Ring Morphism Problems and Circuit Minimization

Zelin Lv *

May 10, 2019

Abstract

Many ring morphism problems held their importance in math, especially in number theory and algebra. And they are considered as candidates of NP-intermediate problems like MCSP, the Minimum Circuit Size Problem. We show that deciding if two given rings are isomorphic is in $\mathsf{RP}^{\mathsf{MCSP}}$. using the techniques of Allender and Das [AD17]. Moreover, we also show that finding an automorphism and counting automorphisms of one ring are in $\mathsf{ZPP}^{\mathsf{MCSP}}$.

1 Introduction

A ring is a set with addition and multiplication operations defined. It is considered as one fundamental structure in Math, especially in algebra and number theory. The importance of researching ring isomorphism includes that many problems can be reduced to it in polynomial time, such as GI [KS06] and the automorphisms group of a ring encodes profitable structure information of a ring. And from the computational complexity view, deciding if two given rings are isomorphic (RI) and finding an automorphism (FRA) of one ring are considered as candidates of NP-intermediate problems, which are, assuming P$\neq$ NP, not in P nor in NP-complete [Lad75].

Besides RI, FRA, and #RA, other prominent candidates for NP-intermediate include Graph Isomorphism (GI) and the Minimum Circuit Size Problem (MCSP). MCSP is the problem that given a number i and a Boolean function f on n variables, represented by its truth table of size 2^n, determine if f has a circuit of size i. Even though the relationship between GI and ring morphism problems has been widely studied and MCSP has attracted special interests in math community [Tra85], no connection between ring morphism problems and MCSP has been estalished. Therefore, in this paper, we present the connection of relative complexity of these problems.

Many hardness results of MCSP are known. Allender and Das showed that entire Statistical Zero Knowledge (SZK) are included in $\mathsf{BPP}^{\mathsf{MCSP}}$ and GI are contained in $\mathsf{RP}^{\mathsf{MCSP}}$ [AD17]. Allender, Buhrman, Koucky, Van Melkebeek, and Ronneburger proved that Integer Factoring is included in $\mathsf{ZPP}^{\mathsf{MCSP}}$ and Discrete Logarithm Problem is in $\mathsf{BPP}^{\mathsf{MCSP}}$[ABK$^+$06], where Rudow later improved result and showed that

*University of Wisconsin–Madison, Madison, WI, USA, zlv7@wisc.edu

Discrete Logarithm Problem is in $\mathsf{ZPP}^{\mathsf{MCSP}}$ [Rud17]. Moreover, for the Minimum KT Problem, where MKTP is a a time-bounded Kolmogorov complexity problem that is similar to MCSP , it has been shown that Graph Isomorphism (GA) and it's related problems are in $\mathsf{ZPP}^{\mathsf{MKTP}}$ [AGvM+18] and the Hidden Subgroup Problem is in $\mathsf{ZPP}^{\mathsf{MKTP}}$ [SdSV18].

Using techiques similar to those have been used in proving the relative complexity of GI and $\mathsf{RP}^{\mathsf{MCSP}}$ [AD17], we present the result relating RI and MCSP. And by relating FRA and $\#\mathsf{RA}$ with Integer Factorization, we can relate them with MCSP.

2 Preliminaries

In this section, we first give basis of rings. Note that a ring $(R, +, *)$ is a set with two operations that generalize the operations of addition and multiplication defined. For each ring the additive group is the set just with addition operation, called $(R, +)$. And $(R, *)$ is the multiplicative group where R^* is the the set of elements in R having multiplicative inverses. In this section we first give formal definition of basic representation of rings and presentation of maps on rings.

Definition 1. [KS06] **Basis representation of rings:** A finite ring R is given by first describing its additive group in terms of n additive generators and then specifying multiplication by giving for each pair of generators, their product as an element of the additive group. More concretely, R is presented as:

$$(R, +, .) :=< (d_1, d_2, ..., d_n), ((a_{i,j,k}))_{1 \leq i,j,k \leq n} >$$

where, for all $1 \leq i, j, k \leq n, 0 \leq a_{i,j,k} < d_k$ and $a_{i,j,k} \in \mathbb{Z}$

One ring R generated by elements $b_1, b_2, ..., b_n$, where each b_i has additive order d_i has additive group $R(, +) = (\mathbb{Z}/d_1\mathbb{Z})b_1 \oplus (\mathbb{Z}/d_2\mathbb{Z})b_2 ... \oplus (\mathbb{Z}/d_n\mathbb{Z})b_n$. And for multiplicative structure in R, it is defined as the product of each pair of generators as an integer linear combination of the generators: for $1 \leq i, j \leq n, b_i b_j = \sum_{k=1}^{n} a_{i,j,k} b_k$.

Definition 2. [KS06] **Representation of maps on rings**: Suppose R_1 is a ring given in terms of its additive generators $b_1, ..., b_n$ and ring R_2 given in terms of $c_1, ..., c_n$. In this paper maps on rings would invariably be homomorphisms on the additive group. Then to specify any map $\phi : R1 \to R2$, it is enough to give the images $\phi(b_1), ..., \phi(b_n)$.

Definition 3. [KS06] **Indecomposable or local ring:** A ring R is said to be indecomposable or local if there do not exist rings R_1, R_2 such that $R \cong R_1 \times R_2$, where $\times$ denotes the natural composition of two rings with component-wise addition and multiplication.

With the formal definition of rings, we can define ring isomorphism and related problems which will be discussed in this paper.

Definition 4. Ring Isomorphism Problem: To decide if two given rings are isomorphic.

$\mathsf{RI} := \{(R_1, R_2) |$ *rings* R_1, R_2 *are given in the basis representations and* $R_1 \cong R_2\}$

Definition 5. Ring Automorphism Problem: To decide if one given ring has a nontrivial ring automorphism.

$$\mathsf{RA} := \{R|\ R \textit{ is a ring in basis } form \textit{ s.t. } \#Aut(R) > 1\}$$

Definition 6. Find Ring Automorphism Problem: To find a nontrivial automorphism of a ring R in basis form.

More information about rings can be found in algebra texts, such as [McD74]. In the following, we give the important preliminaries about MCSP.

Definition 7. The Minimum Circuit Size Problem: Given a number i and a Boolean function f on n variables, represented by its truth table of size 2^n, determine if f has a circuit of size i.

With an oracle of MCSP, we have the sufficient tool to distinguish the uniform distribution and the distribution generated by pseudorandomness, and it's sufficient to invert on average any function that can bu computed uniformly in polynomial time of length of its input [ABK+06]. And we can have the following theorem:

Theorem 1. (from [ABK+06, Theorem 45]) *Let L be a language of polynomial density such that, for some $\epsilon > 0$, for every $x \in L$, $KT(x) \geq |x|^\epsilon$. Let $f(y, x)$ be computable uniformly in time polynomial in $|x|$. There exists a polynomial-time probabilistic oracle Turing machine N and polynomial q such that for any n and y*

$$Pr_{|x|=n,s}[f(y, N^L(y, f(y, x), s)) = f(y, x)] \geq 1/q(n)$$

where x is chosen uniformly at random and s denotes the internal coin flips of N.

3 Ring Automorphism and Circuit Size

In this section, we present the relationship between Ring Automorphism (RA) and circuit minization problem. We know that checking if a ring has nontrivial automorphism can be done in deterministic polynomial time [KS06], but finding such a nontrivial automorphism of rings remains its status that is not in P and not NP-complete. With the existing theorems that establish the relationship of counting version of RA with Integer Factorization IF, we can easily show connection between finding versions of RA and MCSP.

Theorem 2. (follows from [ABK+06, Theorem 47]) $\mathsf{IF} \in \mathsf{ZPP}^{\mathsf{MCSP}}$

Theorem 3. (follows from [KS06, Theorem 8.1]) $\mathsf{IF} \equiv_T^{\mathsf{ZPP}} \mathsf{FRA}$

With these two theorems, we can establish the complexity relative relation between circuit size problem and finding such a nontrivial automorphism of rings.

Theorem 4. $\mathsf{FRA} \in \mathsf{ZPP}^{\mathsf{MCSP}}$

Proof. Given one instance of FRA, we first reduce it to one instance of IF with randomized polynomial time reduction by Theorem 3. And then by Theorem 2, we can find the integer factorization results with an oracle of MCSP. Therefore, we have $\mathsf{FRA} \in \mathsf{ZPP}^{\mathsf{MCSP}}$. □

4 Ring Isomorphism and Circuit Size

In this section, we present the complexity relative relation between RI and MCSP. Our proof follows the techniques in proving [AD17, Theorem 2] where they randomly generate one permutation τ and permuting the two given graphs. Comparatively, we randomly generate one automorphism of the additive group and generating two elements based on the given rings and the automorphism.

Theorem 5. $\mathsf{RI} \in \mathsf{RP}^{\mathsf{MCSP}}$

Proof. We are given two rings R_1 and R_2 as input and we want to determine if there are isomorphic.

First we check if $(R_1, +) \cong (R_2, +)$ which can be decided in polynomial time as given in [KS06, Remark 2.12]. If $(R_1, +) \ncong (R_2, +)$, then we have that $R_1 \ncong R_1$. Therefore, assuming that $(R_1, +) \cong (R_2, +)$, we find the following form of the additive groups of R_1 and R_2:

$$(R_1, +) = \oplus_{i=1}^{n} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})b_i$$

$$(R_2, +) = \oplus_{i=1}^{n} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})c_i$$

where p_i are primes and $\alpha_i \in \mathbb{Z}^{\geq 1}$. Finding such form of additive groups is computationally equivalent to IF, and with oracle of MCSP and by Theorem 2, this can be done in $\mathsf{ZPP}^{\mathsf{MCSP}}$.

Then we describe how to find an automorphism of the additive group of R_1 with the following Lemma 1. This construction is inspired by the proof of [KS06, Proposition 2.13].

Lemma 1. Structure Theorem for Abelian Groups *If R is a finite ring then its additive group $(R, +)$ can be uniquely (up to permutations) expressed as:*

$$(R_1, +) = \oplus_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}),$$

where p_i are primes (not necessarily distinct) and $\alpha_i \in \mathbb{Z}^{\geq 1}$.

Automorphism of the additive group $(R, +)$ is the invertible linear map on the additive generators of R, so it's same to find such an invertible linear map.

Given $(R,+)$ in the form $\oplus_{i=1}^{l} \oplus_j (\mathbb{Z}/p_i^{\alpha_{i,j}}\mathbb{Z})$, where p_i are primes and $\alpha_i \in \mathbb{Z}^{\geq 1}$. Then we can decompose R into subrings R_i where $R \cong R_1 \times ... \times R_l$, for $1 \leq i \leq l$ where

$$R_i := \{r \in R | r \ has \ power - of - p_i \ additive \ order\}$$

.

Therefore, it's enough to show how to construct an automorphism of $(R,+)$ where $(R,+)$ is in the following form:

$$(R,+) = (\mathbb{Z}/p^{\beta_1})e_{1,1} \oplus ... \oplus (\mathbb{Z}/p^{\beta_1})e_{1,n_1} \oplus ... \oplus (\mathbb{Z}/p^{\beta_m})e_{m,1} \oplus ... \oplus (\mathbb{Z}/p^{\beta_m})e_{m,n_m}$$

where $\sum_{i=1}^{m} n_i = n$ and $1 \leq \beta_1 \leq ... \leq \beta_m$.

Then, we can construct such an invertible $(mod\ p)$ matrix A that describes the map $\phi \in Aut(R,+)$ and preserves the additive orders of $e_{i,j}$ as following:

$$A = \begin{bmatrix} B_{1,1} & B_{1,2} & ... & B_{1,m} \\ B_{2,1} & B_{2,2} & ... & B_{2,m} \\ ... & & & \\ B_{m,1} & B_{m,2} & ... & B_{m,m} \end{bmatrix}_{n \times n}$$

The block matrices $B_{i,j}$ are integer matrices of size $n_i \times n_j$ and satisify the following properties:

- for $1 \leq j < i \leq m$: entries in $B_{i,j}$ are from $\{0, 1, ..., p^{\beta_j} - 1\}$,
- for $1 \leq i \leq m$: entries in $B_{i,i}$ are from $\{0, 1, ..., p^{\beta_j} - 1\}$ and $B_{i,i}$ is invertible $(mod\ p)$,
- for $1 \leq i < j \leq m$: entries in $B_{ij,}$ are from $\{0, 1, ..., p^{\beta_j} - 1\}$ and $B_{i,j} \equiv 0(mod\ p^{\beta_j - \beta_i})$.

Based on the properties of such a matrix A that describes the automorphism of the additive group of a ring, $\phi \in Aut(R,+)$, we can pick one $\phi \in Aut(R,+)$ by randomly select primes and elements in A's entries.

Given such automorphism of the additive group of a ring, we first check if this isomorphism preserves the multiplication of the original ring by check for all $i, j \in [n]$, if $A(b_i)A(b_j) = \sum_{k=1}^{n} a_{i,j,k}A(b_k)$. If the randomly generated map statisifies this condition, then it's an isomorphism from R_1 to R_2. We note the number of $(R,+)$ as $m(n)$, which is polynomial and can be found in polynomial time [KS06].

Consider the polynomial-time computable function $f(R, A)$ where the two inputs are a finite ring R and a randomly generate matrix $A \in Aut(R,+)$, which is a matrix of the map of ring isomorphism, it outputs $A(R)$. Note that f is uniformly computable in polynomial time.

Therefore, by Theorem 1, we have

$$Pr_{A \in Aut(R,+),s}[f(y, N^L(R, f(R, A), s)) = f(R, A)] \geq 1/q(n)$$

where A is chosen uniformly randomly and s is the randomness inside our polynomial-time probabilistic oracle Turing machine N. And q is a polynomial that hold the inequality above for any n and R.

Given two inputs (R_1, R_2), we can do following trails for $c \times q(n) \times m(n)$ times where c is a constant that is large enough:

1. pick the automorphism matrix A and probabilistic sequence s uniformly at random.
2. check if this automorphism matrix A describes an automorphism of the given ring, if not report 'not ring automorphism'; if yes, continue.
3. compute $f(R_1, A)$
4. Report 'isomorphic' if $f(N^{\mathsf{MCSP}}(R_2, f(R_1, A), s), R_2) = f(R_1, A)$

Given an automorphism map of additive group of this ring, it has a probability at least $\frac{1}{m(n)}$ is a map of this ring. And when an automorphism map of ring is given, this algorithm has at least $\frac{1}{q(n)}$ chance to report 'isomorphic'. So the excepted number of trails that report isomorphic' is $\#Aut(R) \times c$. By the Chernoff bounds, the probability of having one 'isomorphic' is larger than $\frac{1}{2}$. And if the two given rings are not isomorphic, this algorithm will never return 'isomorphic'. Therefore, we complete the proof that $\mathsf{RI} \in \mathsf{RP}^{\mathsf{MCSP}}$. □

Theorem 6. (follows from [KS06, Theorem 4.4]) $\mathsf{GI} \leq_m^{\mathsf{P}} \mathsf{RI}$.

Corollary 1. $\mathsf{GI} \in \mathsf{RP}^{\mathsf{MCSP}}$

5 Conclusion and Open Problems

In this paper, we showed the relative complexity of two ring morphism problems, FRAand RI, which are two candidates of NP-intermediate problems and MCSP, one of the most famous NP-intermediate problems. For FRA, our proof is involved with reduction from IF to FRA, which is given in [KS06]. And for RI, we first show how to uniformly generate one matrix that describes an automorphism of a ring from uniform distribution, and then by following the proof techniques used by Allender and Das [AD17], we proved that $\mathsf{RI} \in \mathsf{RP}^{\mathsf{MCSP}}$.

Naturally, the next step is two prove the a better reduction, say is RIin $\mathsf{ZPP}^{\mathsf{MCSP}}$? It has been already showed a powerful technique for obtaining zero- sided error reductions of GI [AGvM+18]. So it's possible to employ this technique to the relation of MCSPand RI.

Acknowledgments. This work is done by Zelin Lv under guidance of Professor van Melkebeek at the University of Wisconsin-Madison.

References

[ABK+06] E. Allender, H. Buhrman, M. Koucky, D. van Melkebeek, and D. Ronneburger. Power from random strings. *SIAM Journal on Computing,* 35:14671493, 2006.

[AD17] E. Allender, B. Das. Zero Knowledge and Circuit Minimization. *Information and Computation,* 256:2 8, 2017.

[AGvM+18] E. Allender, J. A. Grochow, D. van Melkebeek, C. Moore, and A. Morgan. Minimum circuit size, graph isomorphism, and related problems. *9th Innovations in Theoretical Computer Science Conference, ITCS*, volume 94 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:20, 2018.

[KS06] N. Kayal and N. Saxena. Complexity of ring Morphism problems. *Computational Complexity*, 15(4):342390, 2006.

[Lad75] R. E. Ladner. On the Structure of Polynomial Time Reducibility. *Journal of the ACM,* 22(1):155171, 1975.

[McD74] B. R. McDonald. Finite Rings with Identity. *Marcel Dekker, Inc.,* 1974.

[Rud17] M. Rudow. Discrete Logarithm and Minimum Circuit Size. *Information Processing Letters,* 128:1 4, 2017.

[SdSV18] N. M. Sdroievski, M. V. G. da Silva and A. L. Vignatti. The Hidden Subgroup Problem and MKTP. *Electronic Colloquium on Computational Complexity (ECCC).* 25:193, 2018.

[Tra85] B. A. Trakhtenbrot. A survey of Russian approaches to perebor (brute-force searches) algorithms. *IEEE Annals of the History of Computing,* 6(4):384400, 1984.