cdot)$ is a nonempty set G endowed with a binary operation $\cdot : G \times G \to G$. An element $e \in G$ is called an *identity* if $a \cdot e = e \cdot a = a$ for all $a \in G$.

As a well-known fact, an identity of a groupoid is necessarily unique if it exists.

Definition 2. For a groupoid $(G, \cdot)$ with identity e and $a, b \in G$, we say that a is an *inverse* of b if $a \cdot b = b \cdot a = e$. An inverse of b, if it is unique, is denoted b^{-1}.

Definition 3. A groupoid $(G, \cdot)$ is

- *Abelian* (or *commutative*) if $a \cdot b = b \cdot a$ for all $a, b \in G$,
- *associative* if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$,
- a *monoid* if it is associative and has an identity,
- a *quasigroup* if, for all $a, b \in G$, there exist unique elements $x, y \in G$ satisfying $a \cdot x = b$ and $y \cdot a = b$,
- a *loop* if it is a quasigroup with an identity, and
- a *group* if it is associative, has an identity, and each element of G has a unique inverse.

Clearly, each element of an Abelian loop has a unique inverse.

Definition 4. A monoid $(G, \cdot)$ is *aperiodic* if, for each $a \in G$, there exists a positive integer n with $a^n = a^{n+1}$.

Definition 5. A *ringoid* $(R, +, \cdot)$ is a nonempty set R endowed with two binary operations $+, \cdot : R \times R \to R$ such that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$.

Definition 6. A ringoid $(R, +, \cdot)$ is a *commutative semiring* if $(R, +)$ and $(R, \cdot)$ are commutative monoids such that, denoting the identity of $(R, +)$ by 0, $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.

Let $\mathbb{Z}^+ \equiv \{1, 2, \ldots\}$ be the set of positive integers. For $n \in \mathbb{Z}^+$, define $[n] \equiv \{1, 2, \ldots, n\}$. An algorithm with oracle access to a groupoid $(G, \cdot)$ is given the set G and may query for $a \cdot b$ for any $a, b \in G$; such a query is called a multiplication query. Depending on the contexts, it may also make an inversion query, which returns a^{-1} given any $a \in G$. An algorithm with oracle access to a ringoid $(R, +, \cdot)$ is given oracle access to $(R, +)$ and $(R, \cdot)$. We tacitly assume a reasonable encoding of the elements of the groundsets G and R, e.g., $G = [|G|]$ and $R = [|R|]$, with integers encoded in binary.

The following theorem is not hard to see from the existing literature (see, e.g., [9]). For completeness, we prove it in the Appendix.

Theorem 7. *The Cayley table of any finite group $(G, \cdot)$ can be computed with $O(|G| \log |G|)$ multiplication queries.*

Below is a well-known fact regarding crossed products of loops [14, Eq. (2)].

Fact 8 *([14]). Let $(H, \cdot_H)$ and $(K, \cdot_K)$ be loops with identities e_H and e_K, respectively, and let A be a function from $H \times H \times K \times K$ to K. Assume the following properties for all $h, h' \in H$ and $k, k' \in K$.*

(i) *There exist unique $x, y \in K$ satisfying $A(h, h', k, x) = k'$ and $A(h', h, y, k) = k'$.*
(ii) *$A(h, e_H, k, e_K) = A(e_H, h, e_K, k) = k$.*

For $(h, k), (h', k') \in H \times K$, denote $(h, k) \lhd (h', k') = (h \cdot_H h', A(h, h', k, k'))$. Then $(H \times K, \lhd)$ is a loop with identity (e_H, e_K).