Automorphisms of Finite Rings and Applications to Complexity of Problems

Manindra Agrawal and Nitin Saxena

National University of Singapore**
{agarwal,nitinsax}@comp.nus.edu.sg

1 Introduction

In mathematics, automorphisms of algebraic structures play an important role. Automorphisms capture the symmetries inherent in the structures and many important results have been proved by analyzing the automorphism group of the structure. For example, Galois characterized degree five univariate polynomials f over rationals whose roots can be expressed using *radicals* (using addition, subtraction, multiplication, division and taking roots) via the structure of automorphism group of the splitting field of f. In computer science too, automorphisms have played a useful role in our understanding of the complexity of many algebraic problems. From a computer science perspective, perhaps the most important structure is that of finite rings. This is because a number of algebraic problems efficiently reduce to questions about automorphisms and isomorphisms of finite rings. In this paper, we collect several examples of this from the literature as well as providing some new and interesting connections.

As discussed in section 2, finite rings can be represented in several ways. We will be primarily interested in the *basis* representation where the ring is specified by its basis under addition. For this representation, the complexity of deciding most of the questions about the automorphisms and isomorphisms is in $\mathrm{FP}^{\mathrm{AM}\cap\mathrm{coAM}}$ [KS04]. For example, *finding ring automorphism* (find a non-trivial automorphism of a ring), *automorphism counting problem* (count the number of automorphisms of a ring), *ring isomorphism problem* (decide if two rings are isomorphic), *finding ring isomorphism* (find an isomorphism between two rings). Also, *ring automorphism problem* (decide if a ring has a non-trivial automorphism) is in P [KS04]. In addition, a number of problems can be reduced to answering these questions. Some of them are:

Primality Testing. Fermat's Little Theorem states that the map $a \mapsto a^n$ is the trivial automorphism in Z_n if n is prime. Although this property is not strong enough to decide primality, the recent deterministic primality test [AKS04] generalizes this to the property that the map is an automorphism in the ring $Z_n[Y]/(Y^r - 1)$ for a suitable r iff n is prime. Further, they prove that it is enough to test the correctness of the map at a "few" elements to guarantee that it is indeed an automorphism.

** On leave from Indian Institute of Technology, Kanpur.

Polynomial Factorization. Factoring univariate polynomials over finite fields uses automorphisms in a number of ways [LN86,vzGG99]. It is used to split the input polynomial into factors with each one being square-free and composed only of same degree irreducible factors. Then to transform the problem of factoring polynomial with equal degree irreducible factors to that of root finding. And finally, in finding the roots of the polynomial in the field (this step is randomized while the others are deterministic polynomial-time).

Integer Factorization. Two of the fastest known algorithms for factoring integers, *Quadratic sieve* [Pom84] and *Number Field sieve* [LLMP90], essentially aim to find a non-obvious automorphism of the ring $Z_n[Y]/(Y^2-1)$. Besides, recently [KS04] have shown that integer factorization can be reduced to (1) automorphism counting for ring $Z_n[Y]/(Y^2)$, (2) finding automorphism of the ring $Z_n[Y]/(f(Y))$ where f is a degree three polynomial, (3) finding isomorphism between rings $Z_n[Y]/(Y^2-1)$ and $Z_n[Y]/(Y^2-a^2)$ where $a \in Z_n$.

Graph Isomorphism. Again, [KS04] show this problem reduces to ring isomorphism problem for rings of the form $Z_{p^3}[Y_1,\ldots,Y_n]/\mathcal{I}$ where p is an odd prime and ideal $\mathcal{I}$ has degree two and three polynomials. Here, we improve this result to the rings with any prime characteristic. As the isomorphism problems for a number of structures reduce to Graph Isomorphism (e.g., Group Isomorphism), this shows that all these problems reduce to ring isomorphism and counting automorphisms of a ring (it can be shown easily that ring isomorphism problem reduces to counting automorphism in a ring [KS04]).

Polynomial Equivalence. Two polynomials $p(x_1,\cdots,x_n)$ and $q(x_1,\ldots,x_n)$ over field F are said to be *equivalent* if there is an invertible linear transformation T, $T(x_i)=\sum_{j=1}^{n} t_{i,j}x_j$, $t_{i,j} \in F$, such that $p(T(x_1),\ldots,T(x_n)) = q(x_1,\ldots,x_n)$.[1] This is a well studied problem: we know a lot about the structure of equivalent polynomials when both p and q are *quadratic forms* (homogeneous degree two polynomials) resulting in a polynomial time algorithm for testing their equivalence (Witt's equivalence theorem, see, e.g., [Lan93]). The structure of *cubic forms* (homogeneous degree three polynomials) is less understood though. There is also a cryptosystem based on the difficulty of deciding equivalence between a collection of degree three polynomials [Pat96]. In [Thi98], it was shown that polynomial equivalence problem is in NP $\cap$ coAM and Graph Isomorphism reduces to *polynomial isomorphism* problem where we require T to be a permutation.

Here, we show that the ring isomorphism problem over finite fields reduces to *cubic polynomial equivalence*. We prove a partial converse as well: deciding equivalence of homogeneous degree k polynomials with n variables over field F_q such that $(k, q-1)=1$, reduces to ring isomorphism problem in time $n^{O(k)}$. This shows that (1) equivalence for homogeneous constant degree polynomials (for certain degrees) can be efficiently reduced to equivalence for degree three polynomials, and (2) Graph Isomorphism reduces to equivalence

[1] In some literature, p and q are said to be equivalent if $p=q$ for all elements in F^n.

for degree three polynomials. In fact, we show that Graph Isomorphism can even be reduced to cubic form equivalence. This explains, at least partly, why cubic form equivalence has been hard to analyze.

The organization of the remaining paper is as follows. The next section discusses the various representations of the rings and their morphisms. Sections 3 to 7 discuss applications of ring automorphisms and isomorphisms in the order outlined above. The last section lists some open questions.

2 Representations of Rings and Automorphisms

We will consider finite rings with identity. Any such ring R can be represented in multiple ways. We discuss three important representations.

Table Representation

The simplest representation is to list all the elements of the ring and their addition and multiplication tables. This representation has size $n = O(|R|^2)$ where $|R|$ is the number of elements of the ring. This is a highly redundant representation and the problem of finding automorphisms or isomorphisms can be solved in $n^{O(\log n)}$ time since any minimal set of generators for the additive group has size $O(\log n)$.

Basis Representation

This representation is specified by a set of generators of the additive group of R. Let n be the *characteristic* of the ring. Then the additive group $(R, +)$ can be expressed as the direct sum $\oplus_{i=1}^{m} Z_{n_i} b_i$ where b_1, ..., b_m are elements of R and $n_i \mid n$ for each i. The elements b_1, ..., b_m are called *basis elements* for $(R, +)$. Therefore, the ring R can be represented as $(n_1, \ldots, n_m, A_1, \ldots, A_m)$ where matrix $A_i = (a_{i,j,k})$ describes the effect of multiplication on b_i, viz., $b_i \cdot b_j = \sum_{k=1}^{m} a_{i,j,k} b_k$, $a_{i,j,k} \in Z_{n_k}$. The size of this representation is $O(m^3)$. This, in general, is exponentially smaller than the size of the ring $|R| = \prod_{i=1}^{m} n_i$. For example, the ring Z_n (it has only one basis element).

The problem of finding automorphisms or isomorphisms becomes harder for this representation. As [KS04] show, these problems belong to the complexity class $\mathrm{FP}^{\mathrm{AM} \cap \mathrm{coAM}}$ and are at least as hard as factoring integers and—in the case of finding isomorphisms—solving graph isomorphism.

Polynomial Representation

A third, and even more compact, representation of R is obtained by starting with the basis representation and then selecting the smallest set of b_is, say b_1, ..., b_m such that the remaining b_is can be expressed as polynomials in b_1, ..., b_m. The representation can be specified by the m basis elements and generators

of the ideal of polynomials satisfied by these. Each polynomial is specified by an arithmetic circuit.

The ring can be written as:

$$R = Z_n[Y_1, Y_2, \ldots, Y_m]/(f_1(Y_1, \ldots, Y_m), \ldots, f_k(Y_1, \ldots, Y_m))$$

where Y_1, ..., Y_m are basis elements and $(f_1(Y_1, \ldots, Y_m), \ldots, f_k(Y_1, \ldots, Y_m))$ is the ideal generated by the polynomials f_1, ..., f_k describing all polynomials satisfied by Y_1, ..., Y_m.[2] Often, this representation is exponentially more succinct that the previous one. For example, consider the ring $Z_2[Y_1, \ldots, Y_m]/(Y_1^2, Y_2^2, \ldots, Y_m^2)$. This ring has 2^m basis elements and so the basis representation would require $\Omega(2^{3m})$ space.

The problem of finding automorphisms or isomorphisms is even harder for this representation:

Theorem 1. *Ring automorphism for polynomial representation is NP-hard and ring isomorphism problem is coNP-hard.*

Proof. To prove NP-hardness of ring automorphism problem, we reduce 3SAT to it. Let F be a 3CNF boolean formula over n variables, $F = \wedge_{i=1}^{m} c_i$. Let $\hat{F} = \prod_{i=1}^{m} \hat{c}_i$ and $\hat{c}_i = 1 - (1 - x_{i_1}) \cdot x_{i_2} \cdot (1 - x_{i_3})$ where $c_i = x_{i_1} \vee \bar{x}_{i_2} \vee x_{i_3}$. It is easy to verify that F is unsatisfiable iff $\hat{F}(x_1, \ldots, x_n) \in (x_1^2 - x_1, \ldots, x_n^2 - x_n)$. Let ring

$$R = F_2[Y_1, \ldots, Y_n]/(1 + \hat{F}(Y_1, \ldots, Y_n), \{Y_i^2 - Y_i\}_{1 \leq i \leq n}).$$

It follows that R is a trivial ring iff formula F is unsatisfiable. So ring $R \oplus R$ has a non-trivial automorphism iff F is satisfiable.

For hardness of ring isomorphism problem, simply note that ring R is isomorphic to trivial ring $\{0\}$ iff F is unsatisfiable.

So the table representation is too verbose while the polynomial representation is too compact. In view of this, we will restrict ourselves to the basis representation for the rings. The rings that we will consider are all commutative with a basis that has all basis elements of the same additive order. In addition, their polynomial representation is of similar size to the basis representation and so, for clarity of exposition, we will use the polynomial representation to express our rings.

Representation of Automorphisms and Isomorphisms

An *automorphism* ϕ of ring R is a one-one and onto map, $\phi : R \mapsto R$ such that for all $x, y \in R$, $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

[2] Throughout the paper, we use lower case letters, e.g., x, y for free variables (as in polynomial $p(x, y) = x^2 - 2y$) and upper case letters, e.g., X, Y for bound variables (as in the ring $Z_n[X, Y]/(X^2 - 2Y, Y^2)$).

An *isomorphism* between two rings R_1 and R_2 is a one-one and onto map ϕ, $\phi : R_1 \mapsto R_2$ such that for all $x, y \in R_1$, $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

Their representations will depend on the representation chosen for the rings. For basis representation, an automorphism (and isomorphism) will be represented as a linear transformation mapping basis elements. Thus, it corresponds to an invertible matrix of dimension n where n is the number of basis elements.

For polynomial representation, say $R = Z_n[Y_1, \ldots, Y_t]/\mathcal{I}$, an automorphism (or isomorphism) ϕ will be specified by a set of t polynomials p_1, ..., p_t with $\phi(Y_i) = p_i(Y_1, \ldots, Y_t)$.

3 Application: Primality Testing

A number of primality tests use the properties of the ring Z_n where n is the number to be tested. The prominent ones are Miller-Rabin test [Mil76,Rab80], Solovay-Strassen test [SS77], Adleman-Pomerance-Rumely test [APR83] etc. There are several others that use a different algebraic structure, e.g., elliptic curve based tests [GK86].

However, even the ones based on Z_n use properties other than automorphisms of Z_n. The reason is that approaches based on automorphisms do not work. For example, when n is prime, the map $\phi(x) = x^n$ is an automorphism (in fact it is the trivial automorphism); on the other hand when n is composite then ϕ may not be an automorphism. We can use this to design a test, however, as testing if $\phi(x) = x \pmod n$ for all x's requires exponential time, we do the test for only polynomially many x's. This test *does* separate prime numbers from non-square-free composites (see Lemma 1 below), however fails for square-free composites. The reason are Carmichael numbers [Car10]: these are composite numbers for which ϕ is the trivial automorphism.

So an automorphism based property *appears* too weak to separate primes from composites. However, it is not so. The strongest known deterministic primality test [AKS04] is based on the same property of automorphisms as outlined above! What makes it work is the idea of using a polynomial ring instead of Z_n. Let $R = Z_n[Y]/(Y^r - 1)$ where r is a "small" number. As before, the map ϕ remains an automorphism of R when n is prime. It is easy to see that ϕ is an automorphism of R iff for every $g(Y) \in R$,

$$g^n(Y) = \phi(g(Y)) = g(\phi(Y)) = g(Y^n). \tag{1}$$

As above, this can be tested for polynomially many $g(Y)$'s. It was shown in [AKS04] that for a suitably chosen r, if the equation (1) holds for $\sqrt{r}\log n$ many $g(Y)$'s of the form $Y + a$ then n must be a prime power. The analysis in the paper can easily be improved to show that when a's are chosen from $[1, \sqrt{r}\log n]$ then n must be a prime: Suppose equation (1) holds for all a's in the above range. Then we know that n is a prime power. Let $n = p^k$ for some $k > 1$. Let ring $R_0 = Z_{p^2}[Y]/(Y - 1) \cong Z_{p^2}$. Clearly, equation (1) will hold in R_0 too. This

implies that for all $a \leq 1 + \sqrt{r}\log n$:

$$a^{p^k} = a \pmod{p^2}.$$

The choice of r is such that $r \geq \log^2 n$ [AKS04] and therefore, the above equation holds for all $a \leq 4\log^2 p$. The following lemma, proved by Hendrik Lenstra [Len] contradicts this:

Lemma 1. *(Hendrik Lenstra) For all large enough primes p, for every $\ell > 0$ there is an $a \leq 4\log^2 p$ such that $a^{p^\ell} \neq a \pmod{p^2}$.*

Proof. Suppose there is an $\ell > 0$ such that $a^{p^\ell} = a \pmod{p^2}$ for all $a \leq 4\log^2 p$. We first prove that we can always assume ℓ to be 1. Consider the case when $\ell > 1$. Since $a^p = a \pmod{p}$, we have

$$a^p = a + p \cdot t \pmod{p^2}$$

for some t. Therefore,

$$\begin{aligned} a^{p^\ell} &= (a + p \cdot t)^{p^{\ell-1}} \pmod{p^2} \\ &= a^{p^{\ell-1}} \pmod{p^2} \end{aligned}$$

Repeating this, we get $a^p = a^{p^\ell} = a \pmod{p^2}$. Now, there are at most p solutions to the equation $a^p = a \pmod{p^2}$ in Z_{p^2}. Since all numbers up to $4\log^2 p$ are solutions to this, so will be all their products. Let $\psi(p^2, 4\log^2 p)$ denote the number of distinct numbers less than p^2 that are $4\log^2 p$-smooth (all their prime factors are at most $4\log^2 p$). Using the bound for ψ [CEG83], $\psi(x, x^{1/u}) = x \cdot u^{-u+o(1)}$ for $u = O(\frac{x}{\log x})$, we get that $\psi(p^2, 4\log^2 p) > p$ for large enough p. This is a contradiction. □

So when n is composite then for at least one of $Y + a$'s, ϕ does not satisfy equation 1 and the test works correctly.

4 Application: Factoring Polynomials

Automorphisms play a central role in efficient factoring of univariate polynomials over finite fields. We outline a randomized polynomial time factoring algorithm using automorphisms. This, and similar algorithms can be found in any text book discussing polynomials over of finite fields, e.g., [LN86,vzGG99]. Let f be a degree d polynomial over finite field F_q. Let $R = F_q[Y]/(f(Y))$ and $\phi : R \mapsto R$, $\phi(x) = x^q$. Clearly, ϕ is an automorphism of R. Notice that if f is irreducible then ϕ^d is trivial. Conversely, if ϕ^d is trivial then, letting f_0 be an irreducible factor of f, ϕ^d is trivial on the ring $F_q[Y]/(f_0(Y))$ as well. Therefore, degree of f_0 divides d. This can be generalized to show that all irreducible factors of f have degrees dividing k iff ϕ^k is trivial. Moreover, ϕ^k is trivial iff $\phi^k(Y) = Y$. An algorithm for *distinct degree square-free* factorization of f follows: for $k = 1$

to d, compute the gcd of $f(Y)$ and $\phi^k(Y) - Y$. The algorithm can also be used to decide if f is irreducible: f is irreducible iff the smallest k with non-trivial $\gcd(f(Y), \phi^k(Y) - Y)$ is d.

For *equal degree factorization*—given f that is square-free and all irreducible factors of the same degree k—some more work is needed. Find an $t(Y) \in R = F_q[Y]/(f(Y))$ with $t(Y) \notin F_q$ and $\phi(t(Y)) = t(Y)$. Since f is reducible, such a $t(Y)$ always exists and can be found using linear algebra as ϕ is a linear map. Clearly, $t(Y) \pmod{f_i(Y)} \in F_q$ where f_i is an irreducible factor of f and so, $\gcd(t(Y) - x, f(Y)) > 1$ for some $x \in F_q$. This condition can be expressed as a polynomial in x, e.g., $\gcd(t(Y) - x, f(Y)) > 1$ iff $R(t(Y) - x, f(Y)) = 0$ where R is the *resultant* polynomial defined as determinant of a matrix over coefficients on two input polynomials. Therefore, $g(x) = R(t(Y) - x, f(Y)) \in F_q[x]$. By above discussion, a root of this polynomial will provide a factor of f.

To factor $g(x)$, we use the distinct degree factorization method. Choose a random $a \in F_q$ and let $h(x) = g(x + a)$. Then with probability at least $\frac{1}{2}$, $h(x^2)$ can be factored over F_q using the above distinct degree factorization algorithm. To see this, let $g(x) = \prod_{i=1}^{d}(x - \eta_i)$ for $\eta_i \in F_q$. Then $h(x^2) = \prod_{i=1}^{d}(x^2 - \eta_i + a)$. With probability at least $\frac{1}{2}$, there exist i and j such that $\eta_i + a$ is a quadratic residue and $\eta_j + a$ is a quadratic non-residue in F_q. The distinct degree factorization algorithm will separate these factors into two distinct polynomials $h_1(x^2)$ and $h_2(x^2)$. This gives $g(x) = h_1(x - a) \cdot h_2(x - a)$.

Algorithms for polynomial factorization over rationals also (indirectly) use automorphisms since these proceed by first factoring the given polynomial f over a finite field, then use Hensel lifting [Hen18] and LLL algorithm for short lattice vectors [LLL82] to obtain factors over rationals efficiently.

Multivariate polynomial factorization can be reduced, in polynomial time, to the problem of factoring a univariate polynomial via Hilbert irreducibility theorem and Hensel lifting [Kal89]. Therefore, this too, *very* indirectly though, makes use of automorphisms.

5 Application: Factoring Integers

Integer factorization has proven to be much harder than polynomial factorization. The fastest known algorithm is *Number Field Sieve* [LLMP90] with a conjectured time complexity of $2^{O((\log n)^{1/3}(\log\log n)^{2/3})}$. This was preceded by a number of algorithms with provable or conjectured time complexity of $2^{O((\log n)^{1/2}(\log\log n)^{1/2})}$, e.g., Elliptic Curve method [Len87], Quadratic Sieve method [Pom84].

Of these, the fastest two—Quadratic and Number Field Sieve methods—can be easily viewed as trying to find a non-obvious automorphism in a ring. Both the methods aim to find two numbers u and v in Z_n such that $u^2 = v^2$ and $u \neq \pm v$ in Z_n where n is an odd, square-free composite number to be factored. Consider the ring $R = Z_n[Y]/(Y^2 - 1)$. Apart from the trivial automorphism, the ring has another obvious automorphism specified by the map $Y \mapsto -Y$. The problem of finding u and v as above is precisely the one of finding a third automorphism of R.

This can be seen as follows. Let ϕ be an automorphism of R with $\phi(Y) \neq \pm Y$. Let $\phi(Y) = aY + b$. We then have $0 = \phi(Y^2 - 1) = (aY + b)^2 - 1 = a^2 + b^2 - 1 + 2abY$ in R. This gives $ab = 0$ and $a^2 + b^2 = 1$ in Z_n. Notice that $(a, n) = 1$ since otherwise $\phi(\frac{n}{(a,n)}Y) = \frac{n}{(a,n)}b = \phi(\frac{n}{(a,n)}b)$. Therefore, $b = 0$ and $a^2 = 1$. By assumption, $a \neq \pm 1$ and so $u = a$ and $v = 1$. Conversely, given a u and v with $u^2 = v^2$, $u \neq \pm v$ in Z_n, we get $\phi(Y) = \frac{u}{v}Y$ as an automorphism of R.

In fact, as shown in [KS04], factoring integers can be reduced to a number of questions about automorphisms and isomorphisms of rings. They show that an odd, square-free composite number n can be factored in (randomized) polynomial time if

- one can count the number of automorphisms of the ring $Z_n[Y]/(Y^2)$, or
- one can find an isomorphism between rings $Z_n[Y]/(Y^2 - a^2)$ and $Z_n[Y]/(Y^2 - 1)$ for a randomly chosen $a \in Z_n$, or
- one can find a non-trivial automorphism of the ring $Z_n[Y]/(f(Y))$ where f is a randomly chosen polynomial of degree three.

6 Application: Graph Isomorphism

In this section, we consider the application of ring isomorphisms for solving the graph isomorphism problem. It was shown in [KS04] that testing isomorphism between two graphs on n vertices can be reduced to testing the isomorphism between two rings of the form $Z_{p^3}[Y_1, \ldots, Y_n]/\mathcal{I}$ where p is any odd prime and $\mathcal{I}$ is an ideal generated by certain degree two and three polynomials. Here, borrowing ideas from [KS04] and [Thi98] we give a different, and more general, reduction.

Let $G = (V, E)$ be a simple graph on n vertices. We define polynomial p_G as:

$$p_G(x_1, \ldots, x_n) = \sum_{(i,j) \in E} x_i \cdot x_j.$$

Also, define ideal $\mathcal{I}_G$ as:

$$\mathcal{I}_G(x_1, \ldots, x_n) = (p_G(x_1, \ldots, x_n), \{x_i^2\}_{1 \leq i \leq n}, \{x_i x_j x_k\}_{1 \leq i,j,k \leq n}). \qquad (2)$$

Then,

Theorem 2. *Simple graphs G_1 and G_2 over n vertices are isomorphic iff either $G_1 = G_2 = K_m \cup D_{n-m}$ (D_{n-m} is a collection of $n-m$ isolated vertices) or rings $R_1 = F_q[Y_1, \ldots, Y_n]/\mathcal{I}_{G_1}(Y_1, \ldots, Y_n)$ and $R_2 = F_q[Z_1, \ldots, Z_n]/\mathcal{I}_{G_2}(Z_1, \ldots, Z_n)$ are isomorphic. Here F_q is a finite field of odd characteristic.*[3]

Proof. If the graphs are isomorphic, then the map ϕ, $\phi : R_1 \mapsto R_2$, $\phi(Y_i) = Z_{\pi(i)}$, is an isomorphism between the rings where π is an isomorphism mapping

[3] The theorem also holds for fields of characteristic two. For such fields though, we need to change the definition of the ideal $\mathcal{I}_G$. It now contains $x_{n+1} \cdot p_G$, x_i^3's and $x_i x_j x_k x_\ell$'s and the ring is defined over $n + 1$ variables. The proof is similar.

G_1 to G_2. This follows since $\phi(p_{G_1}(Y_1, \ldots, Y_n)) = p_{G_2}(Z_1, \ldots, Z_n)$. Conversely, suppose that G_2 is not of the form $K_m \cup D_{n-m}$ and the two rings are isomorphic. Let ϕ, $\phi : R_1 \mapsto R_2$ be an isomorphism. Let

$$\phi(Y_i) = \alpha_i + \sum_{1 \le j \le n} \beta_{i,j} Z_j + \sum_{1 \le j < k \le n} \gamma_{i,j,k} Z_j Z_k.$$

Since $Y_i^2 = 0$ in the ring,

$$0 = \phi(Y_i^2) = \phi^2(Y_i) = \alpha_i^2 + (\text{higher degree terms}).$$

This gives $\alpha_i = 0$. Again looking at the same equation:

$$0 = \phi(Y_i^2) = \phi^2(Y_i) = 2 \sum_{1 \le j < k \le n} \beta_{i,j} \beta_{i,k} Z_j Z_k.$$

If more than one $\beta_{i,j}$ is non-zero, then we must have $\sum_{j,k \in J, j<k} \beta_{i,j} \beta_{i,k} Z_j Z_k$ divisible by $p_{G_2}(Z_1, \ldots, Z_n)$ where J is the set of non-zero indices. Since p_{G_2} is also homogeneous polynomial of degree two, it must be a constant multiple of the above expression implying that $G_2 = K_{|J|} \cup D_{n-|J|}$. This is not possible by assumption. Therefore, at most one $\beta_{i,j}$ is non-zero. Now suppose that *all* $\beta_{i,j}$'s are zero. But then $\phi(Y_i Y_\ell) = 0$ which is not possible. Hence, *exactly one* $\beta_{i,j}$ is non-zero for every i.

Define $\pi(i) = j$ where j is the index with $\beta_{i,j}$ non-zero. Suppose $\pi(i) = \pi(\ell)$ for $i \neq \ell$. Then, $\phi(Y_i Y_\ell) = 0$. Again, this is not possible. Hence π is a permutation on $[1, n]$. Now consider $\phi(p_{G_1}(Y_1, \ldots, Y_n))$. It follows that:

$$\begin{aligned} 0 &= \phi(p_{G_1}(Y_1, \ldots, Y_n)) \\ &= \sum_{(i,j) \in E_1} \phi(Y_i)\phi(Y_j) \\ &= \sum_{(i,j) \in E_1} \beta_{i,\pi(i)} \beta_{j,\pi(j)} Z_{\pi(i)} Z_{\pi(j)} \end{aligned}$$

The last expression must be divisible by p_{G_2}. This gives $\beta_{i,\pi(i)} = \beta_{\ell,\pi(\ell)}$ for all i and ℓ. This implies that the expression is a constant multiple of p_{G_2}, or equivalently, that G_1 is isomorphic to G_2. □

Notice that the rings R_1 and R_2 constructed above have lots of automorphisms. For example, $Y_i \mapsto Y_i + Y_1 Y_2$ is a non-trivial automorphism of R_1. Therefore, automorphisms of graph G_1 do not directly correspond to automorphisms of the ring R_1. In fact, each automorphism of G_1 gives rise to at least $p^{n \cdot (\binom{n}{2} - 1)}$ automorphisms of R_1 (this is the number of ways we can add quadratic terms to the automorphism map).

7 Application: Polynomial Equivalence

Thomas Thierauf [Thi98] analyzed the complexity of *polynomial isomorphism* problem where one tests if the two given polynomials, say p and q, become equal

after a permutation of variables of p. He showed that this problem is in NP $\cap$ coAM and Graph Isomorphism reduces to it. His upper bound proof can easily be generalized to polynomial equivalence. We first prove a lower bound by showing that ring isomorphism problem reduces to it.

Theorem 3. *Ring isomorphism problem for rings of prime characteristic reduces, in polynomial time, to cubic polynomial equivalence.*

Proof. For this proof, we adopt the basis representation of rings. Let R and R' be two rings with additive basis $b_1, \ldots, b_n$ and $d_1, \ldots, d_n$ respectively and characteristic p. Multiplication in R is defined as

$$(\forall)\ i, j, 1 \leq i, j \leq n : b_i \cdot b_j = \sum_{k=1}^{n} a_{i,j,k} b_k \text{ where } a_{i,j,k} \in F_p.$$

Let us define a polynomial which *captures* the relations defining ring R:

$$f_R(\bar{y}, \bar{b}) := \sum_{1 \leq i \leq j \leq n} y_{i,j} \left(b_i b_j - \sum_{1 \leq k \leq n} a_{i,j,k} b_k \right) \tag{3}$$

Similarly, we define $f_{R'}$ over variables $\bar{z}$ and $\bar{d}$.

Let us start off with an easy observation:

Claim 1 *If rings R and R' are isomorphic then f_R is equivalent to $f_{R'}$.*

Proof of Claim. Let ϕ be an isomorphism from R to R'. Note that ϕ sends each b_i to a linear combination of d's and for all i, j, $\phi(b_i)\phi(b_j) - \sum_{1 \leq k \leq n} a_{i,j,k}\phi(b_k) = 0$ in R'. This implies that there exist c's in F_p such that

$$\phi(b_i)\phi(b_j) - \sum_{1 \leq s \leq n} a_{i,j,s}\phi(b_s) = \sum_{1 \leq k \leq l \leq n} c_{i,j,k,\ell} \left(d_k d_\ell - \sum_{1 \leq s \leq n} a'_{k,\ell,s} d_s \right).$$

This immediately suggests that the linear transformation:

$$b_i \mapsto \phi(b_i)$$
$$\sum_{1 \leq i \leq j \leq n} c_{i,j,k,\ell} y_{i,j} \mapsto z_{k,\ell}$$

makes f_R equal to $f_{R'}$. □

Conversely,

Claim 2 *If f_R is equivalent to $f_{R'}$ then R and R' are isomorphic.*

Proof of Claim. Let ϕ be a linear transformation such that

$$\sum_{1\le i\le j\le n} \phi(y_{i,j}) \left(\phi(b_i)\phi(b_j) - \sum_{1\le k\le n} a_{i,j,k}\phi(b_k) \right)$$

$$= \sum_{1\le i\le j\le n} z_{i,j} \left(d_i d_j - \sum_{1\le k\le n} a'_{i,j,k} d_k \right). \tag{4}$$

This immediately implies that

$$\sum_{1\le i\le j\le n} \phi(y_{i,j})\phi(b_i)\phi(b_j) = \sum_{1\le i\le j\le n} z_{i,j} d_i d_j. \tag{5}$$

We intend to show that $\phi(b_i)$ has no z's, i.e., $\phi(b_i)$ is a linear combination of only d's. We will be relying on the following property of rhs of equation (5): *let τ be an invertible linear transformation on the z's then for all $1 \le i \le j \le n$ the coefficient of $z_{i,j}$ in $\sum_{1\le i\le j\le n} \tau(z_{i,j}) d_i d_j$ is nonzero.*

Suppose $\phi(b_1)$ has z's:

$$\phi(b_1) = \sum_i c_{1,i} d_i + \sum_{ij} c_{1,i,j} z_{i,j}$$

We can apply an invertible linear transformation τ on z's in equation (5) so that $\tau : \sum_{i,j} c_{1,i,j} z_{i,j} \mapsto z_{1,1}$ and then apply an evaluation map *val* by fixing $z_{1,1} \leftarrow -(\sum_i c_{1,i} d_i)$. So equation (5) becomes:

$$\sum_{2\le i\le j\le n} val\circ\tau\circ\phi(y_{i,j} b_i b_j) = \sum_{1\le i\le j\le n; i,j\ne 1,1} z_{i,j}(\text{quadratic } d\text{'s}) + (\text{cubic } d\text{'s}) \tag{6}$$

We repeat this process of applying invertible linear transformations on z's and fixing z's in equation (6) so that for all $2 \le i \le j \le n$, $val \circ \tau \circ \phi(y_{i,j} b_i b_j)$ either vanishes or is a cubic in d's. Thus, after $1 + \binom{n}{2}$ z-fixings the lhs of equation (5) is a cubic in d's while the rhs still has $\binom{n+1}{2} - \binom{n}{2} - 1 = (n-1)$ unfixed z's, which is a contradiction.

Since $\phi(b)$'s have no z's and there are no cubic d's in rhs of equation (4) we can ignore the d's in $\phi(y)$'s. Thus, now $\phi(y)$'s are linear combinations of z's and $\phi(b)$'s are linear combinations of d's. Again looking at equation (4), this means that $\left(\phi(b_i)\phi(b_j) - \sum_{1\le s\le n} a_{i,j,s}\phi(b_s)\right)$ is a linear combination of $\left(d_k d_\ell - \sum_{1\le s\le n} a'_{k,\ell,s} d_s\right)$ where $1 \le k, \ell \le n$. This implies that

$$\left(\phi(b_i)\phi(b_j) - \sum_{1\le s\le n} a_{i,j,s}\phi(b_s) \right) = 0$$

in ring R'. This combined with the fact that ϕ is an invertible linear transformation on $\bar{b}$ means that ϕ induces an isomorphism from ring R to R'. □

The above two claims complete the proof. □

In the case of Graph Isomorphism, we can reduce the problem to cubic form equivalence.

Theorem 4. *Graph Isomorphism reduces in polynomial time to cubic form equivalence.*

Proof. Suppose we are given two graphs G_1 and G_2 and we have rings R_1 and R_2 as in the proof of Theorem 2. To simplify matters suppose $(i_0, j_0) \in E(G_1), E(G_2)$. We fix an additive basis $\{1, b_1, \ldots, b_m\}$ of the ring R_1 over F_p such that

$$b_1 = Y_1, \ldots, b_n = Y_n, \{b_{n+1}, \ldots, b_m\} = \{Y_i Y_j\}_{1 \le i < j \le n} \setminus \{Y_{i_0} Y_{j_0}\}. \tag{7}$$

Note that $m = \binom{n+1}{2} - 1$ and that $\{b_1, \ldots, b_m\}$ is an additive basis of the maximal ideal $\mathcal{M}$ ($\mathcal{M}'$) of *local* ring R_1 (R_2). Also, $b_i b_j = 0$ except for $\binom{n}{2}$ unordered tuples (i, j).

As local rings are isomorphic iff their maximal ideals are isomorphic [McD74], we focus on $\mathcal{M}$ and $\mathcal{M}'$. So let us construct homogeneous cubic polynomials *capturing* the relations in $\mathcal{M}, \mathcal{M}'$. These polynomials are similar to the ones seen in the proof of Theorem 3:

$$f_{\mathcal{M}}(u, \bar{y}, \bar{b}) = \sum_{1 \le i \le j \le m} y_{i,j} \left(b_i b_j - u \sum_{1 \le k \le m} a_{i,j,k} b_k \right) + u^3$$

$$f_{\mathcal{M}'}(v, \bar{z}, \bar{d}) = \sum_{1 \le i \le j \le m} z_{i,j} \left(d_i d_j - v \sum_{1 \le k \le m} a'_{i,j,k} d_k \right) + v^3$$

where, $a_{i,j,k}, a'_{i,j,k} \in \{-1, 0, 1\}$ are given by the definition of ideal $\mathcal{I}_G$ and b's in equations (2) and (7).

Let us start off with the easier side:

Claim 3 *If G_1 is isomorphic to G_2 then $f_{\mathcal{M}}$ is equivalent to $f_{\mathcal{M}'}$.*

Proof of Claim. If G_1 is isomorphic to G_2 then by Theorem 2, R_1 is isomorphic to R_2 which means $\mathcal{M}$ is isomorphic to $\mathcal{M}'$. Now by sending $u \mapsto v$ and following the proof of claim 1, we deduce $f_{\mathcal{M}}$ is equivalent to $f_{\mathcal{M}'}$. □

Conversely,

Claim 4 *If $f_{\mathcal{M}}$ is equivalent to $f_{\mathcal{M}'}$ then G_1 is isomorphic to G_2.*

Proof of Claim. We will try to show that if $f_{\mathcal{M}}$ is equivalent to $f_{\mathcal{M}'}$ then $\mathcal{M}$ is isomorphic to $\mathcal{M}'$, which when combined with Theorem 2 means that the graphs are isomorphic.

Suppose ϕ is an invertible linear transformation on $(u, \bar{y}, \bar{b})$ such that:

$$\sum_{1\le i\le j\le m} \phi(y_{i,j}) \left(\phi(b_i)\phi(b_j) - \phi(u) \sum_{1\le k\le m} a_{i,j,k}\phi(b_k) \right) + \phi(u)^3$$

$$= \sum_{1\le i\le j\le m} z_{i,j} \left(d_i d_j - v \sum_{1\le k\le n} a'_{i,j,k} d_k \right) + v^3. \tag{8}$$

The main idea again is to show that $\phi(b_i)$ is a linear combination of d's and the proof is very similar to the one above.

Suppose $\phi(b_1)$ has z's:

$$\phi(b_1) = c_{1,v}v + \sum_i c_{1,i}d_i + \sum_{i,j} c_{1,i,j}z_{i,j}.$$

As before, We apply an invertible linear transformation τ on z's in equation (8) so that $\tau : \sum_{i,j} c_{1,i,j}z_{i,j} \mapsto z_{1,1}$ and then apply an evaluation map val by fixing $z_{1,1} \leftarrow -(c_{1,v}v + \sum_i c_{1,i}d_i)$. So equation (8) becomes:

$$\sum_{2\le i\le j\le m} val\circ\tau\circ\phi(y_{i,j}b_ib_j) - \sum_{1\le i\le j\le m} val\circ\tau\circ\phi \left(uy_{i,j} \sum_{1\le k\le m} a_{i,j,k}b_k \right) + val\circ\tau\circ\phi(u)^3$$

$$= \sum_{1\le i\le j\le m; i,j\neq 1,1} z_{i,j} \left((\text{quadratic } d\text{'s}) - v(\text{linear } d\text{'s}) \right) + (\text{cubic in } v, d\text{'s}). \tag{9}$$

Note that now on the lhs of the equation (9) there are at most $\binom{m}{2}$ terms of the form $val \circ \tau \circ \phi(y_{i,j}b_ib_j)$. And since except for $\binom{n}{2}$ pairs (i, j), the product b_ib_j is zero, there are at most $\binom{n}{2}$ terms of the form $val \circ \tau \circ \phi \left(uy_{i,j} \sum_{1\le k\le m} a_{i,j,k}b_k \right)$. We repeat this process of applying invertible linear transformations on z's and fixing z's in equation (9) so that the expressions $val \circ \tau \circ \phi(y_{i,j}b_ib_j)$ for $2 \le i \le j \le m$, $val \circ \tau \circ \phi \left(uy_{i,j} \sum_{1\le k\le m} a_{i,j,k}b_k \right)$ for $1 \le i \le j \le m$, and $val \circ \tau \circ \phi(u)^3$ either vanish or are cubics in v and d's. Thus, after at most $1 + \binom{m}{2} + \binom{n}{2} + 1$ z-fixings the lhs of equation (8) is a cubic in v and d's while the rhs still has $\binom{m+1}{2} - \binom{m}{2} - \binom{n}{2} - 2 = m - \binom{n}{2} - 2 = \binom{n+1}{2} - 1 - \binom{n}{2} - 2 = n - 3 > 0$ unfixed z's, which is a contradiction.

So $\phi(b_i)$'s have no z's. Now if $\phi(u)$ has $z_{i,j}$ then there is a nonzero coefficient of $z_{i,j}^3$ on the lhs of equation (8) while $z_{i,j}^3$ does not appear on the rhs. Thus, even $\phi(u)$ has no z's. Looking at equation (8) we deduce that all the z's on the lhs occur in $\phi(y)$'s. So we can apply a suitable invertible linear transformation τ on the z's such that for all $1 \le i \le j \le m$:

$$\tau \circ \phi(y_{i,j}) = z_{i,j} + \sum_{1\le k\le m} c_{i,j,k}d_k + c_{i,j,v}v,$$

and then equation (8) simply looks like:

$$\sum_{1\le i\le j\le m} z_{i,j}\left(\phi(b_i)\phi(b_j) - \phi(u)\sum_{1\le k\le m} a_{i,j,k}\phi(b_k)\right) + (\text{cubic in } v,\ d\text{'s})$$

$$= \sum_{1\le i\le j\le m} z_{i,j}((\text{quadratic } d\text{'s}) - v(\text{linear } d\text{'s})) + v^3.$$

Therefore,

$$\sum_{1\le i\le j\le m} z_{i,j}\left(\phi(b_i)\phi(b_j) - \phi(u)\sum_{1\le k\le m} a_{i,j,k}\phi(b_k)\right)$$

$$= \sum_{1\le i\le j\le m} z_{i,j}((\text{quad } d\text{'s}) - v(\text{linear } d\text{'s})). \tag{10}$$

Let us compare the coefficients of $z_{i,i}$ in equation (10):

$$\phi(b_i)^2 = (\text{quadratic } d\text{'s}) - v(\text{linear } d\text{'s}).$$

This clearly rules out $\phi(b_i)$ having a nonzero coefficient of v. Thus, $\phi(b_i)$'s are linear combinations of d's. Since we have obtained equation (10) from equation (8) by applying *invertible* linear transformation on z's, there has to be a nonzero v coefficient in the rhs and hence in the lhs of equation (10). Thus, $\phi(u)$ has a nonzero v coefficient. Say, for some $c_{u,v} \neq 0$:

$$\phi(u) = c_{u,v}v + \sum_{1\le k\le m} c_{u,k}d_k.$$

For any $1 \le i \le j \le m$, by comparing coefficients of $z_{i,j}$ in equation (10) we get that there exist elements $e_{i,j,k,\ell} \in F_p$ such that:

$$\phi(b_i)\phi(b_j) - \left(c_{u,v}v + \sum_{1\le s\le m} c_{u,s}d_s\right)\sum_{1\le s\le m} a_{i,j,s}\phi(b_s)$$

$$= \sum_{1\le k\le \ell\le m} e_{i,j,k,\ell}\left(d_kd_\ell - v\sum_{1\le s\le m} a'_{k,l,s}d_s\right).$$

By fixing $v = 1$ this actually means that in the ring $\mathcal{M}'$:

$$\phi(b_i)\phi(b_j) = \left(c_{u,v} + \sum_{1\le s\le m} c_{u,s}d_s\right)\sum_{1\le s\le m} a_{i,j,s}\phi(b_s). \tag{11}$$

Notice that there is an inverse of the expression $\left(c_{u,v} + \sum_{1\le s\le m} c_{u,s}d_s\right)$ in the ring R_2 that looks like:

$$\left(c_{u,v} + \sum_{1\le s\le m} c_{u,s}d_s\right)^{-1} = \left(c_{u,v}^{-1} + \sum_{1\le s\le m} c'_{u,s}d_s\right). \tag{12}$$

Since the product of any three terms in $\mathcal{M}'$ vanishes, we get the following when we multiply both sides of equation (11) by the inverse (12) in $\mathcal{M}'$:

$$\begin{aligned} c_{u,v}^{-1}\phi(b_i)\phi(b_j) &= \sum_{1\le s\le m} a_{i,j,s}\phi(b_s) \\ \Rightarrow \frac{\phi(b_i)}{c_{u,v}}\frac{\phi(b_j)}{c_{u,v}} &= \sum_{1\le s\le m} a_{i,j,s}\frac{\phi(b_s)}{c_{u,v}}. \end{aligned}$$

In other words, this means that $b_i \mapsto \frac{\phi(b_i)}{c_{u,v}}$ is an isomorphism from $\mathcal{M} \to \mathcal{M}'$. □

This completes the reduction from graph isomorphism to cubic form equivalence. □

Polynomial equivalence for homogeneous constant degree polynomials efficiently reduces to ring isomorphism for certain degrees.

Theorem 5. *Polynomial equivalence for homogeneous degree d polynomials over field F_q with $(d, q-1) = 1$ reduces, in time $n^{O(d)}$, to ring isomorphism.*

Proof. Let p and q be two homogeneous degree d polynomials over field F_q with n variables. Define rings R_p and R_q as:

$$\begin{aligned} R_p &= F_q[\bar{Y}]/(p(\bar{Y}), \{Y_{j_1}Y_{j_2}\cdots Y_{j_{d+1}}\}_{1\le j_1,j_2,\ldots,j_{d+1}\le n}) \\ R_q &= F_q[\bar{Z}]/(q(\bar{Z}), \{Z_{j_1}Z_{j_2}\cdots Z_{j_{d+1}}\}_{1\le j_1,j_2,\ldots,j_{d+1}\le n}). \end{aligned}$$

It is easy to see that if p and q are equivalent, then R_p and R_q are isomorphic.

The converse is also not difficult. Let ϕ be an isomorphism from R_p to R_q. Let

$$\phi(Y_i) = \alpha_i + \sum_{j=1}^{n} \beta_{i,j}Z_j + (\text{higher degree terms}). \tag{13}$$

The fact $\phi^{d+1}(Y_i) = 0$ implies that $\alpha_i = 0$. Let $\psi(Y_i) = \sum_{j=1}^{n} \beta_{i,j}Z_j$, i.e., the linear component of ϕ. We show that ψ is (almost) an equivalence between p and q.

First of all, ψ is an invertible linear transformation. This is because for every j, there exists a polynomial r_j such that $\phi(r_j(\bar{Y})) = Z_j$ (using the fact that ϕ is an isomorphism). Let r_j^L be the linear part of r_j. Then, $\phi(r_j^L(\bar{Y})) = Z_j +$ (higher degree terms). It follows that $\psi(r_j^L(\bar{Y})) = Z_j$.

Now consider the polynomial p. We have

$$\phi(p(\bar{Y})) \in (q(\bar{Z}), \{Z_{j_1} Z_{j_2} \cdots Z_{j_{d+1}}\}_{1 \leq j_1, j_2, \ldots, j_{d+1} \leq n}).$$

Of the polynomials defining the ideal in above equation, only q is of degree d. Hence the degree d part of $\phi(p(\bar{Y}))$ must be divisible by $q(\bar{Z})$. In other words, $\psi(p(\bar{Y}))$ is divisible by $q(\bar{Z})$. Since both p and q have the same degree, this means $\psi(p(\bar{Y})) = c \cdot q(\bar{Z})$ for $c \in F_q$. Since $(d, q-1) = 1$, there exists an $e \in F_q$ with $e^d = c$. Therefore, the map $\frac{1}{e}\psi$ is an equivalence. □

The restriction on degree in the above theorem, $(d, q-1) = 1$, appears necessary. For example, consider polynomials x^2 and ax^2 over field F_q with a being a quadratic non-residue. These two polynomials are *not* equivalent while the rings defined by them, $F_q[Y]/(Y^2)$ and $F_q[Y]/(aY^2)$ are equal.

8 Open Questions

We have listed a number of useful applications of automorphisms and isomorphisms of finite rings in complexity theory. Our list is by no means exhaustive, but should convince the reader about the importance of these. We pose a few questions that we would like to see an answer of:

- It is not clear if automorphisms play a role in some important algebraic problems, e.g., *discrete log*. This problem can easily be viewed as that of finding a certain kind of automorphism in a group, however, we do not know any connections to ring automorphisms.
- Nearly all the effort in integer factoring has been concentrated towards finding automorphism in the ring $Z_n[Y]/(Y^2 - 1)$. Is there another ring where this problem might be "easier"? Can some of the other formulations of [KS04] be used for factoring?
- Theorems 2 and 4 together show that Graph Isomorphism reduces to equivalence of cubic forms over fields of *any* characteristic. Can the theory of cubic forms (over complex numbers) be used to find a subexponential time algorithm for Graph Isomorphism?
- It appears likely that ring isomorphism problem reduces to equivalence of cubic forms, but we have not been able to find a proof.
- It appears likely that equivalence of constant degree polynomials reduces to ring isomorphism at least when $(d, q-1) = 1$. However, we have been able to prove it only for homogeneous polynomials.

References

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160:1–13, 2004.

[APR83] L. M. Adleman, C. Pomerance, and R. S. Rumely. On distinguishing prime numbers from composite numbers. *Annals of Mathematics*, 117:173–206, 1983.

[Car10] R. D. Carmichael. Note on a number theory function. *Bull. Amer. Math. Soc.*, 16:232–238, 1910.

[CEG83] E. R. Canfield, P. Erdos, and A. Granville. On a problem of Oppenhein concerning "Factorisatio Numerorum". *J. Number Theory*, 17:1–28, 1983.

[GK86] S. Goldwasser and J Kilian. Almost all primes can be quickly certified. In *Proceedings of Annual ACM Symposium on the Theory of Computing*, pages 316–329, 1986.

[Hen18] Kurt Hensel. Eine neue Theorie der algebraischen Zahlen. *Mathenatische Zeitschift*, 2:433–452, 1918.

[Kal89] E. Kaltofen. Factorization of polynomials given by straight-line programs. In S. Micali, editor, *Randomness and Computation*, pages 375–412. JAI press, 1989.

[KS04] Neeraj Kayal and Nitin Saxena. On the ring isomorphism and automorphism problems. Technical Report TR04-109, Electronic Colloquium on Computational Complexity (http://www.eccc.uni-trier.de/eccc), 2004. Available at eccc.uni-trier.de/eccc-reports/2004/TR04-109/Paper.pdf.

[Lan93] S. Lang. *Algebra*. Addison-Wesley, 1993.

[Len] H. W. Lenstra, Jr. Private communication.

[Len87] Hendrik Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[LLL82] Arjen Lenstra, Hendrik Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[LLMP90] Arjan K. Lenstra, Hendrik W. Lenstra, M. S. Manasse, and J. M. Pollard. The number field sieve. In *Proceedings of Annual ACM Symposium on the Theory of Computing*, pages 564–572, 1990.

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

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

[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. Sys. Sci.*, 13:300–317, 1976.

[Pat96] J. Patarin. Hidden field equations (HFE) and isomorphism of polynomials (IP): Two new families of assymetric algorithms. In *EUROCRYPT'96*, pages 33–48. Springer LNCS 1070, 1996.

[Pom84] Carl Pomerance. The quadratic sieve factoring algorithm. In *EUROCRYPT 1984*, pages 169–182. Springer LNCS 209, 1984.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12:128–138, 1980.

[SS77] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6:84–86, 1977.

[Thi98] Thomas Thierauf. The isomorphism problem for read-once branching programs and arithmetic circuits. *Chicago Journal of Theoretical Computer Science*, 1998, 1998.

[vzGG99] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra.* Cambridge University Press, 1999.