On the Ring Isomorphism & Automorphism Problems

Neeraj Kayal, Nitin Saxena *
National University of Singapore, Singapore
and
IIT Kanpur, India
{kayaln, nitinsa}@cse.iitk.ac.in

Abstract

We study the complexity of the isomorphism and automorphism problems for finite rings with unity.

*We show that both integer factorization and graph isomorphism reduce to the problem of counting automorphisms of rings. The problem is shown to be in the complexity class **AM** $\cap$ co**AM** and hence is not **NP**-complete unless the polynomial hierarchy collapses. Integer factorization also reduces to the problem of finding nontrivial automorphism of a ring and to the problem of finding isomorphism between two rings.*

We also show that deciding whether a given ring has a non-trivial automorphism can be done in deterministic polynomial time.

1 Introduction

A *ring* consists of a set of elements together with addition and multiplication operations. These structures are fundamental objects of study in mathematics and particularly so in algebra and number theory. It has long been recognized that the group of automorphisms of a ring provides valuable information about the structure of the ring. Galois initiated the study of the group of automorphisms of a field and it was later applied by Abel to prove the celebrated theorem that there does not exist any formula for finding the roots of a quintic (degree 5) polynomial. However, to the best of our knowledge, the computational complexity of the ring isomorphism and automorphism related problems has not been investigated thus far. In this paper, we initiate such a study and show interesting connections to some well known problems.

*This work was done while the authors were visiting Princeton University, Princeton, NJ, USA in 2003-04. Also partially supported by research funding from Infosys Technologies Limited, Bangalore.

We will restrict our attention to finite rings with unity. We assume that the rings are given in terms of the *basis* of their additive group and the multiplication table of basis elements. Given two rings in this form, the *ring isomorphism* problem is to test if the rings are isomorphic. We show that this problem is in $\mathbf{NP} \cap co\mathbf{AM}$ and is at least as hard as the graph isomorphism problem. Thus, ring isomorphism is a natural algebraic problem whose complexity status is similar to that of graph isomorphism. The search version of the isomorphism problem is to *find* an isomorphism between two given rings. We show that integer factoring reduces to the search version of the problem.

Another variant of the problem is to *count* the number of isomorphisms between two rings. We show that both integer factorization and graph isomorphism reduce to this problem. We also show that this problem is equivalent to that of counting the *number of automorphisms in a ring* and lies in the class $\mathrm{FP}^{\mathbf{AM} \cap co\mathbf{AM}}$. This implies that the problem is not **NP**-hard unless the polynomial hierarchy collapses to $\mathbf{\Sigma_2^P}$ [Sch88].

The *ring automorphism* problem is to test if a ring has a non-trivial automorphism. We prove that this problem is in **P**. This is in contrast to the corresponding problem for graphs whose status is still open. On the other hand we show that the problem of *finding* a nontrivial automorphism of a given ring is equivalent to integer factoring. This implies that the search version of the problem is likely to be strictly harder than the decision version.

The most general problem here is to *compute* the automorphism group of a given ring, in terms of a small set of generators. It is easy to see that all the above problems reduce to it. Also, the proof of upper bound on counting automorphisms can be adapted to exhibit an **AM** protocol for it implying that this problem too is not **NP**-hard unless PH $= \mathbf{\Sigma_2^P}$.

2 Representation of finite rings

The complexity of the problems involving finite rings depends on the representation used to specify the ring. We will use the following natural representation of a ring:

Definition 2.1. Basis representation of rings: A ring R is given by first describing its additive group in terms of n generators and then specifying multiplication by giving for each pair of generators, their product as an element of the additive group.

$$(R, +, .) := \langle (d_1, d_2, d_3, \cdots, d_n), ((a_{ij}^k))_{1 \le i,j,k \le n} \rangle$$

where, for all $1 \le i, j, k \le n,\ 0 \le a_{ij}^k < d_k$.

This specifies a ring R generated by n elements $e_1, e_2, \cdots e_n$ with each e_i having additive order d_i and $(R, +) = \langle e_1 \rangle \oplus \langle e_2 \rangle \cdots \oplus \langle e_n \rangle$. Thus $(R, +)$ has the structure $(R, +) \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$. Moreover multiplication in R is specified by specifying the product of each pair of generators as an integer linear combination of the generators: for $1 \le i, j \le n$, $e_i \cdot e_j = \sum_{k=1}^{n} a_{ij}^k e_k$.

Definition 2.2. Representation of maps on rings: Suppose R_1 is a ring given in terms of its additive generators $e_1, \ldots, e_n$ and ring R_2 given in terms of $f_1, \ldots, f_n$. In this paper maps on rings would invariably be homomorphisms on the additive group. Then to specify any map $\phi : R_1 \to R_2$, it is enough to give the images $\phi(e_1), \ldots, \phi(e_n)$. So we represent ϕ by an $n \times n$ matrix of integers A, such that for all $1 \le i \le n$:

$$\phi(e_i) = \sum_{j=1}^{n} A_{ij} f_j$$

and for all $1 \le i, j \le n,\ 0 \le A_{ij} <$ additive order of f_j.

Algebraic structures mostly break into simpler objects. In the case of rings we get the following simpler rings.

Definition 2.3. 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 $R \cong R_1 \otimes R_2$, where $\otimes$ denotes the natural composition of two rings with component wise addition and multiplication.

We collect some of the known results about rings. Their proofs can be found in algebra texts, e.g. [McD74].

Proposition 2.4. [Structure theorem for abelian groups] *If R is a finite ring then its additive group $(R, +)$ can be uniquely (up to permutations) expressed as:*

$$(R, +) \cong \bigoplus_i \mathbb{Z}_{p_i{}^{\alpha_i}}$$

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

Remark. This theorem can be used to check in polynomial time whether for two rings, given in basis form, the additive groups are isomorphic or not. Suppose the two additive groups are $G := \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$ and $G' := \mathbb{Z}_{d'_1} \oplus \cdots \oplus \mathbb{Z}_{d'_n}$. We can take *gcd* of d_is and d'_js and keep factoring them till we stop getting nontrivial factors. At this point G will be isomorphic to G' if and only if the multi-sets $\{d_i\}_i$ and $\{d'_i\}_i$ are equal.

Proposition 2.5. *Given a ring R in terms of generators, all having prime-power additive orders, we can compute the number of automorphisms of the additive group of R, $\#Aut(R, +)$, in polynomial time.*

Proof. Refer to appendix. □

Proposition 2.6. [Structure theorem for rings] *If R is a finite ring with unity then it can be uniquely (up to permutations) decomposed into indecomposable rings $R_1, \ldots, R_s$ such that*

$$R = R_1 \otimes \ldots \otimes R_s.$$

Remark. It follows immediately from the proof ([McD74]) of above proposition that for a commutative ring R its decomposition can be found in polynomial time given oracles to integer and polynomial factorizations. Observe that any commutative ring R with characteristic n can be expressed as:

$$R \ \cong\ \mathbb{Z}_n[x_1, \ldots, x_m]/(f_1(\overline{x}), \ldots, f_l(\overline{x}))$$

and so if we can factor n into its prime factors and multivariate polynomials f_is into irreducible factors (modulo prime powers) then we can effectively factor ring R into its indecomposable components.

Let us also define the multiplication operation on ideals which will be useful in the last section.

Definition 2.7. Let $\mathcal{I}, \mathcal{J}$ be two ideals of a ring R. We define their product as

$$\mathcal{I} \cdot \mathcal{J} :=\ \text{ring generated by the elements } \{ij \mid i \in \mathcal{I}, j \in \mathcal{J}\}$$

$\mathcal{I}^t$, for positive integer t, is defined similarly.
It is easy to see that $\mathcal{I} \cdot \mathcal{J}$ is again an ideal of R.

Finally, we define the ring isomorphism and related problems that we are going to explore.

- The *ring isomorphism problem* is to check whether two given rings are isomorphic. The corresponding language we define as

  $$\textbf{RI} \ :=\ \{(R_1, R_2) \mid \text{rings } R_1, R_2 \text{ are given in the basis representation and } R_1 \cong R_2\}.$$

- $\#$**RI** is defined as the functional problem of *computing the number of isomorphisms* between two rings given in basis form.

- $\#$**RA** is defined as the functional problem of *computing the number of automorphisms* of a given ring. Its decision version can be viewed as the language

$$\textbf{cRA} := \{(R,k) \mid R \text{ is a ring in basis form s.t. } \#Aut(R) \geq k\}.$$

- **RA** is defined as the problem of determining whether a given ring has a *nontrivial ring automorphism*. The corresponding language is:

$$\textbf{RA} := \{R \mid R \text{ is a ring in basis form s.t. } \#Aut(R) > 1\}.$$

3 The Complexity of RI

In this section we prove upper and lower bounds on the complexity of Ring Isomorphism problem. Specifically, we show that **RI** is in **NP** $\cap$ co**AM** and the Graph Isomorphism problem reduces to **RI**.

Theorem 3.1. ***RI*** $\in$ ***NP*** $\cap$ ***coAM***.

Proof. We start with the easier part,

Claim 3.1.1. ***RI*** $\in$ ***NP***.

Proof of Claim 3.1.1. Suppose we are given two rings R and R' together with a map $\phi : R \to R'$. Let

$$(R,+) = \mathbb{Z}_{m_1} e_1 \oplus \ldots \oplus \mathbb{Z}_{m_n} e_n$$

Here we can assume that $(m_1,\ldots,m_n) = (d_1^{\alpha_{11}}, d_1^{\alpha_{12}}, \ldots, d_2^{\alpha_{21}}, d_2^{\alpha_{22}}, \ldots, d_t^{\alpha_{t1}}, d_t^{\alpha_{t2}}, \ldots)$ where $d_1,\ldots,d_t$ are mutually coprime. For otherwise $\exists i \neq j$ s.t. $gcd(m_i,m_j) =: g > 1$ and can be used to break m_i or m_j into coprime factors $a,b \in \mathbb{Z}^{>1}$, hence, breaking $(R,+)$ further by applying:

$$(\mathbb{Z}_{ab} e_k, +) \cong \mathbb{Z}_a(be_k) \oplus \mathbb{Z}_b(ae_k)$$

If $(R,+) \cong (R',+)$ we can apply this process to get basis representations of both the rings R and R' over

$$\mathbb{Z}_{d_1^{\alpha_{11}}} \oplus \mathbb{Z}_{d_1^{\alpha_{12}}} \oplus \ldots \oplus \mathbb{Z}_{d_2^{\alpha_{21}}} \oplus \ldots \oplus \mathbb{Z}_{d_t^{\alpha_{t1}}} \oplus \ldots, \text{ for some}$$

coprime $d_1, d_2, \ldots, d_t$.

Let us define for all $1 \leq i \leq t$,

$$R_i := \{r \in R \mid r \text{ has a power-of-}d_i \text{ additive order}\}$$

and similarly R_i's. Now since the d_i's are mutually coprime it is easy to see that ϕ is an isomorphism from $R \to R'$ iff $\forall i$ ϕ isomorphically maps R_i to R_i'. Thus, wlog we can assume that the additive basis of the rings R and R' is given in the form:

$$\mathbb{Z}_{d^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{d^{\alpha_n}} \text{ where } 1 \leq \alpha_1 \leq \ldots \leq \alpha_n$$

Now in this case ϕ is an isomorphism from $R \to R'$ iff it satisfies the following conditions:

- $det(A) \in \mathbb{Z}_d^*$, where A is the $n \times n$ integer matrix describing the map $\phi : R \to R'$.
- for all $1 \leq i \leq n$, additive order of e_i is the same as that of $\phi(e_i)$.
- for all $1 \leq i,j \leq n$, $\phi(e_i) \cdot \phi(e_j) = \sum_{k=1}^n a_{ij}^k \phi(e_k)$, where $((a_{ij}^k))_{n^2 \times n}$ is the same matrix as given in the description of R.

All these three conditions can be checked in polynomial time. The first two conditions above imply that ϕ is an isomorphism on the additive structure of the two rings, *i.e.* $(R,+) \cong (R',+)$. The third condition ensures that ϕ preserves the multiplicative structure too, *i.e.* for all i,j; $\phi(e_ie_j) = \phi(e_i)\phi(e_j)$. $\square$

The **AM** protocol for ring non-isomorphism is similar to that for graph non-isomorphism.

Claim 3.1.2. ***RI*** $\in$ ***coAM***

Proof of Claim 3.1.2. Arthur has two rings R_1, R_2 in basis forms and he wants a *proof* of their non-isomorphism from Merlin. Arthur checks whether $(R_1,+) \cong (R_2,+)$ (see remark of prop. 2.4), if not then Arthur already has a proof of non-isomorphism. Now Merlin can provide the descriptions of $(R_1,+),(R_2,+)$ in the form:

$$(R_1,+) = \bigoplus_{i=1}^n \mathbb{Z}_{p_i^{\alpha_i}} e_i \text{ and}$$

$$(R_2,+) = \bigoplus_{i=1}^n \mathbb{Z}_{p_i^{\alpha_i}} f_i, \text{ where } p_i\text{'s are primes and } \alpha_i \in \mathbb{Z}^{\geq 1}.$$

Let us also define a set related to the ring R_1:

$C(R_1) := \{\langle ((a_{ij}^k))_{n^2 \times n}, A_\phi \rangle \mid \exists \pi \in Aut(R_1,+)$ s.t. for all $1 \leq i,j \leq n$, $\pi(e_i) \cdot \pi(e_j) = \sum_{k=1}^n a_{ij}^k \pi(e_k)$; for all $1 \leq i,j,k \leq n$, $0 \leq a_{ij}^k < p_k^{\alpha_k}$; A_ϕ is an integer matrix describing some $\phi \in Aut(R_1)$ wrt the additive basis $\{\pi(e_i)\}_{i=1}^n\}$.

$C(R_2)$ is defined similarly by replacing the e_i's above by the f_i's. (Note that in the case of graph isomorphism we consider all permutations on the vertices, here we consider all automorphisms of the additive group.)

It is not difficult to see that $\#C(R) = \#Aut(R,+)$ which can be computed in polynomial time when $(R,+)$ is given in terms of generators all having prime-power additive orders (see prop. 2.5). Thus, Arthur can compute $s := \#Aut(R_1,+) = \#Aut(R_2,+)$.

Define $C(R_1,R_2) := C(R_1) \cup C(R_2)$. Note that:

$$\begin{aligned} R_1 \cong R_2 &\Rightarrow C(R_1) = C(R_2) \\ &\Rightarrow \#C(R_1,R_2) = \#C(R_1) = s \\ R_1 \ncong R_2 &\Rightarrow C(R_1) \cap C(R_2) = \emptyset \\ &\Rightarrow \#C(R_1,R_2) = \#C(R_1) + \#C(R_2) = 2s \end{aligned}$$

Thus, the size of the set $C(R_1,R_2)$ has a gap of 2 between the cases of $R_1 \cong R_2$ and $R_1 \ncong R_2$, which can be distinguished by a standard **AM** protocol. □

The two claims show that **RI** is in **NP** ∩ co**AM**. □

This shows that the ring isomorphism problem cannot be **NP**-hard (unless polynomial hierarchy collapses to $\mathbf{\Sigma}_2^P$ [Sch88]). The proofs above were all similar in spirit to those for graph isomorphism which hints a connection to graph isomorphism. Indeed, we can lower bound the complexity of **RI** by graph isomorphism (**GI**).

Theorem 3.2. ***GI*** $\leq_m^P$ ***RI***.

Proof. The proof involves constructing a commutative local ring that captures the "connectivity" of a given graph. We associate variables to each vertex (v-variable) and pair of vertices (a-variable). The characteristic of a variable encodes whether the variable corresponds to a vertex or an edge or a non-edge of the graph. The product of two vertex-variables is defined to be an a-variable while the other products are defined to be zero.

Given a graph G with n vertices, m edges. Choose an odd prime p and let $l := \binom{n}{2}$. Let $\{a_k\}_k$ be a set of l variables indexed by $k \in \{(i,j) \mid 1 \leq i < j \leq n\}$. Define the following *commutative* ring:

$$R(G) := \mathbb{Z}_{p^3}[v_1,\ldots,v_n,a_1,\ldots,a_l]/I$$

where, ideal I has the following relations:

1. for all $1 \leq i \leq n$, $v_i^2 = 0$.
2. for all $1 \leq i < j \leq n$, $v_j v_i = v_i v_j = a_e$ where $e = (i,j)$.
3. for all i,j; $a_j v_i = v_i a_j = 0,\ a_i a_j = 0$.
4. for all $1 \leq i < j \leq n$, if $e = (i,j) \in E(G)$ then $pa_e = 0$ else $p^2 a_e = 0$.

The v_i's represent the n vertices and have an additive order of p^3. The a_i's with additive order p are for the m edges. Finally, the a_i's with additive order p^2 represent the $(l-m)$ non-edges.

The additive structure of the ring is:

$$(R(G),+) = \mathbb{Z}_{p^3} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}_{p^3} v_i \oplus \bigoplus_{e \in E(G)} \mathbb{Z}_p a_e \oplus \bigoplus_{e \notin E(G)} \mathbb{Z}_{p^2} a_e$$

Multiplication satisfies the associative law simply because the product of any three *variables* (in any order) is zero.

Observe that if $G \cong G'$ then any graph isomorphism ϕ induces a natural isomorphism between rings $R(G)$ and $R(G')$. So we only have to prove the converse:

Claim 3.2.1. *For any two undirected graphs (having no self-loops) G and G', if $R(G) \cong R(G')$ then $G \cong G'$.*

Proof of Claim 3.2.1. Suppose ϕ is an isomorphism from $R(G) \to R(G')$. Let

$$\phi(v_1) = c_{10} + c_{11}v_1' + \ldots + c_{1n}v_n' + (\text{linear combination of } a_i's), \text{ where all coefficients are in } \mathbb{Z}_{p^3} \quad (1)$$

Since, $\phi(v_1)^2 = 0$ we get:

$$c_{10}^2 + (2c_{10}c_{11})v_1' + \ldots + (2c_{10}c_{1n})v_n' + (\text{linear combination of } a_i's) = 0$$

As $1, v_i's$ and $a_j's$ form an additive basis of $R(G')$, we conclude:

$$c_{10}^2 = 2c_{10}c_{11} = \ldots = 2c_{10}c_{1n} = 0 \pmod{p^3}$$

Since p is an odd prime, if $c_{10} \neq 0 \pmod{p^3}$ then $p | c_{10}, c_{11}, \ldots, c_{1n}$. But then by equation (1), $p^2\phi(v_1) = 0$ which is a contradiction to the fact that ϕ is an isomorphism. Thus, $c_{10} = 0 \pmod{p^3}$. Now at least one of the c_{1i}'s has to be a unit (*i.e.* coprime to p) otherwise again by equation (1), $p^2\phi(v_1) = 0$. Say, c_{1i_0} is a unit. From the equation:

$$0 = \phi(v_1)^2 = \sum_{1 \leq i < j \leq n} (2c_{1i}c_{1j})v_i'v_j' \quad (2)$$

it follows that if $(i_0, j) \in E(G)$, for some $j \neq i_0$, then $p | c_{1j}$ else $p^2 | c_{1j}$. Thus, we have shown that *exactly* one of the $c_{11}, \ldots, c_{1n}$ is a unit. So we can define a map $\pi : [n] \to [n]$ with $\pi(1) = i_0$ and satisfying the following condition for all $1 \leq i \leq n$:

$$\phi(v_i) = c_{i\pi(i)}v_{\pi(i)}' + p.\sum_{\substack{j=1 \\ j \neq \pi(i)}}^{n} d_{ij}v_j' + (\text{linear combination of } a_k's). \quad (3)$$

where, all coefficients are in $\mathbb{Z}_{p^3}$ and $c_{i\pi(i)}$ is a unit.

Also note that if $\pi(i) = \pi(j)$ then by equation (3) and by the fact that $\phi(v_i)^2 = \phi(v_j)^2 = 0$ (similar to eqn. 2) we deduce: $0 = \phi(v_i)\phi(v_j) = \phi(v_iv_j)$ which forces $i = j$. Hence, π is a permutation on $[n]$.

We are now almost done, we just have to show that π is indeed an isomorphism from $G \to G'$.

Suppose $e = (i, j) \in E(G)$. Thus, (using eqn. 3)

$$\phi(a_e) = \phi(v_iv_j) = (c_{i\pi(i)}c_{j\pi(j)})v'_{\pi(i)}v'_{\pi(j)} + p \cdot (\text{linear combination of } a'_k s).$$

Since, $p \cdot \phi(a_e) = 0$ and $c_{i\pi(i)}c_{j\pi(j)}$ is a unit we get:

$$p \cdot v'_{\pi(i)}v'_{\pi(j)} = 0$$

Whence we conclude that $v'_{\pi(i)}v'_{\pi(j)}$ is of additive order p implying, by the definition of $R(G')$, that $(\pi(i), \pi(j)) \in E(G')$.

By symmetry this shows that π is an isomorphism from $G \to G'$. □

The theorem follows from the claim. □

Another interesting variant of **RI** is its search version- **FRI** -*finding* an isomorphism given two rings. **FRI** is unlikely to be **NP** hard as it reduces to computing the automorphism group of a ring which we observe later to be in second level of low hierarchy. It turns out that solving **FRI** would mean solving integer factoring (**IF**).

Theorem 3.3. ***IF*** $\leq_T^{ZPP}$ ***FRI***.

Proof. Suppose n is an odd number to be factored. Pick a random $a \in \mathbb{Z}_n^*$ and suppose we can find an isomorphism $\phi : \mathbb{Z}_n[x]/(x^2-a^2) \to \mathbb{Z}_n[x]/(x^2-1)$. Let $\phi(x) = bx+c$, b should be in $\mathbb{Z}_n^*$ otherwise there is a $b' \neq 0 (\text{mod } n)$ such that $bb' = 0 (\text{mod } n)$ implying $\phi(b'x - b'c) = 0$ which contradicts that ϕ is an isomorphism. Further,

$$\begin{aligned} & a^2 = \phi(x)^2 = (bx + c)^2 \ (\text{mod } n, x^2 - 1) \\ \Rightarrow \quad & 2bc = 0 (\text{mod } n) \text{ and } b^2 + c^2 - a^2 = 0 (\text{mod } n) \\ \Rightarrow \quad & c = 0 (\text{mod } n) \text{ and } b^2 = a^2 (\text{mod } n) \end{aligned}$$

If n is composite then with probability at least $\frac{1}{2}$, $b \neq \pm a (\text{mod } n)$. Thus, we can factor n in expected polynomial time. □

A related problem to **RI**, however, is hard. Suppose we are given two rings R_1, R_2 and we want to find an isomorphism $\phi : R_1 \to R_2$ such that the corresponding matrix A, which transforms the basis of $(R_1, +)$ to that of $(R_2, +)$, has elements smaller than a given size bound. It turns out that this problem is **NP**-complete.

$\mathbf{RI}_{\text{boundedIso}} := \{(R_1, R_2, ((b_{ij}))_{n\times n}) \mid R_1, R_2$ are rings given in basis form, having additive dimension n and there is an integer matrix $A, \forall i, j \ A_{ij} \leq b_{ij},$ that defines an isomorphism$\}$.

Theorem 3.4. ***RI****boundedIso* ***is NP-complete.***

Proof. Clearly, $\mathbf{RI}_{\text{boundedIso}}$ is in **NP** by claim 3.1.1.

Suppose we are given $R_1 := \mathbb{Z}_n[x]/(x^2 - a^2),\ R_2 := \mathbb{Z}_n[x]/(x^2 - 1),\ \beta \in \mathbb{Z}$ and we want to find out whether there is an isomorphism $\phi(x) = bx$ s.t. $b \leq \beta$. Now as in the proof of theorem 3.3, $b^2 \equiv a^2 (\text{mod } n)$. Thus, the question at hand is equivalent to asking whether the quadratic equation (in y): $y^2 \equiv a^2 (\text{mod } n)$ has a solution $y \leq \beta$, and this is an **NP**-complete problem by [MA76]. □

4 The Complexity of #RA

This section will explore the complexity of the problem of counting ring automorphisms. We will show that this problem is unlikely to be **NP**-hard but both graph isomorphism and integer factoring reduce to it. There is also a connection between #**RI** and #**RA**.

We will show that given a ring R there is an **AM** protocol in which Merlin sends a number l and convinces Arthur that $\#Aut(R) = l$. The ideas in the proof are basically from [BS84].

Theorem 4.1. $\#\mathbf{RA} \in FP^{\mathbf{AM} \cap co\mathbf{AM}}$. [1]

Proof. Let R be a ring given in its basis form. We will first show how Merlin can convince Arthur that $\#Aut(R) \geq k$.

Claim 4.1.1. ***cRA*** $\in$ ***AM***.

Proof of Claim 4.1.1. Merlin can give Sylow subgroups $S_{p_1}, \ldots, S_{p_m}$ of $Aut(R)$, in terms of generators, to Arthur such that $|S_{p_1}| . \cdots . |S_{p_m}| \geq k$ and $p_1, \ldots, p_m$ are distinct primes. Arthur now has to verify whether for a given Sylow subgroup S_p, $|S_p| = p^t$ or not. So Merlin can further provide the composition series of S_p:

$$S_p = G_t > G_{t-1} > \ldots > G_1 > G_0 = \{id\}.$$

Suppose, for the sake of induction, that Arthur is convinced about $|G_i| = p^i$. Then to prove $|G_{i+1}| = p^{i+1}$, Merlin will provide $x_{i+1} \in G_{i+1}$ to Arthur with the claim that $x_{i+1} \notin G_i$ but $x_{i+1}^p \in G_i$. Finally, the only nontrivial thing left for Arthur to verify is whether $x_{i+1} \notin G_i$, which can be verified by a standard **AM** protocol as there is a gap in the size of the set $X :=$ (group generated by x_{i+1} and G_i):

$$\begin{aligned} x_{i+1} \notin G_i \quad & \Rightarrow \quad \#X = p^{i+1} \\ x_{i+1} \in G_i \quad & \Rightarrow \quad \#X = p^i \end{aligned}$$

[1] FP refers to *functional* problems that can be solved in polynomial time.

To avoid too many rounds, Merlin first provides $x_0 = id, x_1, \ldots, x_t \in Aut(R)$ with the proof of: for all $1 \leq i \leq t$, $x_i^p \in G_{i-1} :=$ (group generated by $x_0, \ldots, x_{i-1}$) to Arthur and then provides the proof of: for all $1 \leq i \leq t$, $x_i \notin G_{i-1}$ in one go for Arthur to verify. □

Now we give the **AM** protocol that convinces Arthur of $\#Aut(R) \leq k$.

Claim 4.1.2. *c**RA** $\in$ co**AM**.*

Proof of Claim 4.1.2. Arthur has a ring R and he wants a proof of $\#Aut(R) \leq k$. As in the proof of claim 3.1.2, we can assume that R is given in terms of generators having prime-power additive orders. For concreteness let us assume:

$$(R, +) = \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{\alpha_i}} e_i$$

Merlin sends Arthur a number $l \leq k$ as a candidate value for $\#Aut(R)$ and also provides some Sylow subgroups, the product of their sizes being equal to l, with the **AM**-proofs for their sizes (as used in claim 4.1.1). Let
$X := \{\langle((a_{ij}^k))_{n^2 \times n}\rangle \mid \exists \pi \in Aut(R, +)$ s.t
$\pi(e_i) \cdot \pi(e_j) = \sum_{k=1}^{n} a_{ij}^k \pi(e_k)$; for all $1 \leq i, j, k \leq n$,
$0 \leq a_{ij}^k < p_k^{\alpha_k}\}$.

Observe that $\#X = \frac{\#Aut(R,+)}{\#Aut(R)}$ and $\#Aut(R, +)$ can be computed in polynomial time when $(R, +)$ is given in terms of generators having prime-power additive orders (see prop. 2.5). Thus, Arthur computes $s := \#Aut(R, +)$. Arthur is already convinced that $l | \#Aut(R)$ and he now wants a proof for $\#Aut(R) \leq l$. A proof can be given by utilizing the gap in the size of X in the two cases:

$$\begin{aligned} \#Aut(R) \leq l &\Rightarrow \#X \geq \frac{s}{l} \\ \#Aut(R) > l &\Rightarrow \#Aut(R) \geq 2l \Rightarrow \#X \leq \frac{s}{2l} \end{aligned}$$

□

The claims above show that $\#\mathbf{RA} \in \mathrm{FP}^{\mathbf{cRA}} \subseteq \mathrm{FP}^{\mathbf{AM} \cap \mathrm{co}\mathbf{AM}}$.

□

Remark. It is easy to see that the same protocol as above works for the problem of computing the automorphism group of a ring (in terms of the generators of Sylow subgroups). Thus, this problem too cannot be **NP**-hard.

In the case of graphs it is easy to show that graph isomorphism (or counting graph isomorphisms) reduces to counting graph automorphisms. The same result continues to hold for rings with a slightly more involved proof.

Lemma 4.2. *$\#$**RI** $\equiv_T^P$ $\#$**RA**.*

Proof. Suppose we are given a ring R. Clearly we can compute $\#Aut(R)$ by giving (R, R) as input to the oracle of $\#\mathbf{RI}$.

Conversely, let R_1, R_2 be the two rings given in basis form. Let us assume the following about their decomposability into *distinct* local rings $S_1, \ldots, S_k$:

$R_1 \cong S_1 \otimes \ldots \otimes S_1 \otimes \ldots \otimes S_k \otimes \ldots \otimes S_k$
where, for all $1 \leq i \leq k$, indecomposable ring S_i occurs $a_i \geq 0$ times and $\#Aut(S_i) = m_i$.

$R_2 \cong S_1 \otimes \ldots \otimes S_1 \otimes \ldots \otimes S_k \otimes \ldots \otimes S_k$
where, for all $1 \leq i \leq k$, indecomposable ring S_i occurs $b_i \geq 0$ times.

The following claim relates the (non)isomorphism of the rings to counting ring automorphisms:

Claim 4.2.1. $R_1 \ncong R_2 \Rightarrow \#Aut(R_1 \otimes R_1) \cdot \#Aut(R_2 \otimes R_2) > (\#Aut(R_1 \otimes R_2))^2$.

Proof of Claim 4.2.1. Due to the uniqueness of decomposition of a ring into indecomposable rings:

$$\begin{aligned} \#Aut(R_1 \otimes R_2) &= \#Aut(S_1 \otimes \ldots a_1 + b_1 \text{ times}) \cdots \\ &\quad \#Aut(S_k \otimes \ldots a_k + b_k \text{ times}) \\ &= (a_1 + b_1)! m_1^{a_1+b_1} \cdots \\ &\quad (a_k + b_k)! m_k^{a_k+b_k} \end{aligned}$$

Similarly,

$$\begin{aligned} \#Aut(R_1 \otimes R_1) &= \#Aut(S_1 \otimes \ldots 2a_1 \text{ times}) \cdots \\ &\quad \#Aut(S_k \otimes \ldots 2a_k \text{ times}) \\ &= (2a_1)! m_1^{2a_1} \cdots (2a_k)! m_k^{2a_k} \end{aligned}$$

$$\begin{aligned} \#Aut(R_2 \otimes R_2) &= \#Aut(S_1 \otimes \ldots 2b_1 \text{ times}) \cdots \\ &\quad \#Aut(S_k \otimes \ldots 2b_k \text{ times}) \\ &= (2b_1)! m_1^{2b_1} \cdots (2b_k)! m_k^{2b_k} \end{aligned}$$

Notice that $\binom{2a_i+2b_i}{a_i+b_i} \geq \binom{2a_i+2b_i}{2a_i}$ which implies $(2a_i)! \cdot (2b_i)! \geq (a_i + b_i)!^2$. This clearly shows:

$$\#Aut(R_1 \otimes R_1) \cdot \#Aut(R_2 \otimes R_2) \geq (\#Aut(R_1 \otimes R_2))^2$$

Now since $R_1 \ncong R_2$, there exists an $i_0 \in [k]$ such that $a_{i_0} \neq b_{i_0}$ in which case $(2a_{i_0})! \cdot (2b_{i_0})! \gneq (a_{i_0} + b_{i_0})!^2$. Thus,

$$\#Aut(R_1 \otimes R_1) \cdot \#Aut(R_2 \otimes R_2) > (\#Aut(R_1 \otimes R_2))^2.$$

□ □

As a corollary of this we get:

Theorem 4.3. Graph Isomorphism $\leq_T^P$ #RA.

Proof. Immediate from theorem 3.2 & lemma 4.2. □

Another interesting open problem that reduces to #**RA** is integer factorization- **IF**.

Theorem 4.4. ***IF*** $\leq_T^{\mathrm{ZPP}}$ #**RA**.

Proof. Let n be the *odd* integer to be factored. Consider the ring

$$R := \mathbb{Z}_n[x]/(x^2)$$

We will show that $\#Aut(R) = \phi(n) := |\mathbb{Z}_n^*|$. The theorem is then immediate as n can be factored in expected polynomial time if we are given $\phi(n)$, see [Mil76].

Suppose $\psi \in Aut(R)$ and let $\psi(x) = ax + b$, for some $a, b \in \mathbb{Z}_n$. Since ψ is an automorphism; a, b should satisfy the following two conditions:

$$(ax+b)^2 = 0 \text{ in } R \Rightarrow ab = b^2 = 0 \pmod n, \text{ and}$$

$$a \in \mathbb{Z}_n^*.$$

These two conditions force $b = 0$ and any $a \in \mathbb{Z}_n^*$ will work. Thus, $\#Aut(R) = |\mathbb{Z}_n^*| = \phi(n)$. □

5 The Complexity of RA

This section studies the problem of checking whether a given ring is rigid (*i.e.* has no nontrivial automorphism) and if not then finding a nontrivial automorphism.

We will show that **RA** can be decided in deterministic polynomial time but finding a nontrivial automorphism is as hard as integer factoring.

Theorem 5.1. ***RA*** $\in$ ***P***.

Proof. Let R be a ring given in basis form. Let us first dispose off the case when R is non-commutative.

Claim 5.1.1. *If R is a non-commutative ring then it has a nontrivial automorphism.*

Proof of Claim 5.1.1. It can be shown ([Len04]) that if the *units* in a ring R commute with the whole of R then $R =< R^* >$, and consequently R will be commutative. Thus, if R is a non-commutative ring then there is a *unit* $r \in R$ that doesn't commute with the whole of R. Then clearly the map $\phi : x \mapsto rxr^{-1}$ gives a nontrivial automorphism of R. □

When R is commutative we first consider the case of odd sized R. We intend to give a classification of rigid commutative rings. We will show that indecomposable *components* of a rigid commutative odd-sized ring R are isomorphic to $\mathbb{Z}_{p^m}$, for some odd prime p:

Claim 5.1.2. *If R is an indecomposable rigid commutative odd-sized ring then $\exists$ prime p and $m \in \mathbb{N}$ such that, $R \cong \mathbb{Z}_{p^m}$.*

Proof of Claim 5.1.2. It is known (e.g. see [McD74]) that any indecomposable commutative ring R contains an associated *Galois ring* G such that:

$G = \mathbb{Z}_{p^m}[x]/(f(x))$ where square-free $f(x)$ is irreducible over $\mathbb{Z}_p$ and,

$R = G[x_1, \ldots, x_k]/(x_1^{n_1}, \ldots, x_k^{n_k}, g_1, \ldots, g_l)$ where g_i's are polynomials in $(x_1, \ldots, x_k)$.

Now if additionally R is rigid then G has to be $\mathbb{Z}_{p^m}$ otherwise G would have a nontrivial automorphism[2] and hence R would have a nontrivial automorphism.

Let $\mathcal{M} :=$ (ring generated by $p, x_1, \ldots, x_k$) be the unique maximal ideal of R and let $t > 0$ be the least integer such that $\mathcal{M}^t = 0$. If $t = 1$ then $R = \mathbb{Z}_p$, thus, assume that $t > 1$. We can assume wlog that x_1 does not occur as a linear term with unit coefficient in any of the relations $g_1, \ldots, g_l$ (if it does we can eliminate x_1 by repeated substitutions). Now choose $\alpha \in \mathcal{M}^{t-1} \setminus \{0, -x_1\}$ and it is easy to see that the map

$$\phi : \begin{cases} x_1 & \mapsto x_1 + \alpha \\ x_2 & \mapsto x_2 \\ & \vdots \\ x_k & \mapsto x_k \end{cases}$$

induces a nontrivial automorphism of R. This contradiction implies that there can be no *variable* in R and therefore $R = \mathbb{Z}_{p^m}$.

Remark. If R was even sized then $\mathcal{M}^{t-1} \setminus \{0, -x_1\}$ could be empty as in the case of $R := \mathbb{Z}_2[x]/(x^2)$, where $\mathcal{M} = \{0, x\}$.

□

As a consequence of the above observations we have that any rigid commutative odd-sized ring R looks like: $\bigotimes_i \bigotimes_j \mathbb{Z}_{p_i^{\alpha_{ij}}}$ where, p_i's are distinct odd primes and

$$1 \leq \alpha_{i1} < \alpha_{i2} < \ldots . \tag{4}$$

Our algorithm for **RA** will test whether a given ring R is of the form (4) or not.

As in the proof of claim 3.1.1, we can assume wlog that the input ring R is given as

$$(R, +) = \mathbb{Z}_{d^{\alpha_1}} e_1 \oplus \ldots \oplus \mathbb{Z}_{d^{\alpha_n}} e_n$$

[2] If $m = 1$ then the map sending $x \mapsto x^p$ is an automorphism of G, for larger m this automorphism can be *lifted* using Hensel lifting.

We can also assume that α_i's are distinct (say, $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_n$) otherwise R would not be rigid as it would not be of the form (4).

Now we sketch an algorithm to check whether R is isomorphic to:

$$\mathbb{Z}_{d^{\alpha_1}} \otimes \ldots \otimes \mathbb{Z}_{d^{\alpha_n}} \tag{5}$$

1) Compute $f(x) :=$ minpoly of e_1 over $\mathbb{Z}_{d^{\alpha_n}}$. This can be found out by checking whether e_1^i can be written as a linear combination of $1, e_1, \ldots, e_1^{i-1}$ which amounts to doing linear algebra $(\text{mod } d^{\alpha_n})$.

2) If $R \cong \mathbb{Z}_{d^{\alpha_1}} \otimes \ldots \otimes \mathbb{Z}_{d^{\alpha_n}}$ then say $e_1 = (\beta_1, \ldots, \beta_n)$ where $\beta_i \in \mathbb{Z}_{d^{\alpha_i}}$. Also, since e_1 has characteristic d^{α_1} and $\alpha_1 \lneq \alpha_2, \ldots, \alpha_n$ we can deduce: β_1 is coprime to d and $d | \beta_2, \ldots, \beta_n$.

   These observations mean that
   $f(x) = \text{lcm}_{i=1}^n \{\text{minpoly of } \beta_i \text{ over } \mathbb{Z}_{d^{\alpha_i}}\}$
   $\equiv (x - \beta_1)x^l \ (\text{mod } d), \ \text{ for some } l \in \mathbb{Z}^{\geq 0}$

   or else R is not of the form (5). So we have a non-repeating root $\beta_1 (\text{mod } d)$ of $f(x) (\text{mod } d)$ and we can use Hensel lifting (see [LN86]) to find a root of $f(x) (\text{mod } d^{\alpha_1})$, which gives β_1.

3) Consider $e_1 - \beta_1 = (0, \beta_2 - \beta_1, \ldots, \beta_n - \beta_1)$. Note that $\beta_2 - \beta_1, \ldots, \beta_n - \beta_1$ are all coprime to d. So if we compute $R_1 := \{\gamma \in R \mid (e_1 - \beta_1)\gamma = 0\}$ then $R_1 \cong \mathbb{Z}_{d^{\alpha_1}}$ or else R is not of the form (5).

4) Let $\hat{e}_1 \in R$ be the unity of R_1. Compute $R_1^{\perp} := \{\gamma \in R \mid \hat{e}_1 \gamma = 0\}$. Check that $R = R_1 \otimes R_1^{\perp}$ otherwise R is not of the form (5).

5) Recursively check whether $R_1^{\perp} \cong \mathbb{Z}_{d^{\alpha_2}} \otimes \ldots \otimes \mathbb{Z}_{d^{\alpha_n}}$ or not.

Let us now take up the case of even sized commutative ring. It is sufficient to consider a ring R whose size is a power of 2. We will show that R is rigid only if the indecomposable rings that appear in the decomposition of R are isomorphic to either $\mathbb{Z}_{2^m}$ or $\mathbb{Z}_2[x]/(x^2)$.

Claim 5.1.3. *If R is an indecomposable rigid commutative power-of-2 sized ring then R is either $\mathbb{Z}_{2^m}$ or $\mathbb{Z}_2[x]/(x^2)$.*

Proof of Claim 5.1.3. Let $\mathcal{M}$ be the unique maximal ideal of R and t be the least integer such that $\mathcal{M}^t = 0$. As in the proof of claim 5.1.2, the rigidity of R implies that
$R = \mathbb{Z}_{2^m}[x_1, \ldots, x_k]/(x_1^{n_1}, \ldots, x_k^{n_k}, g_1, \ldots, g_l)$
where g_i's are polynomials in $(x_1, \ldots, x_k)$.

also, either R is $\mathbb{Z}_{2^m}$ or R is univariate and $\mathcal{M}^{t-1} = \{0, -x_1\}$. In the latter case $\mathcal{M} = \{0, -x_1\}$ and $\mathcal{M}^2 = 0$, which implies that $R = \mathbb{Z}_2[x_1]/(x_1^2)$. □

It follows from the above claim that a commutative power-of-2 sized ring is rigid iff it is isomorphic to one of the following:

$$\mathbb{Z}_{2^{\alpha_1}} \otimes \ldots \otimes \mathbb{Z}_{2^{\alpha_n}} \text{ or}$$

$$\mathbb{Z}_2[x]/(x^2) \otimes \mathbb{Z}_{2^{\alpha_1}} \otimes \ldots \otimes \mathbb{Z}_{2^{\alpha_n}}$$

where, $1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_n$.

Since we can factor polynomials over $\mathbb{Z}_{2^m}$ we can compute the decomposition of R into indecomposable rings (see remark of prop. 2.6) and check whether they are of the forms: $\mathbb{Z}_{2^m}, \mathbb{Z}_2[x]/(x^2)$ or not. Hence, we can check the rigidity of even sized rings too in polynomial time.

□

On the other hand the search version of this problem *i.e.* finding a nontrivial ring automorphism (**FRA**) is as hard as integer factoring (**IF**).

Theorem 5.2. ***IF*** $\equiv_T^{ZPP}$ ***FRA***.

Proof. Let us first see how we can find a nontrivial ring automorphism if we can do integer factoring. Suppose the given ring R is non-commutative then we know from the proof of claim 5.1.1: there is a *unit* of R that does not commute with the whole of R and thus defines a nontrivial automorphism. So we compute the multiplicative generators of R^* in *randomized* polynomial time and surely one of the generators will not commute with the whole of ring R.

Now assume the given ring R is commutative. It can be decomposed into local rings, as remarked in proposition 2.6, in expected polynomial time using randomized methods for polynomial factorization and oracle of integer factorization. Once we have local rings we can output nontrivial automorphisms like ϕ in the proof of claim 5.1.2.

Conversely, suppose we can find nontrivial automorphisms of rings and n is a given number. Let us assume for simplicity that input n is a product of two distinct primes p, q. Randomly choose a cubic $f(x) \in \mathbb{Z}[x]$. Define $R := \mathbb{Z}_{pq}[x]/(f(x))$ and suppose we can find a nontrivial automorphism ϕ of R. It follows from the distribution of irreducible polynomials over finite fields that with probability $\sim \frac{1}{9}$: $f (\text{mod } q)$ is irreducible *and* $f (\text{mod } p)$ has exactly two irreducible factors f_1, f_2, say f_1 is linear. Thus,

$$R \cong \mathbb{Z}_p \otimes \mathbb{Z}_p[x]/(f_2(x)) \otimes \mathbb{Z}_q[x]/(f(x)).$$

Note that we can compute R^{ϕ}, the set of elements of R fixed by ϕ, using linear algebra (if at any point we cannot invert an element $(\text{mod } n)$, we get a factor of n). Let us now see what R^{ϕ} can be given that $R^{\phi} \neq R$.

1) If ϕ fixes $\mathbb{Z}_p[x]/(f_2(x))$:
   Then $R^{\phi} \cong \mathbb{Z}_p \otimes \mathbb{Z}_p[x]/(f_2(x)) \otimes \mathbb{Z}_q$. Thus, $|R^{\phi}| = p^3 q$.

2) If ϕ fixes $\mathbb{Z}_q[x]/(f(x))$:
Then $R^\phi \cong \mathbb{Z}_p \otimes \mathbb{Z}_p \otimes \mathbb{Z}_q[x]/(f(x))$. Thus, $|R^\phi| = p^2q^3$.

3) If ϕ moves both $\mathbb{Z}_p[x]/(f_2(x))$ and $\mathbb{Z}_q[x]/(f(x))$:
Then $R^\phi \cong \mathbb{Z}_p \otimes \mathbb{Z}_p \otimes \mathbb{Z}_q$. Thus, $|R^\phi| = p^2q$.

Since, the size of R^ϕ is in no case of the form n, n^2 or n^3, the process of finding R^ϕ by doing linear algebra $(\mathrm{mod}\, n)$ is going to yield a factor of n. In particular, this means that if the matrix describing ϕ over the natural additive basis $\{1, x, x^2\}$ is:

$$A := \begin{pmatrix} 1 & 0 & 0 \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix}$$

then the determinant of one of the submatrices of $(A - I)$ will have a nontrivial gcd with n.

This idea can be extended to the case of composite n having more prime factors.

Thus, the two problems: finding nontrivial automorphisms of commutative rings and integer factoring have the same complexity. □

6 Open Problems

Let us recap what we know about the various ring isomorphism related problems. The solid arrows in Figure 1 indicate a polynomial time reduction (randomized reduction indicated by **RP**). A dotted arrow from $\mathcal{C}$ to Σ_2 means that $\Sigma_2^{\mathcal{C}} = \Sigma_2$, thus indicating that *probably* $\mathcal{C}$ is not **NP** hard. **ComRA** denotes the problem of computing the group of automorphisms of a ring (in terms of generators) together with its size.

We would like to ask the following questions:

- We have seen two well-known problems of intermediate complexity reduce to $\#$**RA**. Can one reduce some other such problem, e.g., DiscreteLog?
- The ring problems differ from the graph ones in their (in)ability to efficiently "fix" part of the automorphisms. This property allows one to prove the equivalence between computing automorphism groups, counting automorphisms, finding isomorphisms, and testing isomorphisms in the case of graphs. For rings, we cannot prove such equivalence. Does there exist some way of doing such "fixing" for rings which will allow us to prove similar equivalences?
- Is $\#$**RA** $\in$ **BQP** ?
- Consider the ring isomorphism problem over rationals: $\mathbf{RI}_{\mathbb{Q}}$. It is not even clear if this problem is decidable.

Acknowledgment

We would like to thank Manindra Agrawal, Hendrik Lenstra and Shien Jin Ong for many useful discussions. We especially thank Manindra Agrawal for lots of suggestions that made the paper readable. We thank Hendrik Lenstra for pointing out that **RA** $\in$ **P** even for noncommutative finite rings.

References

[AT04] V. Arvind and Jacobo Toran. *Solvable group isomorphism is (almost) in $NP \cap coNP$.* Proc. 19^{th} IEEE Conference on Computational Complexity, 2004.

[BS84] L. Babai and E. Szemeredi. *On the complexity of matrix group problems.* Proc. 25^{th} IEEE Foundations of Computer Science, 1984, 229-240.

[GW02] O. Goldreich and A. Wigderson. *Derandomization That Is Rarely Wrong from Short Advice That Is Typically Good.* Proceedings of the 6^{th} International Workshop on Randomization and Approximation Techniques, 2002, 209-223.

[Len04] Hendrik Lenstra, Jr. *Private communication.* 2004.

[LN86] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications.* Cambridge University Press, 1986.

[MA76] K. Manders and L. Adleman. *NP-complete decision problems for quadratic polynomials.* Proceedings of the 8^{th} ACM Symposium on Theory of Computing, 1976, 23-29.

[Mil76] G. L. Miller. *Riemann's hypothesis and tests for primality.* Journal of Computer and System Science, **13**, 1976, 300-317.

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

[Sch88] U. Schoning. *Graph isomorphism is in the low hierarchy.* Journal of Computer and System Science, **37**, 1988, 312-323.

Appendix

Theorem *Given a ring R in terms of additive generators, all having prime-power additive orders, we can compute the $\#Aut(R, +)$ in polynomial time.*

Proof. Let $(R,+)$ be given as $\cong \bigoplus_{i=1}^{l} \bigoplus_j \mathbb{Z}_{{p_i}^{\alpha_{ij}}}$, where p_i's are distinct primes and $\alpha_{ij} \geq 1$. For $1 \leq i \leq l$ define subrings R_i of R as:

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

Observe that

$$R \cong \bigotimes_{i=1}^{l} R_i$$

this is because if $r_i \in R_i$ and $r_j \in R_j$ $(i \neq j)$ then for some $c_i, c_j \in \mathbb{Z}^{\geq 0}$, $p_i^{c_i} r_i r_j = p_j^{c_j} r_i r_j = 0$ which implies that $r_i r_j = 0$ (since p_i, p_j are coprime) and by a similar argument $r_1, \ldots, r_l$ are *linearly independent*.

This decomposition of R gives us:

$$\#Aut(R,+) = \prod_{i=1}^{l} \#Aut(R_i,+)$$

Thus, it suffices to show how to compute $\#Aut(R,+)$ when $(R,+)$ is given as $\cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p^{\alpha_i}}$ where p is a prime and $\alpha_i \in \mathbb{Z}^{\geq 1}$.

Suppose we are given R in terms of the following additive basis:

$$\begin{aligned}(R,+) \quad = \quad & \mathbb{Z}_{p^{\beta_1}} e_{11} \oplus \ldots \oplus \mathbb{Z}_{p^{\beta_1}} e_{1n_1} \oplus \ldots \\ & \ldots \oplus \mathbb{Z}_{p^{\beta_m}} e_{m1} \oplus \ldots \oplus \mathbb{Z}_{p^{\beta_m}} e_{mn_m}\end{aligned}$$

where, $n_1 + \ldots + n_m = n$ and $1 \leq \beta_1 < \ldots \beta_m$.

Observe that $\phi \in Aut(R,+)$ iff the matrix A describing the map ϕ is invertible $(\text{mod } p)$ and preserves the additive orders of e_{ij}'s. Our intention is to count the number of all such matrices A. To do that let us see how A looks:

$$A = \begin{pmatrix} B_{11} & B_{12} & \ldots & B_{1m} \\ B_{21} & B_{22} & \ldots & B_{2m} \\ \vdots & \ldots & \ddots & \vdots \\ B_{m1} & B_{m2} & \ldots & B_{mm} \end{pmatrix}_{n \times n}$$

where the block matrices B_{ij}'s are integer matrices of size $n_i \times n_j$. The properties of these block matrices which make A describe an automorphism of $(R,+)$ are:

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

It is not difficult to see that the number of matrices satisfying these conditions can be found in time polynomial in $(n_1\beta_1 + \ldots + n_m\beta_m)(\log p)$, and hence the number of A's which describe an automorphism of $(R,+)$. □

One can also consider a different, exponentially larger, representation for rings: when the rings are given in terms of the addition and multiplication tables of all its elements. We do not know if the ring isomorphism problem under this representation can be solved in time polynomial in the size of the representation. However, the problem is likely to be in **NP** $\cap$ *co***NP**.

Let us give this problem a name:

$$\begin{aligned}\mathbf{RI}_{TF} \quad := \quad & \{(R_1, R_2) \mid R_1, R_2 \text{ are given in terms of tables,} \\ & R_1 \cong R_2\}\end{aligned}$$

It is easy to see that $\mathbf{RI}_{TF} \in$ **NP**. The nontrivial part is to show:

Theorem *There exists an **NP**-machine that decides all but $2^{\log^8 n}$ instances of $\overline{\mathbf{RI}}_{TF}$ of length n.*

Proof. The proof is basically one given in [AT04] applied to the case of rings.

We showed in claim 3.1.2 that $\overline{\mathbf{RI}}_{TF} \in \mathbf{AM}(\log^5 n)$, where the parameter bounds the number of random bits used by Arthur. Notice that the number of binary strings that define a ring of size at most n, in basis form, is no more than $2^{\log^3 n}$. ∴ by probability amplification: the random bits used in the **AM** protocol would work for *all* input strings of size n if we use $\log^8 n$ many random bits. Since we are using only a "small" number of random bits we can apply techniques of [GW02] to get an **NP**-machine that fails for at most $2^{\log^8 n}$ inputs of size n. □

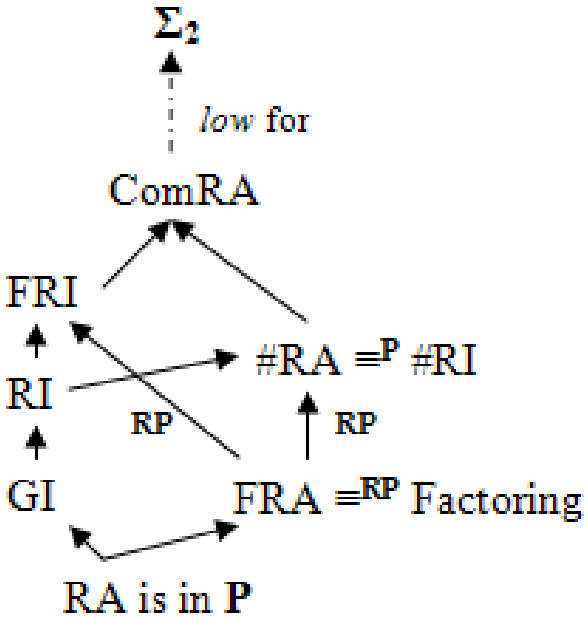

Figure 1. Relations among ring isomorphism and automorphism problems.