Infinite Gröbner Bases And Noncommutative Polly Cracker Cryptosystems

Tapan S. Rai

Dissertation submitted to the faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Mathematics

Edward L. Green, Chair
Ezra Brown
Peter Haskell
Peter Linnell
John Rossi

March 23, 2004
Blacksburg, Virginia

Keywords: Public Key Cryptography, Computational Algebra, Noncommutative Gröbner Bases, Polly Cracker, Information Security.

Infinite Gröbner Bases And Noncommutative Polly Cracker Cryptosystems

Tapan S. Rai

Abstract

We develop a public key cryptosystem whose security is based on the intractability of the ideal membership problem for a noncommutative algebra over a finite field. We show that this system, which is the noncommutative analogue of the Polly Cracker cryptosystem, is more secure than the commutative version. This is due to the fact that there are a number of ideals of noncommutative algebras (over finite fields) that have infinite reduced Gröbner bases, and can be used to generate a public key. We present classes of such ideals and prove that they do not have a finite Gröbner basis under any admissible order. We also examine various techniques to realize finite Gröbner bases, in order to determine whether these ideals can be used effectively in the design of a public key cryptosystem.

We then show how some of these classes of ideals, which have infinite reduced Gröbner bases, can be used to design a public key cryptosystem. We also study various techniques of encryption. Finally, we study techniques of cryptanalysis that may be used to attack the cryptosystems that we present. We show how poorly constructed public keys can in fact, reveal the private key, and discuss techniques to design public keys that adequately conceal the private key. We also show how linear algebra can be used in ciphertext attacks and present a technique to overcome such attacks. This is different from the commutative version of the Polly Cracker cryptosystem, which is believed to be susceptible to "intelligent" linear algebra attacks.

For my parents and my wife

Acknowledgements

First of all, I would like to thank my advisor, Ed Green, for directing my research, and believing in me, when I decided to get back into Mathematics, after a hiatus of almost a decade. Without his support, I might never have achieved this milestone in my career.

I would also like to thank the other members of my committee, most of whom had taught me in various classes in graduate school, or have been professional mentors in other ways. I would particularly like to acknowledge Peter Linnell, who helped renew my interest in Algebra, after an inspiring, but demoralizing semester with Maurice Auslander. I would also like to thank Charlie Aull, who helped me build confidence in my mathematical ability, in the early semesters of my graduate studies. In addition, Bob Mccoy merits mention, for being my advisor through the completion of my prelims, and lending a sympathetic ear, while I spent endless hours, talking about the needs of international graduate students.

There are a number of people that I would like to thank for their support and mentoring in the dark decade that I spent wandering through the mathematical desert. Among these, are Don and Evelyn Mckeon, who have time and again, proved to be the most wonderful international host family, Vic Moose, who helped keep my creative juices flowing in this period, by helping me rediscover my love for writing fiction, and my parents, who lent quiet, unquestioning support, while I struggled to find my career path. This was a period when I learned about life outside the world of mathematics, and made many friends who helped me "just by being there". Of these, I would like to acknowledge Heather Moore, and Bill Spivey, who taught me the meaning of true friendship, and about the American way of life. Of course, I would be remiss, if I didn't acknowledge Scott Elich, and all the employees of Mill Mountain Coffee and Tea, for putting up with me, while I turned cups of coffee into works of fiction and mathematical fact.

The final months of the writing process were made easier by my wife, Madhumita, who provided a pleasing distraction, while ensuring that I didn't shirk the job at hand. I would also like to acknowledge my neighbour, Lee Anderson, who was as emotionally invested in my success, as if it were his own doctorate.

Last, but not least, I would like to thank the support staff in the mathematics department, who helped me in any number of ways, while I was associated with Virginia Tech. I would especially like to thank Hannah Swiger, whose efficiency alleviated a lot of the stress associated with a dissertation defense, and Sandy Blevins, whose cheerful greeting, managed to put me in a good mood, every time I entered the departmental office.

Contents

Chapter 1

Background

1.1 Public Key Cryptography

Cryptology can be loosely defined to be the science concerned with protecting the secrecy of information and the security of communications. It consists of two main branches: *cryptography*, which deals with the design of systems to encrypt (hide or scramble) data, and *cryptanalysis*, which deals with the breaking of such systems. There are several good references on cryptography, some of which include Menezes, van Oorschot and Vanstone [MVoV], Schneier [Sc], Washington and Trappe [WaTr], Buchmann [Bucm] and Koblitz [Ko]. In this section, we provide a brief overview of cryptography with an emphasis on public key cryptosystems.

Encryption schemes, which we call *cryptosystems* have been known since ancient times; in fact, Julius Caesar is believed to have used a simple "shift" cipher, to communicate with his generals. Encryption by the class of shift ciphers, or *Caesar ciphers*, as they are sometimes called, involves shifting each letter of the alphabet by a fixed number of letters. For example, an encryption scheme that maps $a \to c, b \to d, c \to e, \ldots, x \to z, y \to a, z \to b$ involves a shift of two letters. To an adversary who intercepts such an encrypted message during transmission, it appears as a scrambled mess of letters that do not constitute words. On the other hand, the intended recipient is aware of the shift, and can decrypt the message by shifting back the ciphertext by the appropriate number of letters.

In modern times, such shift ciphers provide next to no security, since it is possible for an adversary to use a computer to decrypt a message by trying all possible shifts in very little time. Such an attack (which is called a *brute force attack*) would not only reveal the contents of the message, but also render all communications insecure, since the adversary would gain knowledge of the shift that is used. However, the Caesar cipher has all the basic components of modern cryptosystems. We list these components below:

1. The message space, M, is the set of all possible messages (for example it could consist of all letters of the alphabet).
2. The ciphertext space, C, is the set of all possible encrypted messages
3. The encryption key is the function (or class of functions) that maps messages to ciphertext.
4. The decryption key maps the ciphertext back to the original message.

Modern cryptosystems fall into two basic classes:

1. Private Key or Symmetric Cryptosystems
2. Public Key or Asymmetric Cryptosystems

In symmetric cryptosystems, the encryption and decryption keys are known to both parties (the sender of the message and the receiver), and it is usually easy to determine the decryption key from the encryption key. All classical cryptosystems (that were designed prior to 1970), and some more recent ones such as the *data encryption standard* (DES) and *advanced encryption standard* (AES) are private key systems. One major problem associated with such systems is that of key distribution and key management: before two parties begin regular communications, they need to agree on a key that must be shared via a secure channel or trusted courier, which may be hard to find. The problem becomes even more difficult, if several parties want to exchange encrypted messages. If every pair of users in a communication network consisting of n users, exchanges a key, this involves $n(n-1)/2$ secret key exchanges, and all these keys need to be stored securely.

One way of reducing the number of key exchanges is to use a *key center*, to which every user provides a secret key. If A wants to send a message to B, she encrypts the message using her secret key, and sends it to the key center, where it is decrypted using A's decryption key. It is then encrypted using B's secret key and sent to B. In a communication network consisting of n users, the use of a key center reduces the number of key exchanges to n. However, the key center has access to all secret messages and also must store n secret keys securely.

Public Key cryptosystems, which radically altered the face of cryptography, were first introduced by Diffie and Hellman [DiHe] in 1976. In these systems the encryption key (which is called the *public key*) is published in a public directory, and only the decryption key (called the *private key*) is kept secret. We need the following definitions to formalize these ideas:

Definition 1.1.1: A function, $f : X \to Y$ is said to be a *one-way function* if it is easy to compute $f(x)$ for any $x \in X$, but hard (computationally infeasible) to compute $f^{-1}(y)$ for almost all randomly selected y in the range of f.

We do not formally define the term *computationally infeasible*, but generally we say that a problem is computationally infeasible, if the time and computational resources required to solve it by the best currently known methods exceeds, by a comfortable margin, the resources of an entity trying to solve it.

Definition 1.1.2: A *trapdoor function* is a one-to-one one-way function, $f : X \to Y$, together with some additional information (called *trapdoor information*), which makes it feasible to compute $f^{-1}(y)$ for any given y in the range of f.

Using this terminology, the encryption key of a public key cryptosystem consists of a one-to-one one-way function with a trapdoor. The one-way function is published in a public directory, while the trapdoor information, which forms the decryption key, is kept secret. Thus the one-way function is the public key and the trapdoor information is the private key. If B wants to send an encrypted message to A, he looks up her published public key, and uses it to encrypt the message. When A receives an encrypted message, she decrypts it using her private key (which she and only she knows). There is no need for a secure channel to exchange keys in advance, nor a trusted key center, which has access to all secret messages.

Despite the problem of key management, symmetric cryptosystems served the purpose of military and diplomatic communications fairly well. However, public key cryptosystems have grown in significance with the increase in electronic communications and e-commerce, and the need for greater information and data security. This growth in public key cryptography has led to a dramatic expansion of the role of algebra and number theory in cryptography, since these branches of mathematics seem to provide the best source of one-way functions. In fact, the most widely-used public key cryptosystems, such as RSA and DSA are based on problems in number theory. Generally speaking, the design of a public key cryptosystem consists of a large class of one-to-one one-way functions with trapdoors. Each user generates a function from the family, in such a way that only he/she knows the trapdoor. In RSA, which is based on the computational infeasibility of factoring large integers, this family of functions is $f(x) = x^e (\mathrm{mod}\ n)$, for appropriate values of n and e. A trapdoor is built into the function, by constructing n from carefully selected prime factors.

The class of public key cryptosystems may be further subdivided into two classes based on the type of encryption. Most number theory based cryptosystems, (including RSA and DSA) are *deterministic* in nature. i.e. a given plaintext message will always be encrypted into the same ciphertext. Deterministic encryption systems have one major disadvantage: in the case where the message space is relatively small (e.g. the message is just "yes" or "no"), an adversary can simply encrypt all possible messages, and thus have an explicit map from the message space to the ciphertext space. The adversary would then be able to gain complete knowledge of all intercepted messages. In addition, it appears to be very difficult to prove anything about deterministic encryption systems. This and

other perceived disadvantages of deterministic encryption prompted Goldwasser and Micali [GoMi1], [GoMi2] to introduce *probabilistic* encryption in 1982. The *Polly Cracker* cryptosystem, which was proposed by M. Fellows and N. Koblitz [FeKo] in 1993, is an example of a probabilistic encryption system. Koblitz and Fellows' version of the Polly Cracker cryptosystem, as well as its noncommutative analog (which is the main focus of this work) are presented in chapter 2. We now present some background information on *Gröbner bases*, which form the theoretical basis for these cryptosystems.

1.2 Commutative Gröbner Bases

Gröbner bases provide a powerful computational tool that can be used to solve some fundamental problems of commutative algebra and have received much attention in the past two decades, paralleling the growth in computational power. Despite advances in both, Gröbner basis theory and computational technology, the solution to a number of these problems remains largely intractable, chiefly due to the tremendous resources required to compute Gröbner basis. In this section, we provide some background information on commutative Gröbner bases. There are several good references for this material, some of which include Adams and Loustaunau [AdLo], Cox, Little and O'Shea [CLOs] and Becker and Weispfenning [BeWe]. We refer the reader to these works for the proofs of the results that we present here.

1.2.1 Term orders and commutative Gröbner bases:

Let K be any field, and $R = K[x_1, x_2, \ldots, x_n]$ be the set of all commutative polynomials with coefficients in the field, K. i.e. the elements of R are finite sums of terms of the form $a \cdot x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n}$, where $a \in K$ and $\beta_i \in \mathbb{N}$, $i = 1, 2, \ldots, n$. (Note that we use the symbol $\mathbb{N}$ to denote the set of non-negative integers, $\{0, 1, 2, \ldots\}$.) We note that R is a commutative ring with respect to the usual operations of addition and multiplication of polynomials. R is also a K-vector space with basis $T^n = \{x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n} : \beta_i \in \mathbb{N},\ i = 1, 2, \ldots, n\}$. The elements of T^n are called *power products*. We will use the notation $\boldsymbol{x}^{\beta}$ to denote the power product $x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n}$.

A subset I, of R is called an *ideal* of R, if it is closed under addition, and $f \cdot g \in I$ for all $f \in R$ and all $g \in I$. If F is an arbitrary subset of R, then the ideal generated by F, denoted $\langle F \rangle$, is the smallest ideal of R that contains F. F is called a generating set for $\langle F \rangle$. If F is a finite set, say $F = \{f_1, f_2, \ldots, f_s\}$ then $\langle F \rangle$ is given by:

$$\langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} u_i f_i : u_i \in R,\ i = 1, 2, \ldots, s \right\}.$$

A well-ordering, $<$, on the set T^n of power products is a *term order* if it satisfies the following conditions:

1. Given any $\boldsymbol{x}^\alpha$, $\boldsymbol{x}^\beta \in T^n$, exactly one of the relations $\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta$, $\boldsymbol{x}^\alpha = \boldsymbol{x}^\beta$ or $\boldsymbol{x}^\alpha > \boldsymbol{x}^\beta$ holds. i.e. $<$ is a total order;
2. $1 < \boldsymbol{x}^\beta$ for all $\boldsymbol{x}^\beta \neq 1$ and
3. If $\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta$ then $\boldsymbol{x}^\alpha\ \boldsymbol{x}^\gamma < \boldsymbol{x}^\beta\ \boldsymbol{x}^\gamma$ for all $\boldsymbol{x}^\gamma \in T^n$.

Before presenting examples, we note the following property of term orders, which is clear from the definition:

Proposition 1.2.1.1: For $\boldsymbol{x}^\alpha$, $\boldsymbol{x}^\beta \in T^n$, if $\boldsymbol{x}^\alpha$ divides $\boldsymbol{x}^\beta$, then $\boldsymbol{x}^\alpha \leq \boldsymbol{x}^\beta$.

Example 1.2.1.2: The (left) lexicographic order:

Order the variables $x_1, x_2, \ldots, x_n$ arbitrarily, say $x_1 > x_2 > \cdots > x_n$. For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$ we define $\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta$ if and only if the first coordinates in α and β (from the left), which are different, satisfy $\alpha_i < \beta_i$.

Example 1.2.1.3: The degree-lexicographic order:

Order the variables $x_1, x_2, \ldots, x_n$ arbitrarily, say $x_1 > x_2 > \cdots > x_n$. For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, we define $\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta$ if and only if

(i). $\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i$, or

(ii). if $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ and $\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta$ in the (left) lexicographic order.

Example 1.2.1.4: The degree-reverse-lexicographic order:

Order the variables $x_1, x_2, \ldots, x_n$ arbitrarily, say $x_1 > x_2 > \cdots > x_n$. For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, we define $\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta$ if and only if

(i). $\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i$, or

(ii). if $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ and the first coordinates of α and β from the right, which are different, satisfy $\alpha_i > \beta_i$.

Before defining Gröbner bases, we need the following:

Definition 1.2.1.5: Let $>$ be a term order on $R = K[x_1, x_2, \ldots, x_n]$. Let $f \in R$ and $f = a_1\boldsymbol{x}^{\alpha_1} + a_2\boldsymbol{x}^{\alpha_2} + \cdots + a_r\boldsymbol{x}^{\alpha_r}$, where $a_i \neq 0$ and $\boldsymbol{x}^{\alpha_1} > \boldsymbol{x}^{\alpha_2} > \cdots > \boldsymbol{x}^{\alpha_r}$. We define the *leading power product of* f to be $lp(f) = \boldsymbol{x}^{\alpha_1}$, the *leading coefficient of* f to be $lc(f) = a_1$ and the *leading term of* f to be $lt(f) = a_1\ \boldsymbol{x}^{\alpha_1} = lc(f) \cdot lp(f)$.

For a subset S of $K[x_1, x_2, \ldots, x_n]$, we define the *leading term ideal* of S to be the ideal $Lt(S) = \langle lt(s) : s \in S \rangle$.

We are now ready to define Gröbner bases:

Definition 1.2.1.6: Let I be an ideal in $R = K[x_1, x_2, \ldots, x_n]$. A set of non-zero polynomials, $G = \{g_1, g_2, \ldots, g_t\}$ contained in I is called a *Gröbner basis* for I if and only if, for all $f \in I, f \neq 0$, there exists $i \in \{1, 2, \ldots, t\}$ such that $lp(g_i)$ divides $lp(f)$. Equivalently, G is a Gröbner basis for I if and only if $Lt(G) = Lt(I)$.

We will present additional characterizations of Gröbner bases after presenting the multivariable division algorithm. We end this section with the following:

Remark: If G is a Gröbner basis for I, then it is a generating set for I.

1.2.2 The division algorithm:

In this section, we study a division algorithm in $R = K[x_1, x_2, \ldots, x_n]$ and its relationship to Gröbner bases and the ideal membership problem. The basic idea behind the algorithm is the same as in the one variable case or elementary long division that is studied in grade school i.e. given a set $F = \{f_1, f_2, \ldots, f_s\} \subset R$, and $f \in R$, we want to cancel terms of f using the terms of the f_i's, so that the new terms introduced are smaller than the cancelled terms, and continue this process until it cannot be performed any more.

We begin by looking at the special case of division of f by g, where $f, g \in R$. We fix a term order on R.

Definition 1.2.2.1: Given $f, g, h \in R$,with $g \neq 0$, we say that f *reduces to* h *modulo* g *in one step*, denoted $f \xrightarrow{g} h$, if and only if $lp(g)$ divides a non-zero term X that appears in f, and $h = f - \frac{X}{lt(g)}g$.

If $F = \{f_1, f_2, \ldots, f_s\}$ is a set of non-zero polynomials in R, we say that f *reduces to* h *modulo* F, denoted $f \xrightarrow{F}_+ h$, if and only if there exists a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, s\}$ and a sequence of polynomials $h_{i_1}, h_{i_2}, \ldots, h_{t-1}$ in R, such that $f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} \ldots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$.

A polynomial r is said to be *reduced* with respect to a set of non-zero polynomials $F = \{f_1, f_2, \ldots, f_s\}$, if r cannot be reduced modulo F.

If $f \xrightarrow{F}_+ r$, and r is reduced with respect to F, then we call r a remainder for f with respect to F.

We are now ready to present the division algorithm in pseudocode.

Algorithm 1.2.2.2:

INPUT: $f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ (ordered), with $f_i \neq 0,\ (1 \leq i \leq s)$.

OUTPUT: $u_1, u_2, \ldots, u_s, r$ such that $f = u_1 f_1 + \ldots u_s f_s + r$ and

r is reduced with respect to $\{f_1, f_2, \ldots, f_s\}$, and

$\max(lp(u_1) \cdot lp(f_1)), lp(u_2) \cdot lp(f_2), \ldots, lp(u_s) \cdot lp(f_s), lp(r)) = lp(f)$.

INITIALIZE: $u_1 := 0, u_2 := 0, \ldots, u_s := 0, r := 0, h := f$

WHILE $h \neq 0$ DO

IF there exists i such that $lp(f_i)$ divides $lp(h)$, THEN

choose i least, such that $lp(f_i)$ divides $lp(h)$

$u_i := u_i + \dfrac{lt(h)}{lt(f_i)}$

$h := h - \dfrac{lt(h)}{lt(f_i)} \cdot f_i$

ELSE

$r := r + lt(h)$

$h := h - lt(h)$

DONE

Remark: The order on the set $F = \{f_1, f_2, \ldots, f_k\}$ affects the outcome of the division algorithm.

Example 1.2.2.3: Let K be any field, and $R = K[x, y]$. Let $>$ be the degree-lexicographic order on R, with $y > x$. Let $f = y^2x - x$, $f_1 = y^2 - x$ and $f_2 = yx - x$. Then $lp(f) = y^2x$, $lp(f_1) = y^2$ and $lp(f_2) = yx$.

Now, $y^2x = lp(f_1) \cdot x$. Therefore, if we divide first by f_1, we get the remainder $(y^2x - x) - x(f_1) = x^2 - x$. Since neither $lp(f_1)$ nor $lp(f_2)$ divides $lp(x^2 - x) = x^2$, the algorithm terminates and we have $r = x^2 - x$. i.e. $f = y^2x - x = x(f_1) + (x^2 - x)$.

On the other hand, since $y^2x = y \cdot lp(f_2)$ we could divide by f_2 first. If we do, we get the remainder $f = y^2x - x = y(f_2) + (yx - x)$. Dividing by f_2 once again, we get $yx - x = 1 \cdot f_2 + 0$ i.e. the remainder of the division is zero and the algorithm terminates with $r = 0$. i.e. $f = y^2x - x = (y + 1)f_2$.

The next result provides the additional characterizations of Gröbner bases, which we promised earlier:

Theorem 1.2.2.4: Let I be a nonzero ideal of $R = K[x_1, x_2, \ldots, x_n]$. Let $G = \{g_1, g_2, \ldots, g_t\}$ be a set of nonzero polynomials in I. The following statements are equivalent:

(i). G is a Gröbner basis for I.

(ii). $f \in I$ if and only if $f \xrightarrow{G}_{+} 0$.

(iii). $f \in I$ if and only if $f = \sum_{i=1}^{t} h_i g_i$ with $lp(f) = \max_{1 \leq i \leq t}(lp(h_i) \cdot lp(g_i))$.

(iv.) For any $f \in R$, the remainder of the division of f by G is unique.

We note that in view of part (iv) of theorem 1.2.2.4, the remainder of the division of a polynomial, f, by a Gröbner basis, G is sometimes called the normal form of f, denoted $N_G(f)$. We also note that theorem 1.2.2.4 has tremendous significance since parts (ii) and (iv) of the theorem in effect, provide a method for solving the ideal membership problem i.e. given an ideal I in R and $f \in R$, we can determine whether $f \in I$ as follows:

1. Find a Gröbner basis, G for I.
2. Divide f by G. If the remainder of the division is zero, then $f \in I$, else $f \notin I$.

1.2.3 S-polynomials, the construction of Gröbner bases and uniqueness:

We are now ready to present some ideas that form the theoretical foundation of the algorithm to construct Gröbner bases. We begin with the following definition:

Definition 1.2.3.1: Let $0 \neq f, g \in R = K[x_1, x_2, \ldots, x_n]$. Let $L = \text{lcm}(lp(f), lp(g))$. The polynomial $S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$ is called the S-polynomial of f and g.

Example 1.2.3.2: Let $\mathbb{Z}_3$ be the set of residue classes of the integers modulo 3. Then $\mathbb{Z}_3$ is a field with the usual operations of addition and multiplication. Let $f = yx - y$ and $g = y^2 - x \in \mathbb{Z}_3[x, y]$. Let $>$ be the degree-lexicographic order with $y > x$. Then $L = y^2$ and $S(f, g) = \frac{y^2 x}{yx} f - \frac{y^2 x}{y^2} = yf - xg = -y^2 + x^2$.

We note that $lp(yf) = y^2 x = lp(xg)$ is cancelled out in $S(f, g)$. We also note that there is another way of looking at S-polynomials: In the division of f by $f_1, f_2, \ldots, f_s$, it may happen, that some term, X, appearing in F is divisible by both f_i and f_j for $i \neq j$. If we reduce f by f_i, we get $h_1 = f - \frac{X}{lt(f_i)}$. If we reduce f by f_j, we get $h_2 = f - \frac{X}{lt(f_j)}$. The ambiguity that is introduced is $h_2 - h_1 = \frac{X}{L} S(f_i, f_j)$, where $L = \text{lcm}(lp(f), lp(g))$. These are precisely the kinds of ambiguities that must not occur in Gröbner bases. In fact, we have the following:

Theorem 1.2.3.3: (Buchberger). Let $G = \{g_1, g_2, \ldots, g_t\}$ be a set of non-zero polynomials in $R = K[x_1, x_2, \ldots, x_n]$. Then, G is a Gröbner basis for the ideal $I = \langle g_1, g_2, \ldots, g_t \rangle$ if and only if for all $i \neq j$, $S(f_i, f_j) \xrightarrow{G}_+ 0$.

We are now ready to give Buchberger's algorithm for constructing Gröbner bases.

Algorithm 1.2.3.4:

INPUT: $F = \{f_1, f_2, \ldots, f_s\} \subset K[x_1, x_2, \ldots, x_n]$ with $f_i \neq 0$ $(1 \leq i \leq s)$

OUTPUT: $G = \{g_1, g_2, \ldots g_t\}$, a Gröbner basis for $\langle f_1, f_2, \ldots, f_s \rangle$

INITIALIZE: $G := F,\ H := \{\{f_i, f_j\} : f_i \neq f_j \in G\}$

WHILE $(H \neq)$ DO

Choose any $\{f, g\} \in H$

$H := G - \{\{f, g\}$

$S(f, g) \xrightarrow{G}_+ h$, where h is reduced with respect to G

IF $h \neq 0$ DO

$H := H \cup \{\{u, h\} : u \in G\}$

$G := G \cup \{h\}$

DONE

DONE

Theorem 1.2.3.5: Let $R = K[x_1, x_2, \ldots, x_n]$ be a polynomial ring over a field, K. Let $F = \{f_1, f_2, \ldots, f_s\}$ be a set of non-zero polynomials in R. Then Buchberger's algorithm (algorithm 1.2.3.4) produces a Gröbner basis for the ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$.

Although we have not explicitly stated it, we note that the above theorem implies that every ideal I of $R = K[x_1, x_2, \ldots, x_n]$ has a finite Gröbner basis. We note, however, that the Gröbner basis is not unique, and even if we use the same term order, an ideal can have an infinite number of Gröbner bases. Buchberger overcame this difficulty by introducing the idea of *reduced Gröbner bases*.

Definition 1.2.3.6: A Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ is said to be *reduced* if, for all $i \in \{1, 2, \ldots, t\}$, $lc(g_i) = 1$ and g_i is reduced with respect to $G - \{g_i\}$. i.e. for all i, no non-zero term in g_i is divisible by any $lp(g_j)$ for any $j \neq i$.

We end this section with the following:

Theorem 1.2.3.7: (Buchberger). Fix a term order on $R = K[x_1, x_2, \ldots, x_n]$. Then every non-zero ideal I in R has a unique reduced Gröbner basis with respect to this term order.

1.3 Noncommutative Gröbner Bases

In this section, we present some background information on noncommutative Gröbner bases. Most of what we present here is analogous to the commutative case, which we presented in section 1.2. However one significant difference is that unlike the commutative case, most ideals of noncommutative algebras do not have finite Gröbner bases. In fact, it is precisely this property of noncommutative Gröbner bases that prompted us to study the noncommutative Polly Cracker cryptosystem.

Although most of the results that we present here hold for a wider class of noncommutative algebras over any field, we will assume, throughout this section that K is a finite field and $R = K\langle x_1, x_2, \ldots, x_n \rangle$ is the free algebra over K in n non-commuting variables. A more thorough treatment of this material is presented in E. Green [Gr1] and F. Mora [MF]. We refer the reader to these articles for most of the proofs. E. Green [Gr1] is also a good reference for the generalization of this material to path algebras.

1.3.1 Monomial orders and noncommutative Gröbner bases:

Let $R = K\langle x_1, x_2, \ldots, x_n \rangle$ be the free associative algebra in n non-commuting variables, over a finite field K. A subset, I, of R is said to be a *two-sided ideal* of R if it is closed under addition and for all $g \in I$, and all $f, h \in R$, $f \cdot g \cdot h \in I$.

If X is an arbitrary subset of R, then the ideal generated by X, denoted $\langle X \rangle$, is the smallest ideal of R that contains X. Equivalently, X consists of all finite sums of the form $\sum f \cdot g \cdot h$, where $f, h \in R$ and $g \in X$.

By a *monomial*, we mean a (finite) noncommutative word in the alphabet $\{x_1, x_2, \ldots, x_n\}$. We use the letter B to denote the set of monomials. We note that if $f \in R$, then $f = \sum \alpha_i b_i$, where $\alpha_i \in K$ with only finitely many $\alpha_i \neq 0$, and $b_i \in B$.

We define multiplication in the set B of monomials by concatenation.
i.e. if $b_1 = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_r}$ and $b_2 = x_{\beta_1} x_{\beta_2} \ldots x_{\beta_s}$, then $b_1 \cdot b_2 = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_r} x_{\beta_1} x_{\beta_2} \ldots x_{\beta_s}$. The set B of monomials in $\{x_1, x_2, \ldots, x_n\}$ is a multiplicative basis of R. i.e. B is a K-basis of R and $b, b' \in B$ implies that $b \cdot b' \in B$. We say that an ideal, I in R, is a *monomial ideal*, if it can be generated by elements of B.

A well-order $>$ on B is said to be *admissible* if it satisfies the following conditions for all $p, q, r, s \in B$:

1. if $p < q$ then $pr < qr$
2. if $p < q$ then $sp < sq$ and
3. if $p = qr$ then $p > q$ and $p > r$.

We present a few examples of common orders:

Example 1.3.1.1: The (left) length-lexicographic order:

Order the variables $x_1, x_2, \ldots, x_n$ arbitrarily, say, $x_1 < x_2 < \cdots < x_n$. Let $p, q \in B$, and let $l(p)$ denote the length of p. i.e. if $p = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_r}$, then $l(p) = r$. We define $p < q$

(i). if $l(p) < l(q)$ or

(ii). if $l(p) = l(q)$, say $p = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_r}$ and $q = x_{\beta_1} x_{\beta_2} \ldots x_{\beta_r}$ and for some i, where $1 \leq i \leq r$, $x_{\alpha_j} = x_{\beta_j}$ for $j < i$ and $x_{\alpha_i} < x_{\beta_i}$.

The right length-lexicographic order is defined similarly.

Example 1.3.1.2: The (left) weight-lexicographic (or degree-lexicographic) order:

Let $w : \{x_1, x_2, \ldots, x_n\} \to \mathbb{N}$ be a set map. Let $W : B \to \mathbb{N}$ be the natural extension of w. i.e. if $p = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_r}$, then $W(p) = \sum_{i=1}^{r} w(x_{\alpha_i})$. Define $p < q$

(i). if $W(p) < W(q)$, or

(ii). if $W(p) = W(q)$ then use the left-lexicographic order.

The right weight-lexicographic order is defined similarly.

Remarks:

1. The left length-lexicographic order is a special case of the (left) weight-lexicographic order, with $w(x_i) = 1$ for all $i = 1, 2, \ldots, n$.
2. The (left) lexicographic order is **not** admissible.
   This is clear since $x_2 > x_1 > x_1x_2 > x_1x_1x_2 > x_1x_1x_1x_2 > \ldots$ forms an infinite descending chain under this order. Hence, the (left) lexicographic order is not a well-order. This is different from the commutative case.

Example 1.3.1.3: The (left) weight-reverse-lex or degree-reverse-lex order:

Let $w : \{x_1, x_2, \ldots, x_n\} \to \mathbb{N}$ be a set map. Let $W : B \to \mathbb{N}$ be the natural extension of w. i.e. if $p = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_r}$, then $W(p) = \sum_{i=1}^{r} w(x_{\alpha_i})$. Define $p < q$

(i). if $W(p) < W(q)$, or

(ii). if $W(p) = W(q)$ then use the right-lexicographic order.

Example 1.3.1.4: Commutative orders:

Let $x_1 < x_2 < \cdots < x_n$ be an arbitrary order and let $<_c$ be a term order on the commutative words in $\{x_1, x_2, \ldots, x_n\}$. For any noncommutative monomial p in $\{x_1, x_2, \ldots, x_n\}$,

let $\overline{p}$ be the word obtained by treating p as a commutative word. Define $p < q$

(i). if $\overline{p} <_c \overline{q}$ or,

(ii). if $\overline{p} =_c \overline{q}$ and $p < q$ in the (left) lexicographic order.

Example 1.3.1.5: The total lexicographic order:

This is a special case of a commutative order (see example 1.3.4, above), in which $<_c$ is the (left) lexicographic order.

Before defining noncommutative Gröbner bases, we need the following:

Definition 1.3.1.6 Let K be a field, and $R = K\langle x_1, x_2, \ldots, x_n\rangle$, the noncommutative free algebra over K. Let $>$ be an admissible order on the monomials and $f \in R$. We say that a monomial b_i *occurs* in f if the coefficient of b_i in $f = \sum \gamma_j b_j$ is not zero.

We say that b_i is the *tip* of f, denoted $\mathrm{tip}(f)$, if b_i occurs in f and $b_i \geq b_j$ for all b_j occurring in f. We denote the coefficient of $\mathrm{tip}(f)$ by $\mathrm{Ctip}(f)$.

If $X \subseteq R$, then we write $\mathrm{Tip(X)} = \{b \in B : b = \mathrm{tip}(f) \text{ for some nonzero } f \in X\}$ and $\mathrm{NonTip}(X) = B - \mathrm{Tip}(X)$.

Remark: $\mathrm{Tip}(X)$ and $\mathrm{NonTip}(X)$ depend on the order $>$.

We are now ready to give the following:

Definition 1.3.1.7: Let $>$ be an admissible order on $R = K\langle x_1, x_2, \ldots, x_n\rangle$. Let I be a two-sided ideal of R. We say that $G \subset I$ is a *Gröbner basis* for I with respect to $>$ if $\langle \mathrm{Tip}(G)\rangle = \langle \mathrm{Tip}(I)\rangle$. Equivalently, $G \subset I$ is a Gröbner basis of I if for every $b \in \mathrm{Tip}(I)$, there is some $g \in G$ such that $\mathrm{tip}(g)$ divides b i.e. for every $f \in I$, there exists $g \in G$, and $p, q \in B$ such that $p \cdot \mathrm{tip}(g) \cdot q = \mathrm{tip}(f)$.

Remark: $\mathrm{tip}(f)$ is the noncommutative analog of the leading power product of a polynomial and $\langle \mathrm{Tip}(G)\rangle$ is the analog of the leading term ideal of a set.

Next we note that for any ideal I, of $K\langle x_1, x_2, \ldots, x_n\rangle$, $R = I \oplus \mathrm{Span}(\mathrm{NonTip}(I))$, as vector spaces. In particular, every nonzero $r \in R$ can be written uniquely as $r = i_r + N(r)$, where $i_r \in I$ and $N(r) \in \mathrm{Span}(\mathrm{NonTip}(I))$. $N(r)$ is called the normal form of r. We will use this fact in the definition of reduced Gröbner bases.

1.3.2 Reduced Gröbner bases

We now turn our attention to the definition of reduced (noncommutative) Gröbner bases. Although the definition we give here, differs from the one we gave in the commutative case, we note that reduced Gröbner basis play the same role (that of uniqueness) in noncommutative Gröbner basis theory as they do in the commutative theory.

Before giving the definition, we need the following:

Proposition 1.3.2.1: Let K be a finite field, $R = K\langle x_1, x_2, \ldots, x_n \rangle$, the noncommutative free algebra over K in n variables. If I is a monomial ideal of R, then I has a minimal monomial generating set. That is, there is a unique set of generators of I, none of which can be omitted and still generate I.

Rather than providing a proof of this result, we refer the reader to E. Green [Gr1], in which it is proved in a more generalized setting. Instead, we focus on its consequences, as applied to Gröbner bases and reduced Gröbner bases over noncommutative free algebras.

We note that the minimal monomial generating set guaranteed by proposition 1.3.2.1 need not be finite. This differs from the commutative case, in which Dickson's lemma [Di] proves that every monomial ideal of a commutative ring can be generated by a finite number of monomials.

We are now ready to give the following:

Definition 1.3.2.2: Let K be a finite field, $R = K\langle x_1, x_2, \ldots, x_n \rangle$ and suppose $>$ is an admissible order. Let I be an ideal in R, and let I_{MON} be the ideal generated by $\mathrm{Tip}(I)$, under $>$. Let T be the unique minimal monomial generating set of I_{MON}. Then, the *reduced Gröbner basis* for I, with respect to $>$ is $G = \{t - N(t) : t \in T\}$.

Remark: The following properties of a reduced Gröbner basis are easy to see:

1. G is a Gröbner basis for I.
2. If $g \in G$ then the coefficient of $\mathrm{tip}(g)$ is 1.
3. $g \in G$ then $g - \mathrm{tip}(g) \in \mathrm{Span}(\mathrm{NonTip}(I))$.
4. $\mathrm{Tip}(G)$ is the minimal monomial generating set for I_{MON}.

1.3.3 The noncommutative division algorithm:

Before giving an algorithm to construct noncommutative Gröbner bases, we present a noncommutative division algorithm. i.e. given an ordered set, $F = \{f_1, f_2, \ldots, f_k\}$ of $R = K\langle x_1, x_2, \ldots, x_n\rangle$, and $g \in R$, we show how to divide g by F. i.e. we find non-negative integers $t_1, t_2, \ldots, t_k$ and elements $u_{ij}, v_{ij}, r \in R$, for $1 \leq i \leq k$ and $1 \leq j \leq t_i$ such that:

1. $g = \sum_{i=1}^{k} \sum_{j=1}^{t_i} u_{ij} f_i v_{ij} + r$
2. $\text{tip}(g) \geq \text{tip}(u_{ij} f_i v_{ij})$ for all i and j.
3. tip (f_i) does not divide any monomial that occurs in r, for $1 \leq i \leq k$.

Note that if $r \neq 0$, then $\text{tip}(r) \leq \text{tip}(g)$; r is the remainder of the division.

Algorithm 1.3.3.1:

INPUT: $f_1, f_2, \ldots, f_k$ (ordered), y

OUTPUT: $t_1, t_2, \ldots, t_k, u_{ij}, v_{ij}, r$

INITIALIZE: $t_1 := 0, t_2 := 0, \ldots, t_k := 0, r := 0, h := g$, DIVOCCUR $:= false$

WHILE ($h \neq 0$ and DIVOCCUR $==$ $false$) DO

  FOR ($i = 1$) TO k DO

    IF $\text{tip}(h) = u \cdot \text{tip}(f_i) \cdot v$ for $u, v \in B$, THEN

      $t_i := t_{i+1}$

      $u_{it_i} := [\text{Ctip}(h)/\text{Ctip}(f_i)] \cdot u$

      $v_{it_i} := v$

      $h := h - [\text{Ctip}(h)/\text{Ctip}(f_i)] \cdot u \cdot f_i \cdot v$

      DIVOCCUR $:= true$

    ELSE $i := i + 1$

  IF DIVOCCUR $==$ $false$ THEN

    $r := r + \text{Ctip}(h) \cdot \text{tip}(h)$

    $h := h - \text{Ctip}(h) \cdot \text{tip}(h)$

    DONE

  DONE

DONE

Remark: As in the commutative case, the order on the set $F = \{f_1, f_2, \ldots, f_k\}$ affects the outcome of the division algorithm.

Example 1.3.3.2: Let $R = K\langle x, y, z\rangle$ be the noncommutative free algebra over a finite field K and $>$ be the (left) length-lexicographic order on the monomials, with $x > y > z$. Let $g = zxxyx$, $f_1 = xy - x$ and $f_2 = xx - xz$. Then $\mathrm{tip}(f_1) = xy$ and $\mathrm{tip}(f_2) = xx$.

Now, $zxxyx = (zx) \cdot \mathrm{tip}(f_1) \cdot x$. Therefore, dividing by f_1 first yields the remainder $zxxyx - zx(f_1)x = zxxx$. Next, since $\mathrm{tip}(f_1)$ does not divide $zxxx$, we divide by f_2. Now, $zxxx = z \cdot \mathrm{tip}(f_2) \cdot x$, and dividing by f_2 yields the remainder $zxxx - z(f_2)x = zxzx$. Since neither $\mathrm{tip}(f_1)$ nor $\mathrm{tip}(f_2)$ divides $zxzx$, the algorithm terminates and we have $r = zxzx$. i.e. $g = zxxyx = zx(f_1)x + z(f_2)x + zxzx$.

If, on the other hand, we divide by f_2 first, we get $g = zxxyx = z(f_2)yx + zxzyx$. Since neither $\mathrm{tip}(f_1)$ nor $\mathrm{tip}(f_2)$ divides $zxzyx$, the algorithm terminates and we have $r = zxzyx$. i.e. $g = zxxyx = z(f_2)yx + zxzyx$.

Definition 1.3.3.3: If $F = \{f_1, f_2, \ldots, f_k\}$ is an ordered subset of R, and $g \in R$, is divided by F, we denote the remainder, r, of the division by $g \to_F r$.

Next, we note that if $F = \{f_1, f_2, \ldots\}$ is an infinite set with $\mathrm{tip(f_1)} \leq \mathrm{tip(f_2)} \leq \ \ldots$ and only a finite number of f_i's have any given tip, then only a finite number of f_i's are required to perform division by F. This follows from the fact that given any $g \in R$, there can only be a finite number of f_i's such that $\mathrm{tip}(f_i) \leq \mathrm{tip}(g)$, say $f_1, f_2, \ldots, f_k$. It is clear that $f_{k+1}, f_{k+2}, \ldots$ would never play a role in the division algorithm (when dividing g by F), so that the division of g by F is in fact equivalent to the division of g by $\{f_1, f_2, \ldots, f_k\}$. In fact, we have the following:

Proposition 1.3.3.4: Let G be the Gröbner basis of an ideal I in $R = K\langle x_1, x_2, \ldots, x_n\rangle$. Let $f \in R$ be arbitrary. Let $F = \{g_1, g_2, \ldots, g_k\} = \{g \in G : \mathrm{tip}(g) \leq \mathrm{tip}(f)\}$. If f reduces to r modulo F (i.e. r is the remainder of the division of f by F), then r is independent of the order of $g_1, g_2, \ldots, g_k$ in F. In fact, $r = N(f)$.

1.3.4 Overlap relations and the construction of Gröbner bases:

We are now ready to present some ideas that lead to the algorithm for the construction of noncommutative Gröbner bases. Note that we use the term *algorithm* loosely here, in the sense that the procedure we present does not necessarily terminate in a finite number of steps. In fact, it terminates if and only if the ideal has a finite Gröbner basis. Furthermore, if t is a tip in a minimal generating set of $\langle \mathrm{Tip}(I)\rangle$, then t occurs as the tip of some g produced by the algorithm in a finite number of steps.

Definition 1.3.4.1: Let $f, g \in R = K\langle x_1, x_2, \ldots, x_n \rangle$, and suppose that b, c are monomials such that:

1. $\text{tip}(f) \cdot c = b \cdot \text{tip}(g)$ and
2. $\text{tip}(f)$ does not divide b and $\text{tip}(g)$ does not divide c.

Then the *overlap relation* of f and g by b, c is

$$O(f, g, b, c) = \frac{1}{\text{Ctip}(f)} \cdot f \cdot c - \frac{1}{\text{Ctip}(g)} \cdot b \cdot g.$$

Remarks:

1. $\text{tip}(O(f, g, b, c)) < \text{tip}(f) \cdot c = b \cdot \text{tip}(g)$.
2. Overlap relations are the noncommutative version of the S-polynomials that are found in commutative Gröbner basis theory.

Example 1.3.4.2: Let $g = xyx - xy \in K\langle x, y \rangle$, where K is a finite field. If we use the length-lexicographic order with $x > y$, then $\text{tip}(g) = xyx$, and g contains the self-overlap $O(g, g, yx, xy) = g \cdot yx - xy \cdot g = xyxy - xyyx$.

Example 1.3.4.3: Let K be a finite field and $K\langle x, y, z \rangle$ be the free algebra over K, in three non-commuting variables. Let $f = xzy + yz,\ g = yzx + zy \in K\langle x, y, z \rangle$. If we use the length-lexicographic order with $x > y > z$, then $\text{tip}(f) = xzy$ and $\text{tip}(g) = yzx$, and we have the overlap relations:

1. $O(f, g, zx, xz) = f \cdot zx - xz \cdot g = yzzx - xzzy$ and
2. $O(g, f, zy, yz) = g \cdot zy - yz \cdot f = -yzyz + zyzy$.

Remark: As seen in the above examples, the noncommutative case differs from the commutative one in that each pair of polynomials may contain more than one overlap. In addition, the noncommutative case includes self-overlaps, which must be considered in the algorithm for constructing of Gröbner bases. In the commutative case, we only need to use the least common multiple of the leading monomials.

Before giving the termination theorem, we need the following definition:

Definition 1.3.4.4: Let K be a finite field and let $K\langle x_1, x_2, \ldots, x_n \rangle$ be the free algebra over K in n non-commuting variables. We say that a set $X \subset K\langle x_1, x_2, \ldots, x_n \rangle$ is *tip-reduced* if for distinct elements, $f, g \in X$, $\text{tip}(f)$ does not divide $\text{tip}(g)$.

We are now ready to state the termination theorem, which is a version of G. Bergman's Diamond Lemma [Berg]:

Theorem 1.3.4.5: Let K be a finite field and let $K\langle x_1, x_2, \ldots, x_n\rangle$ be the free algebra over K in n non-commuting variables. Let B be the set of monomials in the alphabet $\{x_1, x_2, \ldots, x_n\}$ and let $>$ be an admissible order on B. Suppose G is a set of tip-reduced elements of $K\langle x_1, x_2, \ldots, x_n\rangle$ such that every overlap relation $O(g_1, g_2, p, q)$ with $g_1, g_2 \in G$ reduces to zero over G i.e. for every pair of polynomials, $g_1, g_2 \in G$ and every overlap of p, q of g_1 with g_2, $O(g_1, g_2, p, q) \rightarrow_G 0$. Then G is a Gröbner basis for $\langle G\rangle$.

Finally, we present noncommutative analog of Buchberger's algorithm [Bucb2] for constructing Gröbner bases. Given $f_1, f_2, \ldots, f_k \in K\langle x_1, x_2, \ldots, x_n\rangle$, let $I = \langle f_1, f_2, \ldots, f_k\rangle$. The algorithm produces a (possibly infinite) sequence of elements $g_1, g_2, \ldots$, where $g_i = f_i$ for $1 \leq i \leq k$, and for $i > k$, $g_i \in I$ such that $\mathrm{tip}(g_i) \notin \langle \mathrm{tip}(g_1), \mathrm{tip}(g_2), \ldots, \mathrm{tip}(g_{i-1})\rangle$. It can be shown that $\{g_1, g_2, \ldots, g_k, g_{k+1}, \ldots\}$ is in fact a Gröbner basis of I. We present the algorithm in pseudocode:

Algorithm 1.3.4.6:

INPUT: $f_1, f_2, \ldots, f_k$
OUTPUT: $g_1, g_2, g_3 \ldots$
FOR $(i = 1)$ TO k DO
  $g_i := f_i$
  $G = \{g_1, g_2, \ldots, g_k\}$
  count $:= k$
DO
  $H := G$
  FOR each pair of elements $h_1, h_2 \in H$ AND
  each overlap relation of h_1, h_2,
    DO
      IF $O(h_1, h_2, p, q) \rightarrow_H r$ AND $r \neq 0$ DO
        Count := Count + 1
        $g_{\mathrm{Count}} := r$
        $G := G \cup \{g_{\mathrm{Count}}\}$
      DONE
    DONE
WHILE $(H \neq G)$

Example 1.3.4.7: Let $K = \mathbb{Z}_3$, $R = K\langle w, x, y, z\rangle$. Let $>$ be the (left) length-lexicographic order with $w < x < y < z$, and $f_1 = yzwx - yx$, $f_2 = xy - zw \in K\langle w, x, y, z\rangle$. Then, $T = \text{tip}(f_1) = yzwx, \text{tip}(f_2) = xy$. Note that $\{f_1, f_2\}$ is tip-reduced. The algorithm for computing Gröbner bases proceeds as follows:
1. Set $g_1 := f_1$, $g_2 := f_2$ and $G := \{g_1, g_2\}$.
2. Compute $O(g_1, g_2, y, yzw) = yzwzw - yxy$, which reduces (modulo g_2) to $yzwzw - yzw$.
3. Set $g_3 := yzwzw - yzw$ and append g_3 to G. i.e. set $G := \{g_1, g_2, g_3\}$.
4. Compute $O(g_2, g_1, zwx, x) = -zwzwx + xyx$, which reduces to $-zwzwx + zwx$, with respect to g_2.
5. Set $g_4 := -zwzwx + zwx$ and append g_4 to G. i.e. set $G := \{g_1, g_2, g_3, g_4\}$.

Since G does not contain any overlap relations other than the ones contained above, and these reduce to zero modulo G, the algorithm terminates, and $G = \{g_1, g_2, g_3, g_4\}$ is a Gröbner basis for $I = \langle\{f_1, f_2\}\rangle$.

We end this section with a couple of results that provides sufficient conditions for the existence of a finite Gröbner basis:

Proposition 1.3.4.8: If I_{MON} has a finite set of monomial generators, then algorithm 1.3.4.6 terminates in a finite number of steps and yields a finite Gröbner basis.

Proposition 1.3.4.8: Let K be a finite field, $R = K\langle x_1, x_2, \ldots, x_n\rangle$, and $>$ be an admissible order. Let I be an ideal such that $\dim_K(R/I)$ is finite. Then I_{MON} has a finite set of monomial generators and I has a finite Gröbner basis.

Chapter 2

Introduction

In 1994, M. Fellows and N. Koblitz [FeKo] proposed a class of combinatorial-algebraic cryptosystems, in which they showed how to use computationally hard combinatorial problems to find trap-door functions that serve as the source of public keys. The generalized version of this class of cryptosystems, which has its security based on the intractability of the ideal membership problem for a commutative algebra over a finite field, is called the *Polly Cracker* cryptosystem. In the present work, we build on this idea by studying the noncommutative analog of this cryptosystem. i.e. we design a cryptosystem based on the ideal membership problem for noncommutative algebras over a finite field.

In this chapter, we describe both the commutative and noncommutative versions of the Polly Cracker cryptosystem. In sections 2.1 and 2.2, we summarize the commutative version, and the weaknesses of this system that are presented in Koblitz [Ko]. In section 2.3, we present the noncommutative Polly Cracker system that we propose. In section 2.4, we present our motivation for studying this system.

2.1 The Generalized (Commutative) Polly Cracker Cryptosystem:

Let K be a finite field, and X a finite set of variables. Let I be an ideal in $K[X]$ and suppose $G = \{g_1, g_2, \ldots, g_t\}$ is a Gröbner basis for I. Then G is used as the private key for the system.

The public key consists of a set $B = \{q_j\}_{j=1}^{s}$ of polynomials in the ideal I, which are chosen so that the computation of a Gröbner basis for $\langle B \rangle$ is infeasible, and the message space M, consists of polynomials, whose terms are not contained in $Lt(I)$, the leading term ideal of I. i.e. the message space M consists of polynomials that are reduced with respect to I.

Encryption is achieved by randomly choosing polynomials $h_1, h_2, \ldots, h_s \in K[X]$, setting $p = \sum_{j=1}^{s} h_j q_j$, and letting $c = p + m$ (where m is the message). Thus, the ciphertext is the sum of $p \in \langle B \rangle \subset I$ and $m \notin I$, where m is reduced with respect to G. Since G is a Gröbner basis for I, by theorem 1.2.2.4, reducing c modulo G yields the unique remainder $N_G(c) = m$. Thus, the ciphertext, is decrypted by applying the multivariable division algorithm (algorithm 1.2.2.2) to $c = p + m$. On the other hand, as seen in example 1.2.2.3, division by a set that is not a Gröbner basis does not yield a unique remainder. Thus,

attempts at decryption by the public key, B will not (in theory) yield the correct plaintext message, m. We note that the encryption here is probabilistic rather than deterministic.

To summarize, we have the following:

Private Key: A Gröbner basis, $G = \{g_1, g_2, \ldots, g_t\}$ for an ideal, I of a polynomial ring $K[X]$ over a finite field K.

Public Key: A set, $B = \left\{ q_j : q_j = \sum_{i=1}^{s_j} h_{ij} g_i \right\}_{j=1}^{s} \subset I$ such that determining a Gröbner basis for $\langle B \rangle$ is computationally infeasible.

Message Space: The set of all polynomials M that cannot be reduced modulo G.

Encryption: $c = p + m$, where $p = \sum_{j=1}^{m} h_j q_j$ is a polynomial in $J = \langle B \rangle$ and $m \in M$ is a message.

Decryption: Reduction of c modulo G yields the message, m.

2.1.1 A special case:

Fellows and Koblitz [FeKo] describe a special case of the Polly Cracker system, which has received much attention from cryptographers and cryptanalysts. See [EGSt], [GeSt], [HoSt] and [Ly] for example.

In this special case, the private key consists of a vector, $\boldsymbol{y} = \langle y_1, y_2, \ldots, y_n \rangle \in K^n$, where K is a finite field, and the public key consists of a finite set of polynomials, $B \subset K[x_1, x_2, \ldots, x_n]$ such that $q_j(y) = 0 \ \forall q_j \in B$. For example, we could have $B = \{x_i - y_i : i = 1, 2, \ldots n\}$. In this system, the message space consists of the constants in K. As above, the ciphertext, c is a polynomial, $c = p + m$, where $p = \sum_{j=1}^{m} h_j q_j$, and m is the message. Decryption is achieved by evaluating the ciphertext polynomial at y. This yields $c(y) = p(y) + m(y) = \sum_{j=1}^{m} h_j(y) \cdot q_j(y) + m = m$.

Although choosing a private key $\boldsymbol{y}$, and constructing a public key, B, are fairly easy in this setting, constructing a secure system is a nontrivial matter. Fellows and Koblitz [FeKo] suggest the use of combinatorial problems to construct specific instances of Polly Cracker cryptosystems. Hence the term, combinatorial-algebraic cryptosystems.

2.2 Attacks On The (Commutative) Polly Cracker Cryptosystem:

In addition to the possibility that the cryptanalyst may be able to find a Gröbner basis for the ideal, J, whose basis, B, is publicly known, Fellows and Koblitz [FeKo] describe a linear algebra attack that looks for weaknesses in the construction of the ciphertext. The method of attack is as follows:

Let c be the ciphertext. Then, $c = \sum_{j=1}^{s} h_j q_j + m$. Let m' be the polynomial that consists of terms of c that are in the message space, M. Set $\sum_{j=1}^{s} f_j q_j + m' = c$ and solve for the unknown f_j. i.e. regard the coefficients of the f_j as unknowns and get linear equations by equating the coefficients of the monomials of $\sum_{j=1}^{s} f_j q_j$ to the corresponding monomials in c.

In [FeKo], Fellows and Koblitz assert that if c and q_j are "sparse" polynomials, then the method in this form of attack is exponential time.

However, in [Ko], Koblitz also describes a more serious "intelligent" linear algebra attack, which was proposed by H.W. Lenstra Jr. in a private communication. A version of the attack is described below:

Let C be the set of monomials occurring in c, and let Q_j be the set of monomials occurring in q_j. Then the cryptanalyst might believe that any monomial, d, occurring in f_j is such that $d \cdot Q_j$ intersects C. The set, D, of those d's is easy to determine and is not too large, so that linear algebra solves the problem in deterministic polynomial time — provided, of course, that the belief is correct.

To defeat this belief, Lenstra suggests that the encryptor must artfully build at least one monomial, d', into at least one f_j, such that d' times any term in q_j is cancelled in the entire sum (so that it doesn't occur in C). Also, the monomials, d' with that property should not be too few and/or easy to guess, since otherwise, the cryptanalyst would simply adjoin those d' to D.

Despite Lenstra's suggestion of a mechanism to defeat the intelligent linear attack which he proposed, the existence of the attack prompted T. Mora and others [MTea] to conjecture that ideal membership (in a commutative algebra over a finite field) cannot be used to construct a public key cryptosystem.

Several other methods of attack have been studied for the special case described in 2.1.1 above. Among these are several variants of the linear algebra attack, which are due to R. Endsuleit, W. Geiselmann, and R. Steinwandt [EGSt] and are described in some detail by Le Van Ly [Ly]; D.Hofheinz and R. Steinwandt [HoSt] describe a "differential" attack that may be used in conjunction with linear algebra attacks; R. Endsuleit, W. Geiselmann, and R. Steinwandt [EGSt] also describe a timing attack that may be used to reveal the secret key assuming that the field, K that is used in constructing the cryptosystem is $\mathbb{Z}_2$, the field of residue classes of integers, modulo 2. W. Geiselmann and R. Steinwandt [GeSt] also describe an attack that reveals the secret key, as does Le Van Ly [Ly] who describes a "lunchtime" attack that is due to R. Cramer [Cram].

We emphasize that each of these attacks (except the linear algebra attack) are known to work only in the special case in which the private key is a vector in K^n, and decryption is achieved by evaluating the ciphertext at this vector. Le Van Ly [Ly] has developed a variant of this cryptosystem, called Polly 2, which he believes is secure against all these forms of attack.

2.3 The Noncommutative Polly Cracker Cryptosystem:

In this article, we investigate the noncommutative analogue of the Polly Cracker cryptosystem. The basic construction, which is very similar to that of the generalized Polly Cracker, is given below:

Let K be a finite field, and X a finite set of non-commuting variables. i.e. suppose $K\langle X\rangle$ is a noncommutative free algebra over K. Let I be a two-sided ideal of $K\langle X\rangle$, and suppose $G = \{g_1, g_2, \ldots, g_t\}$ is a finite Gröbner basis for I. Then G is used as the private key.

The public key, $B = \{q_1, q_2, \ldots, q_s\}$, is a finite set of polynomials in I, which are constructed as follows: Given $G = \{g_1, g_2, \ldots, g_t\}$, fix $r \in \{1, 2, \ldots, s\}$. For each $i,\ 1 \leq i \leq t$, suppose $d_{ir} \in \mathbb{N}$. For each $i, r, j,\ 1 \leq i \leq t,\ 1 \leq j \leq d_{ir}$, choose $f_{rij},\ h_{rij} \in K\langle X\rangle$, and set $q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}$. As in the commutative case, B is constructed so that finding a Gröbner basis of $J = \langle B\rangle$ is computationally infeasible. In this context, we have the following cryptosystem:

Private Key: A Gröbner basis, $G = \{g_1, g_2, \ldots, g_t\}$ for a two-sided ideal, I, of a noncommutative algebra $K\langle X\rangle$ over a finite field, K.

Public Key: A set, $B = \left\{ q_r : q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij} \right\}_{r=1}^{s} \subset I$, chosen so that computing a Gröbner basis of $\langle B\rangle$ is infeasible.

Message Space: $M = \mathrm{NonTip}(I)$ or a subset of $\mathrm{NonTip}(I)$.

Encryption: $c = p + m$, where $m \in M$ is a message and $p = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij}$ is a polynomial in $J = \langle B\rangle \subset I$.

Decryption: Reduction of c modulo G yields the message, m.

2.4 Why The Noncommutative Polly Cracker Cryptosystem:

At first glance, the noncommutative Polly Cracker has two advantages over the commutative version:

First, we note that encryption (in the noncommutative version) is achieved by computing $c = p + m$, where $\{q_j\}_{j=1}^{s}$ is the public key, $p = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij} \in \langle \{q_j\}_{j=1}^{s} \rangle$, and m is the message. So the coefficient of any monomial, W, that occurs in c is quadratic in the coefficients of $F_{rij}, H_{rij},\ i = 1, 2, \ldots, s,\ j = 1, 2, \ldots, k_{ir}$. As a result, it would appear that the noncommutative version of the Polly Cracker cryptosystem that we propose here is not susceptible to a linear algebra attack. For, if we treat the coefficients of F_{rij} and $H_{rij},\ i = 1, 2, \ldots, s,\ j = 1, 2, \ldots, k_{ir}$ as unknowns, we get a non-linear system of equations, for which there are no known methods of solution.

The other advantage of the noncommutative Polly Cracker deals with the "size" of the Gröbner basis of the ideal, J, generated by the public key, $\{q_j\}_{j=1}^{m}$.

In arguing against the (commutative) Polly Cracker cryptosystem, T. Mora et al [MTea] quote a theorem of Giutsi [Gi], which states that even though the degrees of the polynomials of a Gröbner basis can be extremely large, for "almost all" ideals, they are not [in the case of commutative algebras]. This differs from the noncommutative case, where there is a plethora of ideals with infinite Gröbner bases (see E. Green, T. Mora and V. Ufnarovski [GMTU]). It was, in fact, the existence of two-sided ideals (of noncommutative algebras over finite fields) that have no finite Gröbner basis that first inspired us to consider the possibility of developing a noncommutative version of the Polly Cracker cryptosystem.

Our basic approach, then, involves the construction of an ideal, $J \subset I$, where I has a finite Gröbner basis, but J does not. We begin with a chapter on infinite Gröbner bases.

Chapter 3

Infinite Gröbner Bases

Most ideals of the noncommutative free algebra $K\langle x_1, x_2, \ldots, x_n\rangle$, over a field K, are believed to have infinite reduced Gröbner bases under all admissible orders. However, proving that a given class of ideals do not have a finite Gröbner basis under any admissible order appears to be a very difficult problem. Moreover, there are few known techniques to approach this problem. This is partially due to the fact that traditionally, (noncommutative) computational algebra has focused on determining ways of realizing finite Gröbner bases, rather than proving them to be infinite.

In this chapter, we present classes of ideals, which have infinite reduced Gröbner bases under the standard admissible orders. We also determine whether these classes of ideals might be useful in generating public keys for a noncommutative polly cracker cryptosystem. The first two examples of such ideals, which we present in propositions 3.1.1 and 3.1.2 and corollary 3.2.1 are of little value in this direction, because as we show in theorem 3.3, there are techniques to realize a finite Gröbner basis for these ideals. In proposition 3.4.1, we present a third class of ideals, and prove that it has an infinite reduced Gröbner basis under all admissible orders. Finally, we make a conjecture (3.5) about a class of ideals, which we believe to be a rich source of ideals for generating public keys in a noncommutative polly cracker cryptosystem.

Although algebraists have not traditionally focused on proving that a given ideal does not have finite Gröbner bases, there are a few well-known examples of such ideals. For example, E. Green, T. Mora and V. Ufnarovski [GMTU] present what they consider the most amazing principal ideal with an infinite Gröbner basis. They show that the Gröbner basis of the ideal generated by $f = xx - xy \in K\langle x, y\rangle$ is $G = \{g_i = xy^i x - xy^{i+1} : i \in \mathbb{N}\}$ under any admissible order with $x > y$.

Although this result is of mathematical interest, it appears to have little cryptographic value, because, as the authors point out, under any order with $y > x$, $\mathrm{tip}(f) = xy$ and $\{f\}$ is the Gröbner basis of $\langle f\rangle$. However, as an immediate consequence of this result, we have the following:

Proposition 3.1.1:- Let g $= xyx - xy \in K\langle x, y\rangle$. Then $\langle g\rangle \subset K\langle x, y\rangle$ does not have a finite Gröbner basis under any admissible order.

Rather that giving a proof that essentially duplicates the one given by E. Green, T. Mora and V. Ufnarovski [GMTU], we prove the following more general result and explore proposition 3.1.1 as one of its consequences:

Proposition 3.1.2:- Let $A \in K - \{0\}$ and let $g = xyx + Axz \in K\langle x, y, z\rangle$. Then $\langle g\rangle \subset K\langle x, y, z\rangle$ has an infinite reduced Gröbner basis under any admissible order in which $y \geq z$.

Proof:- Let $G = \{g_i : i \in \mathbb{N}\}$, where $g_i = xz^iyx + Axz^{i+1}$. We will show that $G \subset \langle g\rangle$ and that all the overlaps in G are of the form $O(g_m, g_n, z^nyx, xz^myx)$ for some $m, n \in \mathbb{N}$. Moreover, for any $m, n \in \mathbb{N}$, $O(g_m, g_n, z^nyx, xz^myx)$ reduces to g_{m+n+1} with respect to $G - \{g_{m+n+1}\}$, under any admissible order in which $y \geq z$. By the termination theorem (theorem 1.3.4.5), it follows that G is the reduced Gröbner basis of $\langle g\rangle$. We proceed by induction on i.

First, consider $g_0 = xyx + Axz = g$, and $O(g_0, g_0, yx, xy) = Axzyx - Axyxz$, which reduces to $Axzyx + A^2xzz$ (with respect to g_0). If we multiply this by A^{-1}, we get $g_1 = xzyx + Axzz$.

Before proceeding to give an inductive argument, we note that since $y \geq z$, we have $xzyx \geq xzzx > xzz$. i.e. $\text{tip}(g_1) = xzyx$.

Next, consider $g_m = xz^myx + Axz^{m+1}$ and $g_n = xz^nyx + Axz^{n+1}$. Once again, since $y \geq z$, we have $xz^nyx > xz^{n+1}$ and $\text{tip}(g_n) = xz^nyx,\ \text{tip}(g_m) = xz^myx$.

Now, $O(g_m, g_n, z^nyx, xz^myx) = Axz^{m+n+1}yx - Axz^myxz^{n+1}$, which reduces (with respect to g_m) to $Axz^{m+n+1}yx - A^2xz^{m+n+2}$. Once again, if we multiply this by A^{-1}, we get $g_{m+n+1} = xz^{m+n+1}yx + Axz^{m+n+2} \in G$.

Furthermore, $\text{tip}(g_i) = xz^iyx$ does not divide either of the terms of g_{m+n+1}, for any $i \neq m + n + 1$. i.e. g_{m+n+1} is reduced with respect to $G - \{g_{m+n+1}\}$.

Hence, by the termination theorem, it follows that G is the reduced Gröbner basis of $\langle g\rangle$ and that $\langle g\rangle$ does not have a finite Gröbner basis under any admissible order with $y \geq z$. ∎

Remark:- Proposition 3.1.1 is a special case of proposition 3.1.2. To see this, we set $z = y$ and $A = -1$ in $g = xyx + Axz$. This yields $g = xyx - xy \in K\langle x, y\rangle$. Now, since xy divides xyx, $\text{tip}(g) = xyx$ under any admissible order. Similarly, if $g_i = xy^ix - xy^i,\ (i \in \mathbb{N})$, then $\text{tip}(g_i) = xy^ix$. Therefore, by proposition 3.1.2, $G = \{g_i : i \geq 1\}$ is the reduced Gröbner basis of $\langle g\rangle$ under any admissible order.

The next result also follows as a direct consequence of proposition 3.1.2.

Corollary 3.2.1:- Let $g = xTx + AxW \in K\langle x_1, x_2, \ldots, x_n\rangle$, where $x \in \{x_1, x_2, \ldots, x_n\}$, $A \in K - \{0\}$ and T, W are monomials in $x_1, x_2, \ldots, x_n$ such that:

(i). $\{T, W\}$ has no overlaps. i.e. W does not overlap T, and W and T have no self-overlaps.

(ii). T, W do not begin or end with x.

Then $\langle g\rangle \subset K\langle x_1, x_2, \ldots, x_n\rangle$ has an infinite reduced Gröbner basis under any order with $T \geq W$.

As we did in the proof of proposition 3.1.2, we will use the termination theorem (theorem 1.3.4.5) to show that show that under any order with $T \geq W$, the reduced Gröbner basis of $\langle g\rangle$ is $G = \{g_i : i \in \mathbb{N}\}$, where $g_i = xW^iTx + AxW^{i+1}$. But first, we need to prove the following lemma:

Lemma 3.2.2:- Under the hypothesis of corollary 3.2.1, xW^kTx does not divide xW^mTx for any $m > k \geq 0$.

Proof:- Let $W = w_1w_2 \ldots w_\alpha,\ T = t_1t_2 \ldots t_\beta$, where $w_i, t_j \in \{x_1, x_2, \ldots, x_n\},\ \forall i,\ \forall j,\ 1 \leq i \leq \alpha,\ 1 \leq j \leq \beta$.

We will assume that xW^kTx divides xW^mTx for some $m > k \geq 0$ and show that this leads to contradictions.

Suppose, xW^kTx divides xW^mTx, for some $m > k \geq 0$. i.e suppose there exist monomials u, v, such that $xW^mTx = uxW^kTxv$.

Suppose $u \neq 1$, say $u = u_1u_2 \ldots u_s$, where $u_i \in \{x_1, x_2, \ldots x_n\} \forall i = 1, 2, \ldots n$. Since W does not begin with x, it follows that $s \neq 1$, and that there exists $j \in \{1, 2, \ldots, \alpha\}$ such that $u_s = w_j$. If $j = \alpha$, this implies that $w_1 = x$, contradicting the assumption that the first variable of W is not x. If $j \neq \alpha$, and $k \neq 0$, then this yields the sequence of equations, $x = w_{j+1},\ w_1 = w_{j+2},\ w_2 = w_{j+3}, \ldots, w_{\alpha-j-1} = w_\alpha$, contradicting the assumption that $\{W, T\}$ contains no overlaps. If $j \neq \alpha$, and $k = 0$, we have the sequence of equations, $x = w_{j+1},\ t_1 = w_{j+2},\ t_2 = w_{j+3}, \ldots, t_{\alpha-j-1} = w_\beta$. We note here, that $\beta > \alpha - j - 1$, else $T = t_1t_2 \ldots t_\beta = w_{j+2}w_{j+3} \ldots w_{j+\beta+1} < W$, contradicting the assumption that $T \geq W$.

On the other hand, if $u = 1$, then by considering the $(k+1)^{\text{st}}$ copy of W on the left side of the equation $xW^mTx = xW^kTxv$, we get the sequence of equations: $w_1 = t_1$, $w_2 = t_2, \ldots$ There are three possibilities here:

(i). If $\beta > (m-k)\alpha$, then $t_{(m-k)\alpha} = w_\alpha$, $t_{[(m-k)\alpha]+1} = t_1, \ldots, t_\beta = t_{\beta-(m-k)\alpha}$, contradicting the assumption that T has no self-overlaps.

(ii). If $\beta = r\alpha$, for some $r, 1 < r \leq m-k$ then $T = W^r$, contradicting the assumption that T has no self-overlaps.

(iii). If $\beta < (m-k)\alpha$, $\beta \neq r\alpha$, then there exists $j \in \{1, 2, \ldots, \alpha\}$, such that $t_\beta = w_j$, $t_{\beta-1} = w_{j-1}$, $t_{\beta-2} = w_{j-2}, \ldots, t_{\beta-j+1} = w_1$, contradicting the assumption that $\{W, T\}$ does not contain any overlaps.

Hence, xW^kTx does not divide xW^mTx for any $m > k \geq 0$. ∎

Proof of Corollary 3.2.1:- If we set $y = T$ and $z = W$, in the statement of corollary 3.2.1, we get $g = xyx + Axz$. Now, by proposition 3.1.2, the reduced Gröbner basis of $\langle g \rangle$, under any admissible order with $y \geq z$, is $G = \{g_i : i \in \mathbb{N}\}$, where $g_i = xz^iyx + Axz^{i+1}$.

Hence, if $T \geq W$, $G = \{g_i : i \in \mathbb{N}\}$, where $g_i = xW^iTx + AxW^{i+1}$ is a Gröbner basis for $\langle g \rangle \subset K\langle x_1, x_2, \ldots, x_n \rangle$. Also, as seen in lemma 3.2.2, xW^kTx does not divide xW^mTx if $m \neq k$. Note also, that as a consequence of lemma 3.2.2, xW^kTx does not divide xW^m if $m \neq k$. i.e. each $g_m \in G$ is reduced with respect to $G - \{g_m\}$.

Hence, by the termination theorem (theorem 1.3.4.5), G is the reduced Gröbner basis for $\langle g \rangle$ and the reduced Gröbner basis for $\langle g \rangle$ is infinite under any order with $T \geq W$. ∎

Remarks:

1. By symmetric arguments, we can show that the ideals $\langle xyx - yx \rangle \subset K\langle x, y \rangle$, $\langle xyx + Azx \rangle \subset K\langle x, y, z \rangle$ and $\langle xTx + AWx \rangle \subset K\langle x_1, x_2, \ldots, x_n \rangle$ also have infinite reduced Gröbner bases under the hypotheses of propositions 3.1.1, 3.1.2 and corollary 3.2.1 respectively.
2. It is always possible to find monomials, W, T such that $W < T$ under all orders. An example of such a situation would be a monomial W which divides T.

Although we have displayed a class of examples that have infinite reduced Gröbner bases (some under any admissible order), we note that merely having no finite Gröbner basis does not necessarily make an ideal suitable for use in a noncommutative Polly Cracker cryptosystem. In fact, as the next result shows, none of the examples presented so far is suitable for use in a cryptosystem, because there exist techniques to realize a finite Gröbner basis in each of these cases.

Theorem 3.3:- There exist techniques to realize finite Gröbner bases for each of the following ideals:

(a). $\langle g\rangle \subset K\langle x, y\rangle$, where $g = xyx - xy$.

(b). $\langle g\rangle \subset K\langle x, y, z\rangle$, where $g = xyx + Axz,\ A \in K - \{0\}$.

(c). $\langle g\rangle \subset K\langle x_1, x_2, \ldots, x_n\rangle$, where $g = xTx + AxW,\ A \in K - \{0\},\ x \in \{x_1, x_2, \ldots, x_n\}$, and W, T are monomials such that x is not the first or last variable of W or T, $\{W, T\}$ contains no overlaps, and $W \leq T$.

Proof:- (a). Let $g = xyx - xy \in K\langle x, y\rangle$. In order to realize a finite Gröbner basis for $\langle g\rangle$, we introduce a new variable, z, and set $y > z$. Next, we set $g_1 = xy - z$, and show that $I = \langle g_1, g\rangle \subset K\langle x, y, z\rangle$ has a finite Gröbner basis. We then achieve reduction modulo $\langle g\rangle$ in $K\langle x, y\rangle$, by reducing with respect to the Gröbner basis for I in $K\langle x, y, z\rangle$ and setting $xy = z$.

Now, g reduces to $g_2 = zx - z$ (modulo g_1), so that $I = \langle g_1, g_2\rangle$, and $O(g_2, g_1, y, z)$ is the only overlap in $\{g_1, g_2\}$. Furthermore, $O(g_2, g_1, y, z) = zy + zz$. Next, we set $g_3 = zy + zz$. Since $y > z$, we have $zy > zz$, which implies that $\mathrm{tip}(g_3) = zy$ does not overlap the tips of g_1 or g_2. Hence, $\{g_1, g_2, g_3\}$ is a Gröbner basis for I.

We achieve reduction modulo $\langle g\rangle$ in $K\langle x, y\rangle$, by reducing modulo $\{g_1, g_2, g_3\}$ in $K\langle x, y, z\rangle$ and setting $xy = z$.

(b). Let $g = xyx + Axz \in K\langle x, y, z\rangle$. Then $\langle g\rangle$ has a finite Gröbner basis under any order in which $z > yx$.

For example, if $>$ is a weight-lexicographic order, with $w(x) = w(y) = 1$ and $w(z) = 3$, then $W(xz) = w(x) + w(z) = 3 + 1 = 4 > 3 = W(xyx)$, so that $\mathrm{tip}(g) = xz$ has no self-overlaps, and $\{g\}$ is the reduced Gröbner basis of $\langle g\rangle$.

(c). Let T, W be monomials in $\{x_1, x_2, \ldots, x_n\}$ such that $x \in \{x_1, x_2, \ldots, x_n\}$ is not the first or last variable of W or T, $\{W, T\}$ contains no overlaps and $W \leq T$. Let $g = xTx + AxW \in K\langle x_1, x_2, \ldots, x_n\rangle$, where $A \in K - \{0\}$.

We obtain a finite Gröbner basis for $\langle g\rangle$, by the same technique that we used in the proof of 3.3(a). First, we introduce a new variable, z, and set $W > z, xW > zx$. Next, we set $g_1 = xT - z$, and show that the ideal $I = \langle g_1, g\rangle \subset K\langle x_1, x_2, \ldots, x_n, z\rangle$ has a finite Gröbner basis. We then achieve reduction modulo $\langle g\rangle$ in $K\langle x, y\rangle$, by reducing with respect to the Gröbner basis for I in $K\langle x_1, x_2, \ldots, x_n, z\rangle$ and setting $xT = z$.

Now, g reduces to $AxW + zx$ (with respect to g_1). Multiplying this by A^{-1}, we get $g_2 = xW + A^{-1}zx$, so that we have $I = \langle g_1, g_2\rangle$. Furthermore, since $xW > zx$,

$\text{tip}(g_2) = xW$. Also, since x is not the first or last variable of W or T, and $\{W, T\}$ contains no overlaps, it follows that $\{g_1, g_2\}$ does not contain any overlaps. So we're done if xW does not divide xT.

Next, we consider the possibility that xW divides xT, say $xT = u_1 xW v_1$, where u_1, v_1 are monomials in $\{x_1, x_2, \ldots, x_n\}$, which could possibly be 1. Then, g_1 reduces to $u_1 zxv_1 + Az$, whose tip, $u_1 zxv_1$, has no self-overlaps and no overlaps with $\text{tip}(g_2)$, so that we're done if xW does not divide $u_1 zxv_1$.

Now, if xW divides $u_1 zxv_1$, it must divide one (or both) of u_1 or xv_1. If xW divides u_1, say $u_1 = u_2 xW v_2$, then $u_1 zxv_1 + Az$ reduces to $u_2 zxv_2 zxv_1 - A^2 z$. If, on the other hand, xW divides xv_1, say $xv_1 = u_2 xW v_2$, then $u_1 zxv_1 + Az$ reduces to $u_1 zxu_2 zxv_2 - A^2 z$. Once again, if xW does not divide $u_2 zxv_2 zxv_1$ or $u_1 zxu_2 zxv_2$ (as the case may be), then we're done, since neither of these terms can overlap xW, else T overlaps W.

If xW divides $u_2 zxv_2 zxv_1$ or $u_1 zxu_2 zxv_2$ (as the case may be), it must divide at least one of u_1 or xv_1 or u_2 or xv_2. Since T is a monomial of finite length, if we continue recursively, as above, the process ends in a finite number of steps, and we obtain a polynomial, ${g_1}' = u_m W' v_m + (-1)^{m+1} A^m z$, where v_m is a suffix of T, $u_m = 1$ or $u_m = x{u_m}'$, where ${u_m}'$ is a prefix of T and xW does not divide $\text{tip}({g_1}') = u_m W' v_m$. Furthermore, $\{{g_1}', g_2\}$ contains no overlaps, and hence must be a Gröbner basis for I.

As mentioned earlier, we achieve reduction modulo $\langle g \rangle$ in $K\langle x_1, x_2, \ldots, x_n \rangle$ by reducing modulo $\{{g_1}', g_2\}$ in $K\langle x_1, x_2, \ldots, x_n, z \rangle$ and setting $z = xT$. ∎

Remark:- The technique used in the proofs of theorem 3.3 (a) and (c) is known as a *string rewrite system*. Such systems, which are presented in greater generality in R. Book and F. Otto [BoOt], M. Jantzen [Ja] and other works on the subject, are beyond the scope of the current work. However, we note that for an ideal to be of cryptographic interest, it must not yield a finite Gröbner basis by such a technique. Our next two results provide examples of such ideals.

Proposition 3.4.1:- Let K be a finite field, and $K\langle x, y, z \rangle$ the noncommutative free algebra over K. Let $g_1 = xzy + yz \in K\langle x, y, z \rangle$, $g_2 = yzx + zy \in K\langle x, y, z \rangle$. Then, $I = \langle g_1, g_2 \rangle$ does not have a finite Gröbner basis under any admissible order.

Proof:- We will prove that I does not have a finite Gröbner basis by displaying an infinite sequence of polynomials in I, whose tips are not divisible by a finite subset of $\text{Tip}(I)$. We need to consider two scenarios here:

1. $\text{tip}(g_1) = xzy$ and $\text{tip}(g_2) = yzx$
2. $\text{tip}(g_1) \neq xzy$ or $\text{tip}(g_2) \neq yzx$

We begin by proving that I has an infinite (reduced) Gröbner basis under any order for which $\text{tip}(g_1) = xzy$ and $\text{tip}(g_2) = yzx$. This includes most of the standard orders such as length-lex, length-right-lex, weight-lex and weight-reverse-lex.

In order to construct the infinite sequence of polynomials in I, whose tips are not divisible by a finite subset of $\text{Tip}(I)$, we will look at overlap relations in I, using length-lex with $x > y$. We emphasize here that these polynomials need not be in a Gröbner basis under all orders for which $\text{tip}(g_1) = xzy$ and $\text{tip}(g_2) = yzx$. However, the fact that they are elements of I is independent of the order.

Consider $O(g_1, g_2, zx, xz) = yzzx - xzzy$. Since we are using length-lex with $x > y$, we have $xzzy > yzzx$. We set $g_3 = xzzy - yzzx$ so that $\text{tip}(g_3) = xzzy$, and consider $O(g_3, g_2, zx, xzz) = -yzzxzx - xzzzy$. We set $g_4 = yzzxzx + xzzzy$ and note that $\text{tip}(g_4) = yzzxzx$.

Next, we consider $O\left(g_1, g_4, z^2xzx, xz\right) = yzzzxzx - xzxzzzy$. Once again, since $xzxzzzy > yzzzxzx$, we set $g_5 = xzxzzzy - yzzzxzx = (xz)^2 z^2y - yz^2 (zx)^2$, and consider $O\left(g_5, g_2, zx, (xz)^2 z^2\right) = -yz^2 (zx)^3 - (xz)^2 z^3y$.
Set $g_6 = yz^2 (zx)^3 + (xz)^2 z^3y$ and note that $\text{tip}(g_6) = yz^2 (zx)^3$.

Continuing inductively, we get:
$g_{2n} = O\left(g_{2n-1}, g_2, zx, (xz)^{n-1} z^{n-1}\right) = yz^{n-1} (zx)^n + (xz)^{n-1} z^n y$ for all $n \geq 2$ (after appropriate change of signs), and
$g_{2n+1} = O\left(g_1, g_4, z^{n-1} (zx)^n, xz\right) = (xz)^n z^n y - yz^n (zx)^n$ for all $n \geq 2$
(after appropriate change of signs).

Now, if I has a finite Gröbner basis, then the tip of some element of this Gröbner basis would have to divide $\text{tip}(g_{2n})$ for infinitely many $n \in \mathbb{N}$. i.e. the tip of some element of this Gröbner basis would have to divide infinitely many $yz^{n-1} (zx)^n$, $n \geq 2$ or infinitely many $(xz)^n z^{n-1}y$, $n \geq 2$, depending on whether $yz^{n-1} (zx)^n > (xz)^n z^{n-1}y$ or $(xz)^n z^{n-1}y > yz^{n-1} (zx)^n$. We show that both of these are impossible if $\text{tip}(g_1) = xzy$ and $\text{tip}(g_2) = yzx$.

First, suppose that the tip of some element of I divides infinitely many $(xz)^{n-1} z^n y$, $n \geq 2$. But then, the tip of this element would have to be one of:

(i). $(xz)^k z^m$ for some $m, k \in \mathbb{N}$, m, k not both zero or

(ii). $z^m y$ for some $m \geq 0$.

However, since each monomial that occurs in g_1 and each monomial that occurs in g_2 contains y, it is impossible for any monomial that occurs in any element of I to contain only x's and z's. Hence, z^m and $(xz)^k z^m$ cannot occur as elements of $\mathrm{Tip}(I)$.

Similarly, since all monomials that occur in g_1 or g_2 contain z, y cannot occur as a monomial of an element of I. i.e. $m \neq 0$ in the monomials of type (ii), above.

Next, suppose $z^m y \in \mathrm{Tip}(I)$. i.e. suppose there exists $F = f_1 g_1 h_1 + f_2 g_2 h_2 \in I$ such that $\mathrm{tip}(F) = z^m y$ for some $m \in \mathbb{N}$. Note that for $z^m y$ to occur as a monomial in F, z^{m-1} must occur in f_2 and h_2 must contain a constant, so that $f_2 g_2 h_2$ contains $z^{m-1}(yzx + zy) = z^{m-1}yzx + z^m y$. But then, $z^{m-1}yzx > z^m y$ and must be subtracted off in F.

Now, for $z^{m-1}yzx$ to occur in $f_2 g_2 h_2$ as some other product of monomials, zx must occur in h_2 and z^{m-2} must occur in f_2, so that $z^{m-2}(zy)zx$ yields $z^{m-1}yzx$. But then, $f_2 g_2 h_2$ would also contain $z^{m-1}(zy)zx = z^m yzx > z^m y$, which would also have to be subtracted off in F.

Once again, for $z^m yzx$ to occur in $f_2 g_2 h_2$ in some other way, z^m must occur in f_2 with a non-zero coefficient, so that $z^m(yzx)$ yields $z^m yzx$. However, this implies that $z^m(zy) = z^{m+1}y$ occurs in $f_2 g_2 h_2$, and since it cannot occur in F in any other way, we would have $z^{m+1}y > \mathrm{tip}(F)$ occurring in F, a contradiction. Hence, at least one of $z^{m-1}yzx$ or $z^m yzx$ must be subtracted off by a monomial in $f_1 g_1 h_1$.

Since $z^{m-1}yzx$ or $z^m yzx$ are of the same basic form, we can assume, without loss of generality, that $z^{m-1}yzx$ must be subtracted off by a monomial in $f_1 g_1 h_1$.

Now, for $z^{m-1}yzx$ to occur in $f_1 g_1 h_1$, z^{m-1} must occur in f_1 and x must occur h_1, so that $f_1 g_1 h_1$ contains $z^{m-1}(xzy + yz)x = z^{m-1}xzyx + z^{m-1}yzx$. But then, $z^{m-1}xzyx$ and must be subtracted off in F, since $z^{m-1}xzyx > z^{m-1}y$.

For $z^{m-1}xzyx$ to occur in F as a product of some other monomials, f_2 must contain $z^{m-1}x$ and h_2 must contain x, so that $f_2 g_2 h_2$ contains $z^{m-1}x(zy)x$. But then, F also contains $z^{m-1}x(yzx)x = z^{m-1}xyzx^2$. Now, in order to eliminate $z^{m-1}xyzx^2$ from F, h_1 must contain x^2, so that $f_1 g_1 h_1$ contains $z^{m-1}(xzy + yz)x^2 = z^{m-1}xzyx^2 + z^{m-1}yzx^2$, and $z^{m-1}xzyx^2$ must be subtracted off from F.

Proceeding inductively, it follows that h_1 must contain x^n for all $n \in \mathbb{N}$, contradicting the fact that h_1 is a polynomial with a finite number of terms.

Hence $z^m y \notin \mathrm{Tip}(I)$.

It follows that I does not contain any element whose tip divides infinitely many $(xz)^n z^n y, n \geq 2$.

Similarly, for a single element of $\text{Tip}(I)$ to divide infinitely many $yz^{n-1}(zx)^n, n \geq 2$, it would have to be of one of the following forms:

(i). yz^k for some $k \geq 0$ or

(ii). $z^k (zx)^m$ for some $m, k \in \mathbb{N}$, m, k not both zero.

As seen earlier, y cannot occur as a monomial in an element of I, and neither can any monomial containing only z's and x's. Hence, the only possibility is that $yz^k \in \text{Tip}(I)$ for some $k > 0$.

By an argument similar to the one which showed that $z^m y \notin \text{Tip}(I)$ for any $m \in \mathbb{N}$, it follows that $yz^k \notin \text{Tip}(I)$ for any $k \in \mathbb{N}$.

It follows that I cannot have a finite Gröbner basis under any of the order in which $\text{tip}(g_1) = xzy$ and $\text{tip}(g_2) = yzx$.

Next, we turn our attention to orders in which $\text{tip}(g_1) = yz$ or $\text{tip}(g_2) = zy$. Note that we cannot have $\text{tip}(g_1) = yz$ and $\text{tip}(g_2) = zy$, for if $\text{tip}(g_1) = yz$, then g_2 reduces to $xzyx - zy$. Since $xzyx > zy$, it follows that $\text{tip}(g_2) = xzyx$. Similarly, if $\text{tip}(g_2) = zy$, then g_1 reduces to $xyzx - yz$, from which it follows that $\text{tip}(g_1) = xyzx$.

Suppose that $>$ is an order in which $yz > xzy$. i.e. suppose $g_1 = yz + xzy$ and $g_2 = xzyx - zy$, with $tip(g_1) = yz$ and $\text{tip}(g_2) = xzyx$.

As we did in the previous case, we will show that I cannot have a finite Gröbner basis under this order, by constructing a sequence of elements in $\text{Tip}(I)$, which cannot be divided by a finite set of elements in $\text{Tip}(I)$.

To construct this sequence, we consider $g_1 = xzy + yz$ and $g_2 = yzx + zy \in I$ under length-lex with $x > y > z$. Then, $h_1 = O(g_2, g_1 zy, yz) = yzyz - zyzy$. Now, $O(h_1, h_1, yz, yz) = yzzyzy - zyzyyz$. Set $f_1 yzzyzy - zyzyyz$. Next, we consider the overlap, $O(f_1, h_1, z, yzz) = yz^3 yzy - zyzyyz^2$. We set this polynomial equal to f_2. Continuing inductively, we get $f_n = O(f_{n-1}, h_1, z, yz^n) = yz^{n+1} yzy - zyzyyz^n \ \forall\ n \geq 2$. i.e. $\{f_n\}_{n=1}^{\infty}$ is an infinite sequence of elements in I.

Now, if $yz > xzy$, then f_n reduces (modulo $g_1 = yz + xzy$, $g_2 = xzyx - zy$) to $p_n = zxzy^2 (xz)^n y - (xz)^n zxzy^3 \ \forall\ n \geq 2$. Therefore if I has a finite Gröbner basis under $>$, then some $T \in \text{Tip}(I)$ must divide infinitely many elements of $\{\text{tip}(p_n) : n \geq 2\}$.

Next, we show that $(xz)^n zxzy^3 \notin \text{Tip}(I)$ under this order. We do this by assuming that $(xz)^n zxzy^3 \in \text{Tip}(I)$, and showing that this leads to contradictions. Suppose $(xz)^n zxzy^3 \in \text{Tip}(I)$ i.e. suppose there exists $F = f_1 g_1 h_1 + f_2 g_2 h_2 \in I$ such that

$\text{tip}(F) = (xz)^n zxzy^3$ for some $n \in \mathbb{N}$. Now, $(xz)^n zxzy^3$ can occur as a monomial in an element of I in two ways:

(i). In $(xz)^n zxg_2y^2$ or

(ii). In $(xz)^n zg_1y^2$.

First, suppose $(xz)^n zxzy^3$ occurs in F in the form $(xz)^n zxg_2y^2$. Then the term $(xz)^n zx^2zyx > (xz)^n zxzy^3$ also occurs in F and must be subtracted off in order for $\text{tip}(F)$ to be $zxzy^2 (xz)^n y$. Now, if we use g_2 to subtract off this term, we get a new term $(xz)^n zx^3zyx^2 > (xz)^n zx^2zyx > (xz)^n zxzy^3$. If we proceed inductively, using only g_2 to subtract off the larger monomials that are created at each stage, we find that the increasing infinite sequence of monomials, $(xz)^n zx^mzyx^{m-1},\ m \geq 1$, occurs in F, contradicting the fact that F is a polynomial with a finite number of terms and $\text{tip}(F) = zxzy^2 (xz)^n y$ for some $n \in \mathbb{N}$. Hence, some $(xz)^n zx^mzyx^{m-1},\ m \geq 1$ must be subtracted off by a monomial in $f_1g_1h_1$.

Now, if $(xz)^n zx^mzyx^{m-1}$ occurs in $f_1g_1h_1$ for some $m \geq 1$, then $(xz)^n zx^{m-1}yzx^{m-1}$ also occurs in $f_1g_1h_1$. Since $(xz)^n zx^{m-1}yzx^{m-1} > (xz)^n zxzy^3$, and $(xz)^n zx^{m-1}yzx^{m-1}$ cannot occur in F in any other way this contradicts fact that $\text{tip}(F) = (xz)^n zxzy^3$.

Similarly, if $(xz)^n zxzy^3$ occurs in F in the form $(xz)^n zg_1y^2$, then the term $(xz)^n zyz$ also occurs in F. Now, since $(xz)^n zyz > (xz)^n zxzy^3$, it must be subtracted off in order for $\text{tip}(F)$ to be $zxzy^2 (xz)^n y$. This term cannot be subtracted off using g_1. If we use g_2 to subtract it off in F, we get a new term $(xz)^n xzyxz > (xz)^n zyz > (xz)^n zxzy^3$. If we proceed inductively, using only g_2 to subtract off the larger monomials that are created at each stage, we find that the increasing infinite sequence of monomials, $(xz)^n x^mzyx^mz,\ m \geq 1$, occurs in F, contradicting the fact that F is a polynomial with a finite number of terms and $\text{tip}(F) = zxzy^2 (xz)^n y$ for some $n \in \mathbb{N}$. Hence, some $(xz)^n x^mzyx^mz,\ m \geq 1$ must be subtracted off by a monomial in $f_1g_1h_1$.

As before, if $(xz)^n x^mzyx^mz$ occurs in $f_1g_1h_1$ for some $m \geq 1$, then $(xz)^n x^{m-1}yzx^mz$ also occurs in $f_1g_1h_1$. Since $(xz)^n x^{m-1}yzx^mz > (xz)^n x^mzyx^mz$, and $(xz)^n x^{m-1}yzx^mz$ cannot occur in F in any other way, this contradicts the fact that $\text{tip}(F) = zxzy^2 (xz)^n y$.

In either case, a monomial which is larger than $(xz)^n zxzy^3$ occurs in F and any attempt to subtract it out results in an infinite sequence of increasing monomials occurring in F, or yields a term that cannot be subtracted off. Hence, $(xz)^n zxzy^3 \notin \text{Tip}(I)$, and $\text{tip}(p_n) = zxzy^2 (xz)^n y,\ \forall\ n \geq 2$.

Now, for some $T \in \text{Tip}(I)$ to divide infinitely many $\text{tip}(p_n)$, it must be of one of the following forms:

(a). $z, zx, zxz, x, y, y^2, yx, yyx$, or $(xz)^m$ for some $m > 0$ or

(b). $y\,(xz)^m$ or $yy\,(xz)^m$ for some $m \in \mathbb{N}$ or

(c). $xzy, xzyy, xzyyx, zxzy, zy, zyyx, zxzyyx$ or

(d). $(xz)^m\,y, zyy\,(xz)^m$ or $xzyy\,(xz)^m$ or $zxzyy\,(xz)^m$, for some $m \in \mathbb{N}$.

As seen earlier, the monomials listed in (a) above, cannot occur in elements of I. In addition, the monomials listed in (b) cannot occur in elements of I since every occurrence of xz in a monomial of g_1 or g_2 is followed by a y, so these cannot be used to create any of the monomials listed in (b). Similarly, the only monomial in g_1 or g_2 that begins with y is yz, which cannot be used to create any of the monomials listed in (b). Furthermore, routine arguments (similar to the one which showed that $z^m y \notin \mathrm{Tip}(I)$ in the previous case and the one which showed that $(xz)^n\,zxzy^3 \notin \mathrm{Tip}(I)$) can be used to show that the monomials listed in (c) and (d) above are not elements of $\mathrm{Tip}(I)$ under any order in which $yz > xzy$.

Hence, I does not have a finite Gröbner basis under any order with $yz > xzy$.

Similarly, it can be shown that I does not have a finite Gröbner basis under any order in which $zy > yzx$.

Hence, $I = \langle g_1, g_2 \rangle$, where $g_1 = xzy + yz$ and $g_2 = yzx + zy$ does not have a finite Gröbner basis under any admissible order. ∎

Corollary 3.4.2:- Let K be a finite field, and let $K\langle x_1, x_2, \ldots, x_n \rangle$ be the noncommutative free algebra in n variables with $n \geq 5$. Let $A = \prod_{i=1}^{n} x_i$, $B = x_1 \left(\prod_{i=2}^{n-1} \rho(x_i) \right) x_n$ and $C = x_1 \left(\prod_{i=2}^{n-1} \sigma(x_i) \right) x_n$, where $\rho,\ \sigma$ are nontrivial permutations of $\{x_2, x_3, \ldots, x_{n-1}\}$. Let $g_1 = ACB + BC, g_2 = BCA + CB$. Then $I = \langle g_1, g_2 \rangle$ does not have a finite Gröbner basis under any admissible order.

Proof:- Since $\{A, B, C\}$ contains no overlaps, the result follows from proposition 3.4.1, by setting $x = A, y = B$ and $z = C$. ∎

Remarks:-

1. There are several variations of the class of examples provided by proposition 3.4.1, which we believe, do not have a finite Gröbner basis under any admissible order. We mention a couple of these here:

   (a). Let $g_1 = xzy + xwy + yz + yw + xy$ and $g_2 = yzx + ywx + zy + wy + yx$.
   It is easy to see that $I = \langle g_1, g_2 \rangle$ contains polynomials of the type:
   $yz^n (zx)^n + yw^n (wx)^n +$ smaller terms.
   As seen in the proof of proposition 3.4.1, this leads to an infinite (reduced) Gröbner basis.

   (b). Let $g_{i1} = xz_iy + xw_iy + yz_i + yw_i + xy, \ \forall \ i = 1, 2, \ldots, n$
   and $g_{i2} = yz_ix + yw_ix + z_iy + w_iy + yx, \ \forall \ i = 1, 2, \ldots, n.$
   Let $I = \langle g_{11}, g_{12}, g_{21}, g_{22}, \ldots, g_{n1}, g_{n2} \rangle \subset K\langle x, y, z_1, z_2, \ldots, z_n, w_1, w_2, \ldots, w_n \rangle$.
   It seems reasonable to believe that any Gröbner basis of I would contain (as a subset) a Gröbner basis of the example mentioned in (a) above, and hence could not possibly be finite.

Partial Gröbner bases for both these examples were computed using *Opal*, for various standard orders, and appeared to be infinite.

2. Many other examples that were studied using *Opal*, appeared to have infinite (reduced) Gröbner bases under length-lex or weight-lex. In particular, the principal ideals generated by each of the following polynomials appeared to have infinite (reduced) Gröbner bases under standard orders:

   (a). $z (xyz)^n + z^3 +$ all quadratic and lower terms $(n \geq 3)$.

   (b). $z (xyz)^n + zxyz +$ all quadratic and lower terms $(n \geq 2)$.

   (c). $(xy)^n x + (xy)^n + (yx)^n +$ all quadratic and lower terms $(n \geq 3)$.

   (d). $x^3 + xyx + yxy + x^2 + xy + yx + y^2 + x + y + 1$.

3. One surprising example that has a finite Gröbner basis under length-lex with $x > y > z$ is the principal ideal generated by $(xyz)^n + a_1x^3 + a_2y^3 + a_3z^3 + a_4xx + a_5xy + a_6xz + a_7yx + a_8yy + a_9yz + a_{10}zx + a_{11}zy + a_{12}zz + a_{13}x + a_{14}y + a_{15}z + a_{16}$, where each $a_i, \ i = 1, 2, \ldots, 16$ is an arbitrary constant.

We conclude this chapter with one final conjecture that is a useful source of ideals of cryptographic interest:

Conjecture 3.5:- Let K be a finite field, $K\langle x_1, x_2, \ldots, x_n\rangle$ the noncommutative free algebra in n variables ($n \geq 2$). Let $G = \{g_1, g_2, \ldots, g_m\}$ be a finite subset of $K\langle x_1, x_2, \ldots, x_n\rangle$, all of whose elements have the same tip, T. Let N be the words of length $(\alpha - 1)$ that occur in all the g_k's (combined) and suppose that $l(T) = \alpha > 3$. Suppose, in addition:

(i). $m \approx \frac{N}{2}$ and

(ii). N is approximately one-third and strictly less than the number of all possible words of length $(\alpha - 1)$. i.e. $N \approx \frac{1}{3}n^{\alpha-1}$ and $N < \frac{1}{2}n^{\alpha-1}$.

Then there is a high probability that the reduced Gröbner basis of $\langle G\rangle$ is infinite.

Remarks:-

1. The set G, described in conjecture 3.5 consists of elements of the type $g_k = T + \sum_{i=1}^{N_k} a_{ki}W_{ki} + \sum_{j=1}^{s_k} b_{kj}V_{kj}$, where $l(T) = \alpha$, $l(W_{ki}) = \alpha - 1 \; \forall \; i, \; k$, and the number N of words W_{ki} of length $(\alpha-1)$ that occurs in all the g_i's (combined) satisfies the relations $N \approx \frac{1}{3}n^{\alpha-1}$ and $N < \frac{1}{2}n^{\alpha-1}$, $l(V_{kj}) = \alpha$ or $l(V_{kj}) < \alpha - 1 \; \forall \; k, \; j$, and $a_{ki}, \; b_{kj}$ are arbitrary constants for all $i, \; k, \; j$.
2. Some ideals that satisfy conjecture 3.5 have finite Gröbner basis. These are exceptional cases based on specific values of $a_{ki}, \; b_{kj}$ (see example 3.5.1 below).

Example 3.5.1:- Let $K = \mathbb{Z}_3$, $G = \{g_1, g_2\} \subset K\langle x, y\rangle$, where $g_1 = xyyy+xyy+xxy+xyx$ and $g_2 = xyyy + xyy + 2xxy + xyx$. Then, $T = \text{tip}(g_1) = \text{tip}(g_2) = xyyy$ (under length-lex with any order on x, y), $\alpha = l(T) = 4$; $\alpha - 1 = 3$, $N =$ number of words of length 3 is 3, which is approximately equal to $\frac{1}{3} \cdot 2^3$ and $m = 2 \approx \frac{N}{2}$. So $G = \{g_1, g_2\}$ can be considered to satisfy the hypothesis of conjecture 3.5. However, g_2 reduces to $g_2' = xxy$ with respect to g_1, and since $\text{tip}(g_2') = xxy$ and $\text{tip}(g_1) = xyyy$ have no overlaps, $G_1 = \{g_1, g_2'\}$ is a Gröbner basis for $\langle G\rangle$.

Since there are few known techniques to prove that an ideal does not have a finite Gröbner basis and also because conjecture 3.5 depends on the the coefficients of the terms of length $\alpha - 1$ (where α is the length of the common tip, T) being random, we are unable to give a formal proof at this time. In support of the conjecture, however, we note that in computing a Gröbner basis of $\langle G\rangle$, at most one $g_k \in G$ would retain the original tip, T. With one-third of the possible words of length $(\alpha - 1)$ occurring in the g_k's, there is a high probability that the tip-reduced g_k's will have overlaps (assuming, of course, that

the coefficients of the terms of the g_k's are truly random). Since the number, N, of the words of length $(\alpha - 1)$ that occurs in the g_k's is strictly less than $\frac{1}{2} \cdot n^{\alpha-1}$, there is a high probability that not all of these overlaps will reduce to zero. Moreover, in view of proposition 1.3.4.8, which states that an ideal, I, of a K-algebra, R, has a finite Gröbner basis if $\dim_K (R/I)$ is finite, we believe that the upper limit is also required in order to ensure that $\dim_K \left(\frac{K\langle x_1, x_2, \ldots, x_n \rangle}{\langle G \rangle} \right)$ is not finite. Once again, since $N \approx \frac{1}{3} \cdot n^{\alpha-1}$, there is a high probability that the new relations introduced into G during the computation of the Gröbner basis, will have overlaps with its existing elements, and the process continues recursively.

This conclusion is also supported by a number of trial runs on *Opal*.

Before giving an example, we emphasize that in order to construct useful instances where $\langle G \rangle$ has no finite Gröbner basis, α must be reasonably large, say $\alpha \geq 5$.

Example 3.5.2:- Let $K = \mathbb{Z}_{331},\ K\langle x, y \rangle = \mathbb{Z}_{331}\langle x, y \rangle$.

Let $G = \{g_1, g_2, g_3, g_4, g_5\}$, where

$g_1 = xxyyy - 161xyxyyy - 36yxxyyy + 116xxxyx + 140xxxyy + 74xxyyy - 140xyxyx - 32xyxyy - 107xyyyy + 127yxxyx - 75yxxyy - 136yxyyy + 150xxxx - 53xxxy - 22xxyx + 19xxyy + 13xyxx - 73xyxy - 165xyyx - 40xyyy - 104yxxx - 78yxxy + 112yxyx + 59yxyy + 13yyyy - 103xxx + 2xxy - 120xyx + 12xyy - 59yxx - yxy - 147yyx + 6yyy + 77xx + 50xy - 135yx + 45yy - 112x + 71y - 16,$

$g_2 = xxyyy - 83xyxyyy - 149yxxyyy - 135xxxyx + 135xxxyy - 2xxyyy - 49xyxyx + 49xyxyy - 86xyyyy - 76yxxyx + 76yxxyy + 66yxyyy + 48xxxx + 2xxxy - 61xxyx - 19xxyy - 12xyxx + 165xyxy + 25xyyx + 132xyyy + 130yxxx + 33yxxy + 27yxyx - 23yxyy - 110yyyy + 143xxx + 17xxy - 92xyx - 94xyy - 5yxx - 18yxy - 45yyx + 22yyy + 108xx - 65xy - 64yx + 157yy + 85x + 24y + 96,$

$g_3 = xxyyy + 9xyxyyy + 83yxxyyy - 79xxxyx + 90xxxyy + 107xxyyy - 49xyxyx + 148xyxyy + 117xyyyy + 63yxxyx - 143yxxyy + 37yxyyy + 109xxxx - 37xxxy + 153xxyx - 49xxyy - 12xyxx - 2xyxy + 25xyyx - 45xyyy + 110yxxx - 92yxxy + 56yxyx + 25yyyy + 86xxx - 7xxy - 51xyx + 17xyy + 63yxx - 50yxy + 11yyx - 135yyy + 143xx + 32xy + 77yx + 12yy + 152x + 147y - 61,$

$g_4 = xxxyyy + 105xyxyyy + 40yxxyyy + 73xxxyx + 14xxxyy + 36xxyyy + 52xyxyx + 146xyxyy + 41xyyyy - 59yxxyx - 102yxxyy + 77yxyyy - 151xxxx + 87xxxy - 20xxyx + 93xxyy + 33xyxx - 133xyxy + 14xyyx + 133xyyy - 82yxxx - 161yxxy - 6yxyx - 136yxyy - 132yyyy - 87xxx - 76xxy + 138xyx + 69xyy + 92yxx - 144yxy - 37yyx + 110yyy + 34xx - 123xy - 149yx + 91yy - 54x - 119y + 117,$

$g_5 = xxxyyy + 93xyxyyy - 155yxxyyy + 75xxxyx - 143xxxyy - 17xxyyy + 24xyxyx - 59xyxyy - 115xyyyy - 40yxxyx - 12yxxyy + 29yxyyy - 137xxxx - 14xxxy + 49xxyx + 34xxyy - 163xyxx + 22xyxy - 19xyyx - 20xyyy + 51yxxx - 147yxxy - 142yxyx - 22yxyy + 92yyyy - 60xxx - 9xxy + 142xyx - 88xyy - 95yxx + 145yxy - 51yyx + 32yyy + 125xx + 2xy + 128yx - 96yy + 158x + 155y - 146.$

Here, after reducing the tips, G is rewritten as:

$\{78xyxyyy - 113yxxyyy + 80xxxyx - 5xxxyy - 76xxyyy + 91xyxyx + 81xyxyy + 21xyyyy + 128yxxyx + 151yxxyy - 129yxyyy - 102xxxx + 55xxxy - 39xxyx - 38xxyy - 25xyxx - 93xyxy - 141xyyx - 159xyyy - 97yxxx + 111yxxy - 85yxyx - 82yxyy - 123yyyy - 85xxx + 15xxy + 28xyx - 106xyy + 54yxx - 17yxy + 102yyx + 16yyy + 31xx - 115xy + 71yx + 112yy - 134x - 47y + 112,$

$-110yxxyyy + 55xxxyx - 107xxxyy - 39xxyyy + 3xyxyx - 22xyxyy + 5yxxyx - 134yxxyy - 106yxyyy + 54xxxx - 19xxxy - 71xxyx - 104xxyy + 21xyxx + 70xyxy + 39xyyx + 36xyyy + 35yxxx + 126yxxy - 32yxyx - 67yxyy - 118xxx + 162xxy - 9xyx - 78xyy - 123yxx + 22yxy + 63yyx - 91yyy - 44xx - 5xy - 104yx - 14yy - 72x + 136y - 26,$

$-13xxxyx - 114xxxyy + 35xxyyy - 10xyxyx - 126xyxyy + 138yxxyx + 133yxxyy + 121yxyyy - 91xxxx + 33xxxy + 72xxyx - 109xxyy - 70xyxx - 129xyxy - 130xyyx - 149xyyy - 27yxxx + 91yxxy - 2yxyx + 2yxyy - 82yyyy + 79xxx - 8xxy - 154xyx + 131xyy - 53yxx + 104yxy + 153yyx - 153yyy - 43xx - 100xy - 51yx - 72yy - 116x - 44y + 23,$

$116xxxyy + 86xxyyy - 153xyxyx + 46xyxyy + 30yxxyx + 165yxxyy - 10yxyyy - 29xxxy - 92xxyx - 88xxyy - 78xyxx - 108xyxy - 3xyyx + 86xyyy - 121yxxx - 89yxxy - 90yxyx - 95yxyy - 130yyyy + 89xxx - 127xxy + 110xyx + 119xyy - 153yxx + 125yxy + 49yyx + 140yyy - 71xx - 133xy - 59yx - 118yy - 122x + 21y + 80,$

$-132xxyyyy+27xyxyxy+84xyxyyy+131yxxyxy-143yxxyyy-154yxyyyy+116xxxyx-108xxxyy-159xxyxy+109xxyyy-142xyxxy-140xyxyx+26xyxyy+20xyyxy+92xyyyy-76yxxxy+127yxxyx+77yxxyy-62yxyxy+56yxyyy-16yyyyy+150xxxx+126xxxy-22xxyx-17xxyy+13xyxx-34xyxy-165xyyx-61xyyy-104yxxx-51yxxy+112yxyx-2yxyy-106yyxy-148yyyy-103xxx+34xxy-120xyx+16xyy-59yxx-49yxy-147yyx-90yyy+77xx+91xy-135yx-95yy-112x-21y-16\}$

Note that the original common tip, $xxyyy$ does not survive in any of the polynomials, after G is rewritten, as above. Note also, that the tips of the polynomials in this rewritten set have several overlaps.

A partial Gröbner basis of G, computed by *Opal*, under length-lex with $x > y$ is presented in Appendix A.

Chapter 4

Noncommutative Polly Cracker Cryptosystems

We are now ready to present some of our attempts at developing noncommutative Polly Cracker cryptosystems. For completeness, we summarize the generic system below:

Private Key: A Gröbner basis, $G = \{g_1, g_2, \ldots, g_t\}$ for a two-sided ideal, I, of a noncommutative algebra $K\langle X\rangle$ over a finite field, K.

Public Key: A set, $B = \left\{ q_r : q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij} \right\}_{r=1}^{s} \subset I$, chosen so that computing a Gröbner basis of $\langle B\rangle$ is infeasible.

Message Space: $M = \mathrm{NonTip}(I)$ or a subset of $\mathrm{NonTip}(I)$.

Encryption: $c = p + m$, where $m \in M$ is a message and $p = \sum_{i=1}^{s} \sum_{j=1}^{k_{ir}} F_{rij} q_i H_{rij}$ is a polynomial in $J = \langle B\rangle \subset I$.

Decryption: Reduction of c modulo G yields the message, m.

Although the private key can, in theory, be any finite set which is the Gröbner basis of an ideal in $K\langle x_1, x_2, \ldots, x_n\rangle$, we generally use a single polynomial, whose tip (under some order) contains no self-overlaps. This is due to practical considerations, some of which include minimizing the time required for decryption, and algorithmically developing public keys, consisting of sets that do not have finite Gröbner bases.

We note, also that not all instances of ideals that do not have finite Gröbner bases are useful as public keys in a Polly Cracker cryptosystem. Any cryptosystem, for example, that uses a public key based on the class of ideals described in propositions 3.1.1 and 3.1.2 and corollary 3.2.1 would not be secure, in view of theorem 3.3, which provides techniques for realizing finite Gröbner bases in these instances. More generally, we believe that most principal ideals (even if they have no finite Gröbner basis) are not likely to lend themselves to the development of secure cryptosystems since the tips of the Gröbner bases of such ideals tend to be predictable and strictly growing, in the sense that the algorithm to find Gröbner bases of such ideals produces a sequence of polynomials: $g_1, g_2, g_3, \ldots$ such that $\mathrm{tip}(g_1) < \mathrm{tip}(g_2) < \mathrm{tip}(g_3) \ldots$

4.1 Cryptosystems That Use Public Keys Based On Proposition 3.4.1:

In proposition 3.4.1, we showed that the ideal given by $I = \langle g_1, g_2 \rangle \subset K\langle x, y, z \rangle$, where $g_1 = xzy + yz$ and $g_2 = yzx + zy$, does not have a finite Gröbner basis under any order. Our first serious attempts at developing a noncommutative Polly Cracker system were based on this result. Before describing our attempts and providing examples, we note that although our proof of proposition 3.4.1 used a sequence of polynomials whose tips were predictable and strictly increasing, in reality, the Gröbner basis for I contains many such sequences (unlike the situation with principal ideals, which we mentioned earlier). Some of the sequences that we discovered in the Gröbner basis for I, under length-lex with $x > y$ are:

1. $x\,(zx)^{n-1}\,z^{n+1}y - yz^n x\,(zx)^{n-1} \;\; n \geq 1$
2. $yz^n x\,(zx)^{n-1} + (xz)^{n-1}\,z^n y, \;\; n > 1$
3. $zyzy^{n-1}x + y^{n-2}yzzy, \;\; n > 1$
4. $yz^{n+1}yzy - zyzyyz^n, \;\; n \geq 1$
5. $xz^{n+2}yzy + yzzyz^{n+1}, \;\; n \geq 1$
6. $zyzy\,(yzz)^n\,x + (yzz)^n\,yzzy, \;\; n \geq 1.$
7. $xy^n zzy - yzzy^n x, \;\; n \geq 1$
8. $yzzyx^n zx + x^n yzzy, \;\; n \geq 1$
9. $zyzyyz^{n+1}x + yz^{n+1}yzzy, \;\; n \geq 1$
10. $zyzzyzy^n x + yzy^n x + yzy^{n+1}zzy, \;\; n \geq 1$
11. $yzzy^n xzx + xy^n zzzy, \;\; n > 2$
12. $zyzy^{n+1}zzx + y^n zzyzzy, \;\; n \geq 2$
13. $zyzyyzzy^n x + yzzy^{n+1}zzy, \;\; n \geq 1.$

While studying partial Gröbner bases computed using *Opal*, we found new patterns, such as those listed above, emerging as we increased the parameters of the computation. In fact, we found numerous instances in which the length of the tip of an element computed in the partial Gröbner basis was smaller than that of the element computed in the preceding step. This suggested that the current line of enquiry was, indeed, a promising one.

To construct a public key for a Polly Cracker cryptosystem based on proposition 3.4.1, we begin by picking a polynomial $g \in K\langle x, y, z\rangle$, whose tip has no self-overlaps (under some order $>$). Then $\{g\}$ is the private key. Next, suppose $f, h \in K\langle x, y, z\rangle$ are such that $\text{tip}(f),\ \text{tip}(h)$ have no self-overlaps, and in addition, $\text{tip}(f) \cdot \text{tip}(g) \cdot \text{tip}(h)$, and $\text{tip}(h) \cdot \text{tip}(g) \cdot \text{tip}(f)$ have no self-overlaps. Set $q_1 = fgh + hg$ and $q_2 = hgf + gh$. Then $\{q_1, q_2\}$ is the public key.

The message space consists of elements of $\text{NonTip}(\langle g\rangle)$ and varies depending on the private key used.

Example 4.1.1:- Let $f = x - a,\ g = z - c,\ h = y - b$, where $a, b, c \in K$ are constants. Set $g = z - c$ as the private key.
Let $q_1 = fgh + hg = xzy - azy - cxy - bxz + yz + bcx + (ac - c)y + (ab - b)z + (bc - abc)$ and $q_2 = hgf + gh = yzx - bzx - cyx - ayz + zy + bcx + (ab - b)z + (ac - c)y + (bc - abc)$. Set $B = \{q_1, q_2\}$ as the public key.

By proposition 3.4.1 (or a variation mentioned in one of the remarks following the proposition), $\langle\{q_1, q_2\}\rangle$ does not have a finite Gröbner basis.

Since $\text{tip}(g) = z$, it is clear that $x, y \notin \text{Tip}(\langle g\rangle)$. So the message space, M, could consist of all polynomials that contain no z-terms. i.e. $M = K\langle x, y\rangle$.

To encrypt a message, $m \in M$, we use polynomials $F_1, F_2, H_1, H_2 \in K\langle x, y, z\rangle$. The ciphertext, c, is written as $c = F_1 q_1 H_1 + F_2 q_2 H_2 + m$.

In theory, F_1, F_2, H_1, H_2 can be arbitrary polynomials in $K\langle x, y, z\rangle$. In practice, however, unless $\text{tip}(c)$ is fairly large, c can be reduced (correctly) using the public key, $B = \{q_1, q_2\}$, and even in the case where $\text{tip}(c)$ is large, reduction may be achieved using a partial Gröbner basis.

In view of the observation made in the last paragraph, we studied several techniques of finding polynomials, F_1, F_2, H_1, H_2 so that the ciphertext polynomial, c, cannot be reduced (correctly) using the public key, $B = \{q_1, q_2\}$.

1. Find polynomials F_1, F_2, H_1, H_2 such that $\text{tip}(c)$ is of the form $x\,(zyzx)^n\,(zy)^k$ or $(yz)^k\,(xzyz)^n\,x$ for some $n \in \mathbb{N},\ k = 1$ or 2. Say, for example, $F_1 = yzxzyz$+smaller terms, $H_1 = zxzyzx$+smaller terms, $F_2 = xzyzxz$+smaller terms and $H_2 = zyzx$+smaller terms. Then, $c = yzxzyzxzyzxzyzx + xzyzxzyzxzyzx +$ smaller terms.

While this approach ensures that $B = \{q_1, q_2\}$ does not (correctly) reduce c, in most cases, we found that the polynomial obtained by reducing c with respect to $\{q_1, q_2\}$ is often a monomial multiple of an element of the Gröbner basis, and can easily be reduced if the cryptanalyst has the ability to compute a partial Gröbner basis. This leads us to the next technique:

2. In this approach, we extend the existing public key, $\{q_1, q_2\}$ by adding selected elements of a partial Gröbner basis, so that the public key, Q, consists of a finite set of polynomials, $\{q_1, q_2, \ldots, q_r\},\ r > 2$. The elements, $q_2, q_3, \ldots, q_r$ of the public key are carefully selected, so that their tips have "overlapping overlaps". i.e. for each $q_i \in Q,\ i \geq 3$ with $\text{tip}(q_i) = T_i$, there exist $q_j, q_k \in Q$ with $\text{tip}(q_j) = T_j$ and $\text{tip}(q_k) = T_k$ such that $T_i = W_1W_2W_3$, $T_j = W_2W_3W_4$, $T_k = W_3W_4W_5$, where W_1, W_2, W_3, W_4, W_5 are monomials in x, y, z.

For example, if we refer to the partial Gröbner basis, some of whose elements are listed earlier in this section, we could select $q_i = yzzxzx + xzzzy$, $q_j = xzxzzzy - yzzzxzx$, and $q_k = xzzzyzy + yzzyzz$. Then, $W_1 = yzz,\ W_2 = xz,\ W_3 = x,\ W_4 = zzzy, W_5 = zy$ satisfy the required conditions.

To encrypt a message, m, we create a ciphertext polynomial, c as follows:
Choose arbitrary constants $\alpha, \beta \in K$, and
set $c = \alpha q_i W_4W_5 + \beta W_1 q_j W_5 - (\alpha + \beta)W_1W_2q_k + m$.

This ensures that the tips of the polynomials q_i, q_j, q_k are subtracted off in c, and reduction by the public key, $Q = \{q_1, q_2, \ldots, q_r\}$ does not yield the message, m. However, it leaves us in the same vulnerable position as the previous technique, in the event that the cryptanalyst is able to compute a partial Gröbner basis. While using polynomials, $q_1, q_2, \ldots, q_r$ with a greater number of "overlapping overlaps" might increase the amount of time (and resources) required by the cryptanalyst to find m, it does not provide absolute security.

3. In the final technique that we present, we use q_1, q_2 to create a set of polynomials, $Q = \{F_1, F_2, \ldots, F_t\} \subset J = \langle q_1, q_2 \rangle$, all of which have the same tip, T. We then set Q as the public key.

To encrypt a message, m, we choose arbitrary constants, $\alpha_1, \alpha_2, \ldots, \alpha_t \in K$ (not all of which are zero), such that $\sum_{i=1}^{t} \alpha_i = 0$. The ciphertext polynomial, c, is then written as $c = \sum_{i=1}^{t} \alpha_i \cdot F_i + m$.

As in the previous technique that we discussed, the tip of the F_i's used is subtracted off in c, and the message m, cannot be obtained by reducing c with respect to the public key, Q. This technique, however, does once again, leave the message vulnerable against a cryptanalyst who has the ability to compute a partial Gröbner basis of $\langle Q \rangle$ or even the ability to re-write Q in its "tip-reduced" form.

Other variations of this technique include writing c as:

$$c = \alpha_1(F_1 - F_2) + (\alpha_1 + \alpha_2)F_2 + \alpha_3 F_3 + \cdots + \alpha_t F_t + m \quad \text{or}$$
$$c = \alpha_1(F_1 - F_2) + (\alpha_1 + \alpha_2)F_2 + \alpha_3 F_3 + \cdots + \left(\sum_{i=1}^{t} \alpha_i\right)(F_t - F_{t-1}) + m.$$

However, neither of these variations provides any additional security.

It was the study of this technique, however, that led us to the study of cryptosystems based on conjecture 3.5, which we discuss in section 4.2. Before we get to those, we take a moment to discuss a cryptosystem based on corollary 3.4.2:

A cryptosystem based on corollary 3.4.2:

Let K be a finite field, $K\langle x_1, x_2, \ldots, x_6 \rangle$ be the free algebra over K in six non-commuting variables. Let $Z = \prod_{i=1}^{6} x_i$ and $c_0, c_1, \ldots, c_6 \in K - \{0\}$ be arbitrary constants. Set $g = Z + \sum_{i=1}^{6} c_i x_i + c_0 \in K\langle x_1, x_2, \ldots, x_6 \rangle$ as the private key. We develop the public key as follows:

Let $X = x_1 \cdot \prod_{i=2}^{5} \rho(x_i) \cdot x_6$, $Y = x_1 \cdot \prod_{i=2}^{5} \sigma(x_i) \cdot x_6$, where ρ, σ are distinct, nontrivial permutations of $\{x_2, x_3, x_4, x_5\}$. Let $a_0, a_1, \ldots, a_6, b_0, b_1, \ldots, b_6 \in K$ be nonzero constants and set $f = X + \sum_{i=1}^{6} a_i x_i + a_0$, $h = Y + \sum_{i=1}^{6} b_i x_i + b_0 \ \in K\langle x_1, x_2, \ldots, x_6 \rangle$. Then, by corollary 3.4.2, $J = \langle q_1, q_2 \rangle$, where $q_1 = fgh + hg$, $q_2 = hgf + gh$ does not have a finite Gröbner basis under any admissible order. Set $B = \{q_1, q_2\}$ as the public key.

In this setting, the message space, $M \subseteq \text{NonTip}(\langle g \rangle)$ could consist of all linear polynomials in $K\langle x_1, x_2, \ldots, x_6 \rangle$.

Encryption may be achieved by any of the three techniques presented earlier, for cryptosystems based on proposition 3.4.2 (with modification of the public key, as appropriate). We note, however, that *Opal* was unable to produce a partial Gröbner basis for J after running for twenty-four hours or more. So the second technique that was discussed for cryptosystems based on proposition 3.4.2 may not be practical. On the other hand, the inability of *Opal* to produce a partial Gröbner basis makes this cryptosystem more promising and worthy of further investigation.

4.2 Cryptosystems That Use Public Keys Based On Conjecture 3.5:

Our final cryptosystem, which is based on conjecture 3.5, appears to be successful.

Let K be a finite field, $K\langle x_1, x_2, \ldots, x_n \rangle$ the noncommutative free algebra in n variables (over K). Let W be a word that has no self-overlaps, and contains all the variables, $x_1, x_2, \ldots, x_n$.

Let $g = W + \sum_{i=1}^{n} a_i x_i + a_0 \ \in K\langle x_1, x_2, \ldots, x_n \rangle$, where $a_0, a_1, \ldots, a_n \in K - \{0\}$ are arbitrary constants. Since W contains all the variables, it is clear that $\text{tip}(g) = W$ under any admissible order. Also, since W contains no self-overlaps, $\{g\}$ is a Gröbner basis of $\langle g \rangle$ (under any order). We set g as the private key.

The public key, B, consists of a finite number (say t) of polynomials, $q_i = f_i g h_i$, where $f_i,\ h_i \in K\langle x_1, x_2, \ldots, x_n \rangle,\ i = 1, 2, \ldots, t$ are such that:

(1) Each f_i has the same tip, say $\text{tip}(f_i) = W_F \ \forall\ i = 1, 2, \ldots, t$

(2) Each h_i has the same tip, say $\text{tip}(h_i) = W_H \ \forall\ i = 1, 2, \ldots, t$

(3) The f_i contain a sufficient number of words of length $l(W_F)$ and $l(W_F) - 1$ and the h_i contain a sufficient number of words of length $l(W_H)$ and $l(W_H) - 1$ so that the number, N, of words of length $l(W_F \cdot W \cdot W_H) - 1$ that occur in the q_i's is approximately equal to one-third and strictly less than half the number of possible words of length $l(W_F \cdot W \cdot W_H) - 1$, and

(4) The number t of the q_i's is approximately $\frac{1}{2}N$.

We note that conditions (1) and (2) on the choice of the f_i's and h_i's ensure that all the q_i's have the same tip, $T = W_F \cdot W \cdot W_H$, and that together with conditions (3) and (4), this ensures that $B = \{q_1, q_2, \ldots, q_t\}$ satisfies the hypothesis of conjecture 3.5. So it is reasonable to believe that $J = \langle B \rangle$ does not have a finite Gröbner basis.

The message space, $M \subseteq \text{NonTip}\left(\langle g \rangle\right)$ could consist of all possible linear polynomials. Alternatively, since $W = \text{tip}(g)$ contains all the variables, and $\{g\}$ is a Gröbner basis of $\langle g \rangle$, it is clear that $\langle g \rangle$ cannot contain any polynomial that is homogeneous in one of the variables. So we could set M to be the set of all homogeneous polynomials of degree $\leq D$ for some $D \in \mathbb{N}$.

We studied two methods of encryption:

1. Choose arbitrary constants, $\beta_1, \beta_2, \ldots, \beta_{t-1} \in K$ (not all of which are zero). Next, set $\beta_t = -(\beta_1 + \beta_2 + \cdots + \beta_{t-1})$, so that $\sum_{i=1}^{t} \beta_i = 0$. To encrypt a message, $m \in M$, we construct a ciphertext polynomial, $c = \sum_{i=1}^{t} \beta_i q_i + m$. Since $\sum_{i=1}^{t} \beta_i = 0$, it is clear that $\mathrm{tip}(c) < T$, and it is reasonable to believe that reduction by the public key, $B = \{q_1, q_2, \ldots, q_t\}$, would not yield the message m. However, as we found in cases where t is relatively small, *Opal* was able to correctly reduce c, using the set $B = \{q_1, q_2, \ldots, q_t\}$. This is due to the fact that *Opal* is designed to reduce the tip of any set that it stores. This method of encryption is thus rendered insecure.

2. To encrypt a message, m, choose arbitrary polynomials $F_i, H_i \in K\langle x_1, x_2, \ldots, x_n\rangle$ such that $\mathrm{tip}(F_i) \cdot \mathrm{tip}(H_i) \geq T \ \forall \ i = 1, 2, \ldots, t$, and construct the ciphertext polynomial, $c = \sum_{i=1}^{t} F_i q_i H_i + m$.

As is predicted by (noncommutative) Gröbner basis theory, attempts at reducing c by the public key, $B = \{q_1, q_2, \ldots, q_t\}$, results in a remainder that has more terms than the original ciphertext. In the case where $n = 2$ or 3, the same is true, even when reducing c be a partial Gröbner basis. For some examples with $n = 3$, *Opal* was unable to compute a partial Gröbner basis , after running for over twenty-four hours.

Example 4.2:- Let $K = \mathbb{Z}_{331}$, the field of residue classes of integers modulo 331 and consider $K\langle x, y\rangle = \mathbb{Z}_{331}\langle x, y\rangle$.

Let $g = xy + 7x + 13y + 11 \in K\langle x, y\rangle$ be the private key.

Let $f_1 = xx + 170xy + 295yx + 61x + y + 274,\ h_1 = yy + 116x + 133y + 9$

$f_2 = xx + 248xy + 182yx + 316x + 17y + 1,\ h_2 = yy + 196x + 128y - 232$

$f_3 = xx + 9xy + 83yx + 94x + 282y + 177,\ h_3 = yy + 252x + 83y + 44$

$f_4 = xx + 105xy + 40yx + 23x + 219y + 47,\ h_4 = yy + 73x + 7y + 38$

$f_5 = xx + 93xy + 176yx + 301x + 58y + 302,\ h_5 = yy + 75x + 181y + 43.$

Then, we have:

$q_1 = f_1 g h_1 = xxxyyy - 161xyxyyy - 36yxxyyy + 116xxxyx + 140xxxyy + 74xxyyy - 140xyxyx - 32xyxyy - 107xyyyy + 127yxxyx - 75yxxyy - 136yxyyy + 150xxxx - 53xxxy - 22xxyx + 19xxyy + 13xyxx - 73xyxy - 165xyyx - 40xyyy - 104yxxx - 78yxxy + 112yxyx + 59yxyy + 13yyyy - 103xxx + 2xxy - 120xyx + 12xyy - 59yxx - 1yxy - 147yyx + 6yyy + 77xx + 50xy - 135yx + 45yy - 112x + 71y - 16,$

$q_2 = f_2gh_2 = xxxyyy - 83xyxyyy - 149yxxyyy - 135xxxyx + 135xxxyy - 2xxyyy - 49xyxyx + 49xyxyy - 86xyyyy - 76yxxyx + 76yxxyy + 66yxyyy + 48xxxx + 2xxxy - 61xxyx - 19xxyy - 12xyxx + 165xyxy + 25xyyx + 132xyyy + 130yxxx + 33yxxy + 27yxyx - 23yxyy - 110yyyy + 143xxx + 17xxy - 92xyx - 94xyy - 5yxx - 18yxy - 45yyx + 22yyy + 108xx - 65xy - 64yx + 157yy + 85x + 24y + 96$

$q_3 = f_3gh_3 = xxxyyy + 9xyxyyy + 83yxxyyy - 79xxxyx + 90xxxyy + 107xxyyy - 49xyxyx + 148xyxyy + 117xyyyy + 63yxxyx - 143yxxyy + 37yxyyy + 109xxxx - 37xxxy + 153xxyx - 49xxyy - 12xyxx - 2xyxy + 25xyyx - 45xyyy + 110yxxx - 92yxxy + 56yxyx + 25yyyy + 86xxx - 7xxy - 51xyx + 17xyy + 63yxx - 50yxy + 11yyx - 135yyy + 143xx + 32xy + 77yx + 12yy + 152x + 147y - 61$

$q_4 = f_4gh_4 = xxxyyy + 105xyxyyy + 40yxxyyy + 73xxxyx + 14xxxyy + 36xxyyy + 52xyxyx + 146xyxyy + 41xyyyy - 59yxxyx - 102yxxyy + 77yxyyy - 151xxxx + 87xxxy - 20xxyx + 93xxyy + 33xyxx - 133xyxy + 14xyyx + 133xyyy - 82yxxx - 161yxxy - 6yxyx - 136yxyy - 132yyyy - 87xxx - 76xxy + 138xyx + 69xyy + 92yxx - 144yxy - 37yyx + 110yyy + 34xx - 123xy - 149yx + 91yy - 54x - 119y + 117$

$q_5 = f_5gh_5 = xxxyyy + 93xyxyyy - 155yxxyyy + 75xxxyx - 143xxxyy - 17xxyyy + 24xyxyx - 59xyxyy - 115xyyyy - 40yxxyx - 12yxxyy + 29yxyyy - 137xxxx - 14xxxy + 49xxyx + 34xxyy - 163xyxx + 22xyxy - 19xyyx - 20xyyy + 51yxxx - 147yxxy - 142yxyx - 22yxyy + 92yyyy - 60xxx - 9xxy + 142xyx - 88xyy - 95yxx + 145yxy - 51yyx + 32yyy + 125xx + 2xy + 128yx - 96yy + 158x + 155y - 146$

Set $B = \{q_1, q_2, q_3, q_4, q_5\}$ as the public key. Note that this is the same set described in example 3.5.2.

To encrypt a message, we create a polynomial, p, as follows:

Let $F_1 = xxx - 98,\ H_1 = yyy + 97$

$F_2 = xxx + 79,\ H_2 = yyy + 9$

$F_3 = xxx + 1,\ H_3 = yyy - 5$

$F_4 = xxx + 59,\ H_4 = yyy - 160$

$F_5 = xxx + 47,\ H_5 = yyy + 33$

Then, $p = F_1q_1H_1 + F_2q_2H_2 + F_3q_3H_3 + F_4q_4H_4 + F_5q_5H_5$ has 130 terms and any attempt to reduce p by the public key, B, yields a remainder with approximately 668 terms. So a message, m, that is encrypted as $c = p + m$ cannot be found by reducing c with respect to the public key. In fact the number of terms in the remainder obtained from such a reduction has roughly five times as many terms as the original ciphertext polynomial. Furthermore, reducing p by a partial Gröbner basis of $\langle B \rangle$ increases the number of terms in the remainder by roughly ten times the number of terms in p to 1353.

Complete data from this example are given in Appendix A.

Chapter 5

Constructing A Secure System

In the design of noncommutative Polly Cracker cryptosystems, which we presented in chapter 4, we considered the possibility that a cryptanalyst might be able to compute a partial Gröbner basis of the ideal generated by the public key, and (correctly) reduce the ciphertext polynomial by using this partial Gröbner basis. In this chapter, we consider two other security issues that arise in the development of a noncommutative Polly Cracker cryptosystem and present ways to defeat them in the cases of the examples that we studied in the previous chapter. The first deals with constructing a public key that adequately conceals the private key, while the second deals with the construction of ciphertext that is not susceptible to linear algebra type attacks.

5.1 Constructing Public Keys That Conceal The Private Key:

In this section, we consider the possibility that an analysis of the coefficients of the polynomials in the public key of a noncommutative Polly Cracker cryptosystem might reveal information about the private key. We study this possibility for each of the systems that were presented in chapter 4.

5.1.1 Cryptosystems with public keys based on proposition 3.4.1:

In example 4.1.1, we presented a cryptosystem whose public key is based on proposition 3.4.1. We begin by studying the public key of this system, to see whether it reveals any information about the private key. Recall that in this system, we have the following:
Private key: $g = z - c \in K\langle x, y, z\rangle$, where $c \in K$.
Public key: Let $f = x - a,\ h = y - b \in K\langle x, y, z\rangle$, where $a, b \in K$.
Let $q_1 = fgh + hg = xzy - azy - cxy - bxz + yz + bcx + (ac - c)y + (ab - b)z + (bc - abc)$ and $q_2 = hgf + gh = yzx - bzx - cyx - ayz + zy + bcx + (ab - b)z + (ac - c)y + (bc - abc)$. Then $B = \{q_1, q_2\}$ is the public key.
Message Space: $M = K\langle x, y\rangle$.

Note that the constant, c, shows up as the coefficient of xy in q_1 (and also as the coefficient of yx in q_2). Furthermore, since $M = K\langle x, y\rangle$, it is clear (to anyone who is familiar with the basic design of the system) that the variable used in the private key is z. It is easy to conclude from this, that the private key is $z - c$.

One way of plugging this hole, in the security of this system, might be to choose a more complex polynomial as the private key, or to choose more complex polynomials f and h in the construction of the public key. However, as we will see when we consider the cryptosystem based on corollary 3.4.2, choosing a more complex polynomial as the private key does not, in itself, guarantee security against this type of attack. We do, however, have the following modification, which makes the system more secure against this type of attack:

Private key: Let $g_1 = z - c,\ g_2 = w - d \in K\langle x, y, z, w\rangle$, where $c,\ d \in K$.

Set $\{g_1, g_2\}$ as the private key.

Public key: Let $q_1 = xg_1y + xg_2y + yg_1 + yg_2 + g_1 + g_2$

$= xzy + xwy - (c+d)xy + yz + yw - (c+d)y + z + w - (c+d)$,

and $q_2 = yg_1x + yg_2x + g_1y + g_2y + g_1 + g_2$

$= yzx + ywx - (c+d)yx + zy + wy - (c+d)y + z + w - (c+d)$.

Set $B = \{q_1, q_2\}$ is the public key.

Since the coefficients of q_1 and q_2 yield only one equation in the two variables, c and d, we believe that the private key is fairly well concealed in this system. In addition, based on remark 1(b) after proposition 3.4.1, we have reason to believe that $\langle B\rangle$ does not have a finite Gröbner basis. We note, also, that although this system deviates from our norm in that the private key contains more than one polynomial, we can still achieve fast decryption by evaluating the ciphertext polynomial at $z = c,\ w = d$.

However, this system is still vulnerable to an attack by a cryptanalyst who can compute a partial Gröbner basis of $\langle B\rangle$. Even increasing the number of variables, and the number of polynomials in the private key does not increase the security in this respect.

5.1.2 Cryptosystems with public keys based on corollary 3.4.2:

We now turn our attention to cryptosystems whose public keys are based on corollary 3.4.2. Recall that we presented one such system in section 4.1. In this system, we have a finite field, K, and $K\langle x_1, x_2, \ldots, x_6\rangle$ is the noncommutative free algebra (over K) in six variables. Z is the word $\prod_{i=1}^{6} x_i$, and $X,\ Y$ are the words defined by $X = x_1 \cdot \prod_{i=2}^{5} \rho(x_i) \cdot x_6,\ Y = x_1 \cdot \prod_{i=2}^{5} \sigma(x_i) \cdot x_6$, where ρ, σ are distinct, nontrivial permutations of $\{x_2, x_3, x_4, x_5\}$.

In this setting, we have the following:

Private key: $g = Z + \sum_{i=1}^{6} c_i x_i + c_0 \in K\langle x_1, x_2, \ldots, x_6 \rangle$, where $c_0, c_1, \ldots, c_6 \in K - \{0\}$ are arbitrary constants.

Public key: Let $f = X + \sum_{i=1}^{6} a_i x_i + a_0,\ h = Y + \sum_{i=1}^{6} b_i x_i + b_0 \ \in K\langle x_1, x_2, \ldots, x_6 \rangle$, where $a_0, a_1, \ldots, a_6, b_0, b_1, \ldots, b_6 \in K - \{0\}$ are arbitrary constants.
Let $q_1 = fgh + hg$ and $q_2 = hgf + gh$.
Then $B = \{q_1, q_2\}$ is the public key.

We note that the polynomials $f,\ g,\ h$ used in the construction of this system are substantially more complex than those used in the construction of example 4.1.1. However, it is just as easy to find the private key from the publicly known information:

Consider $q_1 = fgh + hg = XZY + \underbrace{a_0 ZY + b_0 XZ + c_0 XY}_{\text{terms of length 12}}$
$+ \underbrace{\sum_{i=1}^{6} a_i x_i ZY + \sum_{i=1}^{6} c_i X x_i Y + \sum_{i=1}^{6} b_i XZ x_i}_{\text{terms of length 13}} +$ terms of length less than 12.

By examining $\text{tip}(q_1) = XZY$, a cryptanalyst who is familiar with the construction of this cryptosystem can easily determine $\text{tip}(g) = Z$ to be the tip of the private key, as well as $\text{tip}(f) = X$ and $\text{tip}(h) = Y$. Once X, Y and Z are known, the constants $c_1, c_2, \ldots, c_6$ can be found by looking at the coefficients of $X x_i Y\ \forall\ i = 1, 2, \ldots, 6$, and c_0 can be determined by looking at the coefficient of XY.

One simple way to defeat this type of attack on this cryptosystem is to avoid the use of monic polynomials in the construction of the public key. i.e. suppose $\alpha,\ \beta,\ \gamma \in K$ are non-zero constants. Set $g = \gamma Z + \sum_{i=1}^{6} c_i x_i + c_0$ as the private key. To construct the public key, use polynomials $f = \alpha X + \sum_{i=1}^{6} a_i x_i + a_0$ and $h = \beta Y + \sum_{i=1}^{6} b_i x_i + b_0$. Set $B = \{q_1, q_2\}$ is the public key, where $q_1 = fgh + hg,\ q_2 = hgf + gh$.

In this modified version of the system, we have:

$$q_1 = (\alpha\beta\gamma)XZY + \underbrace{\sum_{i=1}^{6}(a_i\gamma\beta)x_iZY + \sum_{i=1}^{6}(c_i\alpha\beta)Xx_iY + \sum_{i=1}^{6}(b_i\alpha\gamma)XZx_i}_{\text{terms of length 13}}$$
$$+\underbrace{(a_0\gamma\beta)ZY + (b_0\alpha\gamma)XZ + (c_0\alpha\beta)XY}_{\text{terms of length 12}} + \text{terms of length less than 12.}$$

It is clear that the constant $c_0, c_1, \ldots, c_6$ are concealed in q_1, and even if a cryptanalyst were to set up a system of equations with the constants $\alpha,\ \beta,\ \gamma,\ a_i,\ b_i, c_i$ $(i = 1, 2, \ldots, 6)$ as unknowns, it would at best be a system of cubic equations for which there are no known methods of solution. We note, also, that the coefficients of the bigger terms of q_2 are identical to those of similar terms of q_1, so looking at the coefficients of q_2 does not provide any additional information.

This technique of concealing the private key is presented in greater detail when we discuss the cryptosystems based on conjecture 3.5, which we do next.

5.1.3 Cryptosystems with public keys based on conjecture 3.5:

In studying this security issue for cryptosystems whose public key is based on conjecture 3.5, we note that given the complex nature of the public keys generated in these systems, it may not, in general, be possible to determine the private key unless a lot of information is publicly known. However, as in the case of the system based on corollary 3.4.2, it is best to avoid the use of monic polynomials. We present one situation, in which we show how the security is compromised by the use of monic polynomials, and how to guard against this security breach.

Recall that in example 4.2, our private key had the form $g = xy + \alpha x + \beta y + \gamma$, where $\alpha, \beta, \gamma \in K$ are non-zero constants. Suppose that this is always the case, and that the security of the system comes from the secrecy of the constants α, β and γ. Suppose, in addition that the polynomials, $f,\ h$ that we use in the construction of the public key are of the form $f = x^2 + axy + byx + cx + dy + e$ and $h = y^2 + mx + ny + k$, where $a, b, c, d, e, m, n, k \in K$ are nonzero constants. Suppose also, that it is publicly known that the $f,\ h$ are of this form (note that we are dropping the subscripts i, for notational convenience). Then the first few terms of an element $q = fgh$ of the public key are:

$q = x^3y^3 + mx^3yx + (n+\alpha)x^3y^2 + (\beta + c)x^2y^3 + \alpha mx^4 + (k + \alpha n)x^3y + (\beta m + cm)x^2yx + (\beta n + \gamma + cn + c\alpha)x^2y^2 + (\alpha k + \gamma m + c\alpha m)x^3 + (\beta k + n + ck + c\alpha n)x^2y + (\gamma k + c\alpha k + e\alpha m)x^2 + axyxy^3 + amxyxy + a(n+\alpha)xyxy^2 + a\beta xy^4 + \ldots$

A cryptanalyst who is familiar with the construction of this public key, as well as the field K, which is presumed to be publicly known, can use the coefficients of these terms to find α, β and γ by the following steps:

1. The coefficients of x^3yx and $xyxy^3$ give us m and a respectively.
2. Use the term $\alpha m x^4$ and the knowledge of m to find α.
3. Use the term $a\beta xy^4$ and the knowledge of a to find β.
4. Use the term $(n+\alpha)x^3y^2$ and the knowledge of α to find n.
5. Use $(\beta+c)x^2y^3$ and β to find c.
6. Use $(k+\alpha n)x^3y$ and α and n to find k.
7. Use coefficient of x^3 and α, k, c, m to find γ.

Suppose, on the other hand, the polynomials used in the construction of q are not monic, say for example, we set $g = \alpha xy + \beta x + \gamma y + \delta$ as the private key, and suppose we set $f = ax^2 + bxy + cyx + dx + ey + u$ and $h = my^2 + nx + ky + l$, where $a, b, c, d, e, u, m, n, k, l, \alpha, \beta, \gamma, \delta \in K$ are non-zero constants. Then,

$q = fgh$

$= (a\alpha m)x^3y^3 + (a\alpha n)x^3yx + (a\alpha k + a\beta m)x^3y^2 + (a\alpha l + a\beta k)x^3y + (a\beta n)x^4 + (a\beta l + a\delta n + d\beta n)x^3 + (a\beta m + d\alpha m)x^2y^3 + (a\beta k + d\alpha k + ma\delta + md\beta)x^2y^2 + (a\beta l + d\alpha l + a\delta k + d\beta k)x^2y + (\alpha bm)xyxy^3 + (a\delta l + d\beta l + d\delta n + u\beta n)x^2 + (\alpha bn)xyxyx + (\alpha bk + b\beta m)xyxy^2 + (\alpha bl + b\beta k)xyxy + (b\beta n)xyx^2 + (b\beta l + d\gamma n + b\delta n + u\alpha n)xyx + (b\gamma m)xy^4 + (b\gamma n)xy^2x + (c\alpha m)yx^2y^3 + [b\gamma k + (d\gamma + b\delta + u\alpha)m]xy^3 + (c\alpha n)yx^2yx + (b\gamma l + d\gamma k + b\delta k + u\alpha k + d\delta m + u\beta m)xy^2 + (ld\gamma + b\delta l + u\alpha l + d\delta k + u\beta k)xy + (c\alpha l + c\beta k)yx^2y + (c\alpha k + c\beta m)yx^2y^2 + (c\beta n)yx^3 + (c\beta l + c\delta n + e\beta n)yx^2 + (c\gamma m + e\alpha m)yxy^3 + (c\gamma n + e\alpha n)yxyx + (e\gamma m)y^4 + (c\gamma k + e\alpha k + c\delta m + e\beta m)yxy^2 + (c\gamma l + e\alpha l + c\delta k + e\beta k)yxy + (c\delta l + e\beta l + e\delta n + u\gamma n)yx + (e\gamma n)y^2x + (e\gamma k + e\delta m + u\gamma m)y^3 + (e\gamma l + e\delta k + u\delta m + u\gamma k)y^2 + (d\delta l + u\beta l + u\delta n)x + (e\delta l + u\gamma l + u\delta k)y + u\delta l.$

In order to use the coefficients of q to find α, β, γ and δ, a cryptanalyst would have to solve a system of cubic equations with $a, b, c, d, e, u, m, n, k, l, \alpha, \beta, \gamma$ and δ as the unknowns. Since there are no known methods for solving such systems, it is reasonable to believe that the private key is adequately concealed by this construction of the public key.

There is one additional precaution that may help conceal the private key of a non-commutative Polly Cracker cryptosystem. We will discuss this precaution at the end of section 5.2.

5.2 Constructing Secure Ciphertext Polynomials:

As we mentioned in chapter 2, the noncommutative Polly Cracker cryptosystem does not appear to be susceptible to linear algebra attacks. This is due to the fact that encryption (in the noncommutative version) is achieved by $c = p+m$, where $\{q_j\}_{j=1}^{s}$ is the public key, $p = \sum_{i=1}^{s}\sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij}$, and m is the message. As a result, the coefficient of any monomial, W, that occurs in c is quadratic in the coefficients of F_{rij}, H_{rij}, $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, k_{ir}$. So if we treat the coefficients of F_{rij}, H_{rij}, $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, k_{ir}$, as unknowns, we get a non-linear system of equations, for which there are no known methods of solution.

However, we believe that a "linear algebra type" attack might be successful in the case of poorly constructed ciphertext. This attack, which we describe below, is a blend of the linear algebra attack on the commutative Polly Cracker cryptosystem and a failed cryptanalysis of Patarin's Little Dragon [Pa] that is described in Koblitz [Ko].

Let c be the ciphertext polynomial. Then $c = \sum_{i=1}^{s}\sum_{j=1}^{k_{ir}} F_{rij}q_iH_{rij} + m$ and the coefficient of any monomial, W, that occurs in c is quadratic in the coefficients of F_{rij}, H_{rij}, $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, k_{ir}$. Thus, by treating the coefficients of the polynomials F_{rij} and H_{rij}, $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, k_{ir}$ as unknowns, we get a system of quadratic equations. Now, the coefficient of any monomial, W, in c consists of sums of constants of the form $\alpha_i\gamma_j\beta_k$ and m_W, where α_i is the coefficient of a monomial that occurs in some F_{rij}, γ_j is the coefficient of a monomial that occurs in some q_i, β_k is the coefficient of a monomial that occurs in some H_{rij} and m_W is the coefficient of W in m. Next, we introduce new variables, δ_l, for all the products $\alpha_i\beta_k$ that appear in the coefficient of W. i.e. we replace each product of the form $\alpha_i\beta_k$ with a new variable, δ_l. This results in a system of linear equations in the variables δ_l and m_W. If the number of such equations equals (or exceeds) the number of such unknowns, it has a unique solution that can be determined using Gaussian elimination. Since the cryptanalyst is only interested in the coefficients of the terms that occur in m, solving this system of equations would serve his/her purpose.

In order to ensure that a noncommutative Polly Cracker cryptosystem is not vulnerable to such an attack, we need to ensure that the number of the products, $\alpha_i\beta_k$, that occur in c exceeds the number of such equations. Since each monomial in c contributes a set of equations, one way of ensuring this is to make k_{ir} sufficiently large for each i. In the case of the cryptosystem described in example 3.2, where $s = 5$, the number of monomials is 130, and for each r, i, j, $F_{rij} = \alpha_{rij} \cdot xxx - \alpha'_{rij}$, $H_{rij} = \beta_{rij} \cdot yyy - \beta'_{rij}$, where

$\alpha_{ri}, \alpha'_{rij}, \beta_{rij}, \beta'_{rij} \in K - \{0\}$, we would need to use $k_{ir} \geq 7$ for each i. We note that this secures the system against this type of attack even when the cryptanalyst knows the precise form of the polynomials F_{rij} and H_{rij} and all the monomials that could occur in p. However, in order to avoid specific cases that might leave the ciphertext vulnerable to a cryptanalyst, it is best to vary the form of F_{rij} and H_{rij}, as well as the value of k_{ir} for each i.

Before ending this chapter, we note that the technique that we suggest for securing against linear algebra type attacks may also be used to provide an additional layer of security in protecting the private key of noncommutative Polly Cracker cryptosystems. i.e. If $G = \{g_1, g_2, \ldots, g_t\}$ is the private key, let $q_r = \sum_{i=1}^{t} \sum_{j=1}^{d_{ir}} f_{rij} g_i h_{rij}$ be such that d_{ir} varies with i and is fairly large for most i. Set $\{q_r\}_{r=1}^{s}$ as the public key. This should secure virtually all noncommutative Polly Cracker cryptosystems from the type of attack described in section 5.1.

Chapter 6

Conclusions

6.1 Summary:

The main focus of this work was to explore the possibility of developing a provably secure public-key cryptosystem, whose security is based on the intractability of the ideal membership problem for a noncommutative algebra over a finite field. To do this, we proposed and studied a noncommutative analog of the Polly Cracker cryptosystem. Our motivation to study this system came from the fact that most ideals of a noncommutative free algebra over a finite field are believed to have infinite Gröbner bases under all admissible orders. In addition, unlike its commutative cousin, the noncommutative version appeared to be resistant to linear algebra attacks.

We began our work with a search for ideals that have infinite Gröbner bases. Although most ideals of a noncommutative free algebra over a finite field are believed to have infinite reduced Gröbner bases, proving this turned out to be a very difficult problem. We were, however, successful in our search, and were able to present classes of ideals whose reduced Gröbner basis is infinite under all admissible orders. There were also some surprising cases, in which we found ideals to have finite Gröbner bases where we did not expect them. We also studied techniques to realize finite Gröbner bases. Some of the ideals which had been proven to have infinite Gröbner bases succumbed to such techniques and could not be used in the development of a secure cryptosystem. These ideals are, nevertheless, of mathematical interest.

Next, we studied techniques for generating public keys based on each class of ideals which do not have finite Gröbner bases, and which do not succumb to a technique for realizing finite Gröbner bases. We also studied techniques for encrypting messages that cannot be decrypted using the publicly known information. After studying several such techniques, we were successful in that we were able to develop one cryptosystem that appears to work as we would like it to, and one which shows promise and is worthy of further investigation.

Finally, we put on the cryptanalyst's hat, and attempted to break our noncommutative Polly Cracker system without solving the ideal membership problem, on which its security is based. We showed how poorly constructed public keys can reveal enough information for a cryptanalyst to find the private key, rendering the entire system insecure. We also showed how a cryptanalyst might use a "linear algebra type" attack against poorly constructed

ciphertext. However, we were able to find ways to protect against both these methods of cryptanalysis and suggest ways of building a secure noncommutative Polly Cracker cryptosystem.

6.2 Potential for Further Investigation:

We believe that this work will stimulate further research in two directions. The first, more obvious direction, is in the implementation and further development of the noncommutative Polly Cracker cryptosystem. Some of the avenues for further work in this direction are:

1. Implementation: In order for any cryptosystem to be useful and practical, it needs to be coded and implemented.
2. Further Exploration: of the cryptosystem based on corollary 3.4.2, which as we mentioned earlier, appears to be secure and is worthy of further investigation. Also, there could be an exploration of additional techniques for generating secure public keys.
3. Digital Signatures: Digital signatures schemes, which can be based on most public-key cryptosystems, play an important role in authentication. The development of such a scheme was beyond the scope of this work. However, we believe that there is potential for the development of digital signature schemes based on the noncommutative Polly Cracker cryptosystem.
4. Benchmarking: We believe that there should be significant interest in benchmarking the complexity of the encryption and decryption schemes of the noncommutative Polly Cracker cryptosystem against those of RSA and other industry-standard cryptosystems.

A second, less obvious, direction in which this dissertation could stimulate research comes from the cryptanalysis of the noncommutative Polly Cracker system: Since the known methods of attack require the cryptanalyst to either solve a system of non-linear equations or to determine methods to realize finite Gröbner bases, attempts at breaking the system could lead to partial solutions to these problems, both of which are of independent interest to algebraists.

Appendix A

Complete Data From Some Examples

Example 3.5.2:- Let $K = \mathbb{Z}_{331},\ K\langle x,y\rangle = \mathbb{Z}_{331}\langle x,y\rangle$. Let $G = \{g_1, g_2, g_3, g_4, g_5\}$, where

$g_1 = xxyyy - 161xyxyyy - 36yxxyyy + 116xxxyx + 140xxxyy + 74xxyyy - 140xyxyx - 32xyxyy - 107xyyyy + 127yxxyx - 75yxxyy - 136yxyyy + 150xxxx - 53xxxy - 22xxyx + 19xxyy + 13xyxx - 73xyxy - 165xyyx - 40xyyy - 104yxxx - 78yxxy + 112yxyx + 59yxyy + 13yyyy - 103xxx + 2xxy - 120xyx + 12xyy - 59yxx - yxy - 147yyx + 6yyy + 77xx + 50xy - 135yx + 45yy - 112x + 71y - 16,$

$g_2 = xxyyy - 83xyxyyy - 149yxxyyy - 135xxxyx + 135xxxyy - 2xxyyy - 49xyxyx + 49xyxyy - 86xyyyy - 76yxxyx + 76yxxyy + 66yxyyy + 48xxxx + 2xxxy - 61xxyx - 19xxyy - 12xyxx + 165xyxy + 25xyyx + 132xyyy + 130yxxx + 33yxxy + 27yxyx - 23yxyy - 110yyyy + 143xxx + 17xxy - 92xyx - 94xyy - 5yxx - 18yxy - 45yyx + 22yyy + 108xx - 65xy - 64yx + 157yy + 85x + 24y + 96,$

$g_3 = xxyyy + 9xyxyyy + 83yxxyyy - 79xxxyx + 90xxxyy + 107xxyyy - 49xyxyx + 148xyxyy + 117xyyyy + 63yxxyx - 143yxxyy + 37yxyyy + 109xxxx - 37xxxy + 153xxyx - 49xxyy - 12xyxx - 2xyxy + 25xyyx - 45xyyy + 110yxxx - 92yxxy + 56yxyx + 25yyyy + 86xxx - 7xxy - 51xyx + 17xyy + 63yxx - 50yxy + 11yyx - 135yyy + 143xx + 32xy + 77yx + 12yy + 152x + 147y - 61,$

$g_4 = xxyyy + 105xyxyyy + 40yxxyyy + 73xxxyx + 14xxxyy + 36xxyyy + 52xyxyx + 146xyxyy + 41xyyyy - 59yxxyx - 102yxxyy + 77yxyyy - 151xxxx + 87xxxy - 20xxyx + 93xxyy + 33xyxx - 133xyxy + 14xyyx + 133xyyy - 82yxxx - 161yxxy - 6yxyx - 136yxyy - 132yyyy - 87xxx - 76xxy + 138xyx + 69xyy + 92yxx - 144yxy - 37yyx + 110yyy + 34xx - 123xy - 149yx + 91yy - 54x - 119y + 117,$

$g_5 = xxyyy + 93xyxyyy - 155yxxyyy + 75xxxyx - 143xxxyy - 17xxyyy + 24xyxyx - 59xyxyy - 115xyyyy - 40yxxyx - 12yxxyy + 29yxyyy - 137xxxx - 14xxxy + 49xxyx + 34xxyy - 163xyxx + 22xyxy - 19xyyx - 20xyyy + 51yxxx - 147yxxy - 142yxyx - 22yxyy + 92yyyy - 60xxx - 9xxy + 142xyx - 88xyy - 95yxx + 145yxy - 51yyx + 32yyy + 125xx + 2xy + 128yx - 96yy + 158x + 155y - 146.$

Here, after reducing the tips, G is rewritten as:

$\{78xyxyyy - 113yxxyyy + 80xxxyx - 5xxxyy - 76xxyyy + 91xyxyx + 81xyxyy + 21xyyyy + 128yxxyx + 151yxxyy - 129yxyyy - 102xxxx + 55xxxy - 39xxyx - 38xxyy - 25xyxx - 93xyxy - 141xyyx - 159xyyy - 97yxxx + 111yxxy - 85yxyx - 82yxyy - 123yyyy - 85xxx + 15xxy + 28xyx - 106xyy + 54yxx - 17yxy + 102yyx + 16yyy + 31xx - 115xy + 71yx + 112yy - 134x - 47y + 112,$

$-110yxxyyy + 55xxxyx - 107xxxyy - 39xxyyy + 3xyxyx - 22xyxyy + 5yxxyx - 134yxxyy - 106yxyyy + 54xxxx - 19xxxy - 71xxyx - 104xxyy + 21xyxx + 70xyxy + 39xyyx + 36xyyy + 35yxxx + 126yxxy - 32yxyx - 67yxyy - 118xxx + 162xxy - 9xyx - 78xyy - 123yxx + 22yxy + 63yyx - 91yyy - 44xx - 5xy - 104yx - 14yy - 72x + 136y - 26,$

$-13xxxyx - 114xxxyy + 35xxyyy - 10xyxyx - 126xyxyy + 138yxxyx + 133yxxyy + 121yxyyy - 91xxxx + 33xxxy + 72xxyx - 109xxyy - 70xyxx - 129xyxy - 130xyyx - 149xyyy - 27yxxx + 91yxxy - 2yxyx + 2yxyy - 82yyyy + 79xxx - 8xxy - 154xyx + 131xyy - 53yxx + 104yxy + 153yyx - 153yyy - 43xx - 100xy - 51yx - 72yy - 116x - 44y + 23,$

$116xxxyy + 86xxyyy - 153xyxyx + 46xyxyy + 30yxxyx + 165yxxyy - 10yxyyy - 29xxxy - 92xxyx - 88xxyy - 78xyxx - 108xyxy - 3xyyx + 86xyyy - 121yxxx - 89yxxy - 90yxyx - 95yxyy - 130yyyy + 89xxx - 127xxy + 110xyx + 119xyy - 153yxx + 125yxy + 49yyx + 140yyy - 71xx - 133xy - 59yx - 118yy - 122x + 21y + 80,$

$-132xxyyyy + 27xyxyxy + 84xyxyyy + 131yxxyxy - 143yxxyyy - 154yxyyyy + 116xxxyx - 108xxxyy - 159xxyxy + 109xxyyy - 142xyxxy - 140xyxyx + 26xyxyy + 20xyyxy + 92xyyyy - 76yxxxy + 127yxxyx + 77yxxyy - 62yxyxy + 56yxyyy - 16yyyyy + 150xxxx + 126xxxy - 22xxyx - 17xxyy + 13xyxx - 34xyxy - 165xyyx - 61xyyy - 104yxxx - 51yxxy + 112yxyx - 2yxyy - 106yyxy - 148yyyy - 103xxx + 34xxy - 120xyx + 16xyy - 59yxx - 49yxy - 147yyx - 90yyy + 77xx + 91xy - 135yx - 95yy - 112x - 21y - 16\}$

Note that the original common tip, $xxyyy$ does not survive in any of the polynomials, after G is rewritten, as above. Note also, that the tips of the in this rewritten set have several overlaps.

A partial Gröbner basis of $\langle G \rangle$, computed by *Opal*, under length-lex with $x > y$, is given below. Note that the last tip of the last relation computed by opal has a self-overlap, as well as overlaps with tips of the other relations. It is clear from this that the current set is not a complete Gröbner basis:

$\{xyxyyy - 98xxyyy + 4xyxyx - 102xyxyy + 13xyyyy + 20yxxyx + 143yxxyy + 12yxyyy - 7xxxy - 81xxyx - 51xxyy + 28xyxx - 64xyxy + 52xyyx + 158xyyy + 140yxxx - 68yxxy - 97yxyx - 43yxyy + 156yyyy + 46xxx - 163xxy - 2xyx - 91xyy - 163yxx - 93yxy - 7yyx - 46yyy + 122xx - 13xy - 116yx + 66yy - 164x + 143y + 158,$

$yxxyyy + 58xxyyy - 86xyxyx - 127xyxyy - 41yxxyx + 27yxxyy + 21yxyyy + 79xxxy - 135xxyx + 132xxyy + 60xyxx + 69xyxy - 125xyyx + 10xyyy + 44yxxx + 53yxxy + 158yxyx + 91yxyy + 104yyyy - 61xxx - 57xxy + 158xyx - 121xyy + 136yxx - 128yxy + 46yyx - 126yyy + 139xx - 30xy + 158yx + 133yy - 131x - 51y - 91,$

$xxxyx + 11xxyyy - 68xyxyx - 57xyxyy - 84yxxyx + 19yxxyy + 117yxyyy + 7xxxx - 64xxxy + 26xxyx - 143xxyy - 145xyxx - 118xyxy + 109xyyx + 127xyyy + 74yxxx - 49yxxy + 93yxyx + 54yxyy - 134yyyy - 15xxx - 35xxy - 79xyx - 16xyy + 139yxx - 161yxy - 152yyx - 127yyy - 98xx - 110xy - 86yx - 47yy + 12x - 104y + 159,$

$xxxyy + 132xxyyy - 27xyxyx + 86xyxyy - 131yxxyx + 107yxxyy + 154yxyyy - 83xxxy + 159xxyx - 35xxyy + 142xyxx - 58xyxy - 20xyyx + 132xyyy + 76yxxx - 152yxxy + 62yxyx + 139yxyy + 16yyyy + 152xxx + 36xxy - 39xyx + 21xyy - 27yxx + 61yxy + 106yyx + 161yyy - 32xx - 4xy + 48yx + 96yy - 41x + 140y + 92,$

$xxyyyy - 98xyxyxy + 162yxxyxy - 54yxyyyy + 99xxyxy + 59xxyyy - 24xyxxy + 24xyxyx + 110xyxyy + 50xyyxy + 148xyyyy + 141yxxxy - 91yxxyx - 115yxxyy - 155yxyxy + 34yxyyy - 40yyyyy - 137xxxy - 55xxyx + 11xxyy - 163xyxx + 147xyxy - 19xyyx + xyyy + 25yxxx - 19yxxy + 43yxyx + 41yxyy + 66yyxy - 103yyyy + 94xxx - 120xxy + 137xyx - 61xyy - 149yxx - 99yxy + 50yyx + 5yyy + 22xx + 48xy + 75yx - 151yy + 85x + 116y - 135,$

$yxyxyxy - 130yyxxyxy - 67yyxyyyy - 105xyxyxy - 23yxxyxy + 7yxyxxy - 7yxyxyx + 161yxyxyy + 13yxyyxy - 20yxyyyy + 83yyxxxy - 70yyxxyx - 63yyxxyy + 59yyxyxy + 128yyxyyy + 122yyyyyy + 65xxyxy + 137xxyyy - 73xyxxy - 66xyxyx + 27xyxyy - 41xyyxy - 47xyyyy - 112yxxxy + 105yxxyx + 21yxxyy - 49yxyxx + 129yxyxy - 91yxyyx + 129yxyyy - 159yyxxx - 91yyxxy + 84yyxyx + 57yyxyy - 102yyyxy + 144yyyyy - 123xxxy - 15xxyx - 12xxyy - 131xyxx - 45xyxy + 135xyyx - 113xyyy + 85yxxx - 29yxxy + 99yxyx + 16yxyy + 140yyxx - 95yyxy + 13yyyx - 11yyyy + 152xxx + 50xxy + 23xyx - 44xyy + 78yxx - 118yxy + 32yyx + 70yyy - 135xx + 163xy - 105yx - 6yy - 26x + 18y + 147,$

$xxyxyxy - 130xyxxyxy + 7xxyxxy - 7xxyxyx + 161xxyxyy + 13xxyyxy + 83xyxxxy - 70xyxxyx - 63xyxxyy + 131xyxyxy - 62yxxyxy - 101yxyyyy + 49xxxxy - 49xxyxx + 41xxyxy - 91xxyyx + 109xxyyy - 159xyxxx + 82xyxxy - 43xyxyx - 162xyxyy - 159xyyxy - 70xyyyy - 103yxxxy + 37yxxyx - 30yxxyy - 69yxyxy - 59yxyyy + 11yyyyy + 12xxxx - 37xxxy + 73xxyx + 51xxyy - 87xyxx - 118xyxy + 17xyyx - 37xyyy - 72yxxx - 77yxxy +$

$136yxyx - 131yxyy - 18yyxy + 114yyyy - 19xxx - 61xxy + 108xyx + 123xyy + 22yxx + 54yxy + 149yyx - 148yyy + xx + 121xy + 95yx - 108yy - 18x + 138y + 147,$

$yxyyyyyy - 122xxyxxyx - 111xxyxxyy + 150xyxyxyy - 88xyyxxyx + 99xyyxxyy - 128xyyxyyy - 2xyyyyyy + 113yxxyxyy - 76yxyxxyx - 80yxyxxyy + 4yxyyyyx - 98yxyyyyy + 13yyyyyyy + 142xxxxxy + 139xxyxxx + 150xxyxxy + 111xxyxyx - 149xxyxyy + 43xxyyyx + 97xyxxxy + 112xyxxyx + 37xyxxyy + 27xyxyxx + 119xyxyxy - 119xyxyyx + 46xyyxxx - 98xyyxxy + 126xyyxyx + 12xyyxyy - 8xyyyyx - 144xyyyyy + 159yxxxxy + 136yxxyxx + 140yxxyxy + 144yxxyyx + 130yxyxxx + 126yxyxxy + 137yxyxyx + 125yxyxyy + 39yxyyyx + 87yxyyyy - 61yyxxyx + 22yyxxyy - 79yyxyyy + 52yyyyyx - 56yyyyyy + xxxxx - 127xxxxy - 128xxyxx + 20xxyxy + 134xxyyx + 32xxyyy - 3xyxxx - 165xyxxy + 61xyxyx - 75xyxyy + 88xyyxx + 149xyyxy + 55xyyyx - 83xyyyy + 79yxxxx + 47yxxxy + 6yxxyx - 111yxxyy + 51yxyxx + 111yxyxy - 84yxyyx + 132yxyyy - 96yyxxx - 133yyxxy + 89yyxyx + 36yyxyy + 83yyyyx - 42yyyyy + 73xxxx + 127xxxy + 136xxyx - 65xxyy + 58xyxx + 60xyxy - 135xyyx - 75xyyy - 152yxxx - 106yxxy - 126yxyx + 23yxyy + 22yyxx - 114yyxy + 77yyyx + 137yyyy - 23xxx - 62xxy + 106xyx - 45xyy + 7yxx - 89yxy - 11yyx + 39yyy - 99xx + 118xy - 44yx + 86yy + 164x + 22y + 121,$

$xxyxxyxy + 17xyyxxyxy - 116xyyxyyyy + 120yxyxxyxy - 48yxyyyyxy + 7xxyxxxy + 26xxyxxyx - 109xxyxxyy + 146xxyyyxy + 32xyxxyxy + 7xyxyxxy + 104xyxyyxy + 119xyyxxxy + 111xyyxxyx + 133xyyxxyy + 50xyyxyxy + 24xyyxyyy + 96xyyyyxy + 147xyyyyyy + 23yxxyxxy - 73yxxyyxy - 153yxyxxxy + 141yxyxxyx + 160yxyxxyy - 137yxyyyxy + 5yxyyyyx - 115yxyyyyy + 106yyxxyxy + 96yyxyyyy + 38yyyyyxy + 48xxxxxy - 149xxyxxx + 87xxyxxy + 111xxyxyx - 59xxyxyy + 141xxyyxy - 29xxyyyx + 96xyxxxy + 145xyxxyx - 160xyxxyy - 49xyxyxx + 46xyxyxy - 66xyxyyx + 115xyyxxx - 150xyyxxy - 112xyyxyx + 32xyyxyy - 53xyyyxy - 10xyyyyx - 108xyyyyy - 37yxxxxy - 161yxxyxx - 134yxxyxy - 151yxxyyx - 6yxyxxx + 99yxyxxy + 63yxyxyx - 118yxyxyy - 4yxyyxy - 34yxyyyx + 156yxyyyy + 80yyxxxy - 75yyxxyx + 27yyxxyy - 111yyxyxy - 140yyxyyy - 3yyyyxy + 65yyyyyx + 84yyyyyy + 5xxxxx - 155xxxxy + 56xxyxx + 43xxyxy - 156xxyyx - 143xxyyy + 95xyxxx - 87xyxxy - 129xyxyx - 99xyxyy + 150xyyxx - 112xyyxy + 12xyyyx - 49xyyyy + 135yxxxx + 148yxxxy - 125yxxyx - 85yxxyy - 121yxyxx - 145yxyxy - 104yxyyx - 135yxyyy + 137yyxxx + 44yyxxy + 32yyxyx + 134yyxyy + 137yyyxy + 21yyyyx + 84yyyyy + 62xxxx + 97xxxy - 112xxyx + 47xxyy - 152xyxx + 131xyxy + 45xyyx + 123yxxx + 2yxxy - 81yxyx + 52yxyy + 93yyxx - 113yyxy + 96yyyx + 14yyyy + 80xxx - 18xxy + 95xyx - 112xyy - 148yxx + 15yxy + 100yyx - 21yyy + 150xx - 93xy + 141yx + 53yy - 148x - 122y - 101,$

$yxxyxxyx + 123yxxyxxyy + 161yxyyxxyx - 57yxyyxxyy - 157yxyyxyyy + 164yyxxyxyy -$

$64yyxyxxyx + 72yyxyxxyy + 33yyxyyyyy + 27xxyxxyx + 11xxyxxyy - 59xyxyxyy -$
$97xyyxxyx - 15xyyxxyy - 111xyyxyyy - 92xyyyyyy - 50yxxxxxy + 7yxxyxxx +$
$129yxxyxxy + 68yxxyxyx + 101yxxyxyy - 106yxyxxxy + 46yxyxxyx - 39yxyxxyy +$
$155yxyxyxx + 117yxyxyyx + 134yxyyxxx - 84yxyyxxy + 108yxyyxyx - 148yxyyxyy -$
$155yxyyyyy - 110yyxxxxy + 35yyxxyxx - 34yyxxyxy - 76yyxxyyx - 117yyxyxxx +$
$19yyxyxxy + 113yyxyxyx + 35yyxyxyy + 8yyxyyyx - 69yyxyyyy - 158yyyxxyx -$
$130yyyxxyy - 23yyyxyyy + 98yyyyyyy - 26xxxxxy - 142xxyxxx - 158xxyxxy +$
$125xxyxyx + 142xxyxyy + 65xxyyyx - 115xyxxxy + 72xyxxyx - 150xyxxyy - 42xyxyxx +$
$160xyxyxy + 147xyxyyx - 17xyyxxx + 65xyyxxy + 11xyyxyx - 22xyyxyy - 37xyyyyx +$
$68xyyyyy - 19yxxxxx - 132yxxxxy + 21yxxyxx + 54yxxyxy + 143yxxyyx + 3yxyxxx +$
$158yxyxxy - 99yxyxyx + 33yxyxyy + 40yxyyxx - 158yxyyxy + 151yxyyyx + 137yyxxxx -$
$124yyxxxy + 53yyxxyx - 19yyxxyy - 68yyxyxx + 115yyxyxy + 71yyxyyx - 115yyxyyy -$
$113yyyxxx + 46yyyxxy - 81yyyxyx - 136yyyxyy + 104yyyyyx - 43yyyyyy + 149xxxxx +$
$84xxxxy - 22xxyxx + 20xxyxy + 146xxyyx - 34xxyyy + 67xyxxx - 113xyxxy + 62xyxyx -$
$31xyxyy - 125xyyxx + 35xyyxy - 46xyyyx + 17xyyyy - 91yxxxx - 96yxxxy - 86yxxyx +$
$49yxxyy - 57yxyxx - 160yxyxy - 131yxyyy + 69yyxxx + 62yyxxy - 15yyxyx - 13yyxyy +$
$111yyyxx + 119yyyxy - 38yyyyx - 53yyyyy - 146xxxx - 87xxxy - 128xxyx - 71xxyy +$
$41xyxx - 144xyxy + 104xyyx - 47xyyy - 25yxxx - 76yxxy + 23yxyx + 153yxyy +$
$157yyxx - 60yyxy + 22yyyx + 6yyyy + 146xxx - 149xxy + 96xyx - 110xyy - 152yxx -$
$134yxy - 82yyx + 104yyy + 18xx + 116xy - 66yx - 61yy + 136x - 80y + 161,$

$yxyyxxyxy - 130yyxyxxyxy - 110yyxyyyyxy - 105xyyxxyxy + 128xyyxyyyy -$
$162xyyyyyyy - 118yxxyxxyy + 10yxyxxyxy - 35yxyxyxxy - 48yxyxyyxy + 7yxyyxxxy +$
$34yxyyxxyx + 82yxyyxxyy + 56yxyyxyxy + 92yxyyxyyy - 102yxyyyyxy - 30yyxxyxxy -$
$47yyxxyxyx - 18yyxxyxyy - 100yyxxyyxy + 83yyxyxxxy - 21yyxyxxyx - 55yyxyxxyy -$
$59yyxyyyxy + 149yyxyyyyx + 86yyxyyyyy - 118yyyyxxyxy - 54yyyyxyyyy - 106yyyyyyxy +$
$xxyxxyx - 84xxyxxyy + 21xxyyyxy - 28xyxxyxy + 82xyxyxxy + 27xyxyxyx + 29xyxyxyy +$
$102xyxyyxy - 73xyyxxxy - 108xyyxxyx + 164xyyxxyy - 11xyyxyxy + 38xyyxyyy +$
$32xyyyyxy - 160xyyyyyy + 21yxxxxxy + 77yxxyxxy - 10yxxyxyx + 91yxxyxyy -$
$4yxxyyxy - 125yxyxxxy + 110yxyxxyx - 37yxyxxyy + 127yxyxyxx - 67yxyxyyx -$
$93yxyyxxx + 23yxyyxxy - 134yxyyxyx + 111yxyyxyy + 9yxyyyxy + 8yxyyyyx +$
$51yxyyyyy + 17yyxxxxy - 2yyxxyxx - 128yyxxyxy + 16yyxxyyx - 147yyxyxxx +$
$66yyxyxxy - 49yyxyxyx + 72yyxyxyy + 162yyxyyxy + 22yyxyyyx - 94yyxyyyy -$
$164yyyxxxy + 111yyyxxyx - 157yyyxxyy + 161yyyxyxy - 109yyyxyyy + 87yyyyyxy -$
$49yyyyyyx - 35yyyyyyy - 145xxxxxy + 7xxyxxx + 33xxyxxy + 138xxyxyx + 53xxyxyy +$

$$131xxyyxy - 106xxyyyx - 103xyxxxy + 50xyxxyx + 2xyxxyy + 118xyxyxx + 27xyxyxy - 151xyxyyx - 94xyyxxx + 32xyyxxy + 80xyyxyx - 15xyyxyy + 17xyyyxy + 161xyyyyx - 117xyyyyy + 147yxxxxx + 35yxxxxy - 89yxxyxx + 41yxxyxy - 66yxxyyx + 23yxyxxx - 36yxyxxy + 54yxyxyx + 21yxyxyy + 102yxyyxx + 118yxyyxy - 96yxyyyx - 113yxyyyy - 94yyxxxx + 73yyxxxy + 145yyxxyx - 78yyxxyy - 150yyxyxx - 105yyxyxy - 23yyxyyx + 153yyxyyy + 115yyyxxx + 126yyyxxy - 46yyyxyx + 65yyyxyy + 31yyyyxy + 55yyyyyx - 53yyyyyy - 22xxxxx - 9xxxxy - 63xxyxx + 132xxyxy - 9xxyyx - 56xxyyy + 127xyxxx + 106xyxxy - 114xyxyx + 163xyxyy - 51xyyxx - 151xyyxy + 46xyyyx - 89xyyyy - 137yxxxx - 69yxxxy + 20yxxyx - 149yxxyy + 23yxyxx - 36yxyxy + 94yxyyx - 61yxyyy + 36yyxxx + 155yyxxy + 54yyxyx - 112yyxyy + 92yyyxx - 57yyyxy - 65yyyyx - 154yyyyy - 48xxxx + 87xxxy + 92xxyx - 57xxyy - 15xyxx - 138xyxy + 70xyyx - 96xyyy - 31yxxx - 91yxxy + 138yxyx - 40yxyy - 108yyxx + 160yyxy - 102yyyx + 32yyyy + 160xxx - 63xxy - 91xyx - 120xyy - 51yxx - 152yxy + 76yyx + 97xx - 116xy + 37yx - 129yy - 76x + 69y,$$

$$yxyyxyyyy - 52xyyyxyyyy - 155xyyyyyyyy - 23yxxyxxyy - 13yxyxxyxy + 43yxyxyxxy + 41yxyxyyxy + 24yxyyyxxyx - 89yxyyyxxyy - 55yxyyyxyxy + 116yxyyyxyyy - 33yyyxxyxxy - 141yyyxxyxyx - 54yyyxxyxyy - 4yyyxxyyxy + 147yyyxyxxyx + 24yyyxyxxyy - 17yyyxyyyxy + 123yyyxyyyyx + 97yyyxyyyyy - 72yyyyxxyxy - 105yyyyxyyyy - 66xxyxxyx - 133xxyxxyy - 14xxyyyxy - 104xyxxyxy - 159xyxyxxy + 81xyxyxyx + 123xyxyxyy + 60xyxyyxy + 73xyyxxyx - 44xyyxxyy - 119xyyxyxy + 42xyyxyyy + 120xyyyyxy - 164xyyyyyy + 63yxxxxxy + 67yxxyxxy + 61yxxyxyx + 147yxxyxyy + 57yxxyyxy - 115yxyxxxy - 140yxyxxyx + 163yxyxxyy + 7yxyxyxx + 159yxyxyyx - 163yxyyxxx + 69yxyyxxy + 124yxyyxyx - 101yxyyxyy - 98yxyyyxy + 147yxyyyyx - 124yxyyyyy - 28yyxxxxy - 74yyxxyxx - 69yyxxyxy - 38yyxxyyx + 36yyxyxxx - 108yyxyxxy - 25yyxyxyx - 2yyxyxyy + 54yyxyyxy - 61yyxyyyx + 70yyxyyyy + 158yyyxxxy - 129yyyxxyx - 108yyyxxyy + 138yyyxyxy - 33yyyxyyy + 110yyyyyxy - 56yyyyyyx + 29yyyyyyy + 36xxxxxy - 131xxyxxx + 44xxyxxy + 8xxyxyx + 101xxyxyy - 99xxyyxy - 7xxyyyx - 17xyxxxy + 112xyxxyx - 15xyxxyy - 141xyxyxx - 101xyxyxy - 163xyxyyx - 151xyyxxx - 144xyyxxy - 27xyyxyx + 22xyyxyy - 155xyyyxy + 88xyyyyx + 154xyyyyy + 110yxxxxx - 128yxxxxy + 81yxxyxx + 102yxxyxy - 46yxxyyx + 104yxyxxx + 93yxyxxy - 161yxyxyx - 154yxyxyy + 17yxyyxx - 53yxyyxy + 46yxyyyx + 62yxyyyy - 132yyxxxx - yyxxxy + 4yyxxyx + 152yyxxyy - 90yyxyxx - 150yyxyxy - 122yyxyyx - 40yyxyyy + 90yyyxxx + 72yyyxxy - 109yyyxyx - 81yyyxyy + 154yyyyxy - 116yyyyyx + 48yyyyyy - 79xxxxx + 128xxxxy + 103xxyxx + 99xxyxy - 70xxyyx - 4xxyyy - 10xyxxx + 33xyxxy - 65xyxyx + 137xyxyy - 74xyyxx + 121xyyxy + 132xyyyx + 70xyyyy - yxxxx + 84yxxxy - 48yxxyx +$$

$$134yxxyy+32yxyxx+66yxyxy+64yxyyx+85yxyyy+16yyxxx-123yyxxy+81yyxyx-3yyxyy+45yyyxx-108yyyxy+54yyyyx-31yyyyy+xxxx-11xxxy-26xxyx+31xxyy-143xyxx+15xyxy+xyyx-102xyyy+33yxxx-61yxxy-27yxyx-20yxyy-121yyxx-8yyxy-104yyyx-33yyyy+105xxx-154xxy-5xyx-68xyy-100yxx+158yxy+150yyx-101yyy-93xx-130xy-154yx-87yy-105x+5y-156,$$

$$xxyyxxyx+123xxyyxxyy-149xxyyxyyy+49xyxxyxyy-130xyxyxxyx-102xyxyxxyy-50xxyxxxy-68xxyxxyx+90xxyxxyy+69xxyxyxx-162xxyxyyx+7xxyyxxx+129xxyyyxxy-24xxyyyxyx-151xxyyxyy-120xyxxxxy+163xyxxyxx+23xyxxyxy+138xyxxyyx+83xyxyxxx+111xyxyxxy+142xyxyxyx-57xyxyxyy-63xyyxxyx-104xyyxxyy-36xyyxyyy+146xyyyyyy-104yxxyxyx-91yxxyxyy+57yxyxxyx+60yxyxxyy+112yxyyyyx-71yxyyyyy-21xxxxxy-12xxyxxx-134xxyxxy-165xxyxyx+106xxyxyy+159xxyyxx-112xxyyxy+71xxyyyx-30xyxxxx+57xyxxxy+138xyxxyx+153xyxxyy+57xyxyxx-29xyxyxy+125xyxyyx-110xyyxxx+89xyyxxy+109xyyxyx-22xyyxyy+29xyyyyx-94xyyyyy+129yxxxxy-18yxxyxx-115yxxyxy-56yxxyyx+68yxyxxx+71yxyxxy+40yxyxyx-36yxyxyy+129yxyyyx+87yxyyyy+68yyxxyx+98yyxxyy-155yyxyyy+132yyyyyx-18yyyyyy-147xxxxx+53xxxxy+46xxyxx-118xxyxy+72xxyyx+142xxyyy-70xyxxx+95xyxxy+74xyxyx-109xyxyy-161xyyxx+29xyyxy+19xyyyx+155xyyyy-85yxxxx-40yxxxy-125yxxyx+55yxxyy+50yxyxx-46yxyxy+133yxyyx-87yxyyy+145yyxxx-118yyxxy+165yyxyx-32yyxyy+45yyyyx-30yyyyy+44xxxx+64xxxy+137xxyx+40xxyy-145xyxx+97xyxy-27xyyx-42xyyy+10yxxx+125yxxy+24yxyx-95yxyy-148yyxx-132yyxy+99yyyx+65yyyy+164xxx+127xyx-77xyy+115yxx+63yxy-111yyx+13yyy-6xx+123xy+43yx-4yy+18x-34y+55,$$

$$xxyyyxyx+123xxyyyxyy-50xyxxyxyy+113xyxyxxyx-3xyxyxxyy+55xyxyyyxyx+145xyxyyyxyy+92yxxyyyxyx+62yxxyyyxyy+86yxyyxxyx-14yxyyxxyy+95yxyyxyyy+131yxyyyyxyx-106yxyyyyxyy+139yyyxxyxyy+83yyyxyxxyx-52yyyxyxxyy-79yyyxyyyyy+155xxxxxxy+61xxyxxyx+154xxyxxyy+63xxyxyxx-155xxyxyyx-13xxyyyxyx+56xxyyyxyy+7xxyyyyx+129xxyyyyxy+29xyxxxxy-115xyxxyxx+99xyxxyxy+131xyxxyyx+129xyxyxxx+13xyxyxxy-86xyxyxyx+98xyxyxyy+54xyxyyyx+144xyxyyyxy+79xyyyxxyx-76xyyyxxyy-97xyyxyyy+162xyyyxyx+66xyyyxyy-148xyyyyyy-111yxxxxxy+107yxxyxyx+129yxxyxyy-18yxxyyxx-48yxxyyxy+3yxyxxxy+37yxyxxyx+86yxyxxyy-20yxyxyxx+81yxyxyyx-60yxyyxxx-160yxyyxxy-43yxyyxyx-75yxyyxyy-76yxyyyxx+18yxyyyxy+125yxyyyyx-129yxyyyyy+153yyxxxxy-154yyxxxyx-49yyxxxyy-129yyxxyyx-81yyxyxxx+115yyxyxxy-100yyxyxyx-154yyxyxyy+31yyxyyyx+105yyxyyyy-33yyyxxyx-$$

$$90yyyxxyy+35yyyxyyy+48yyyyxyx-54yyyyxyy-34yyyyyyy+92xxxxxx-128xxxxxy-125xxyxxx+59xxyxxy-116xxyxyx-22xxyxyy+66xxyyxx-22xxyyxy+113xxyyyx+60xyxxxx+63xyxxxy-14xyxxyx+158xyxxyy-9xyxyxx+23xyxyxy-51xyxyyx-109xyyxxx-46xyyxxy+23xyyxyx-120xyyxyy+141xyyyxx+45xyyyxy+151xyyyyx-35xyyyyy-115yxxxxx+101yxxxxy-125yxxxyx-75yxxxyy+100yxxyyx+140yxyxxx-90yxyxxy+48yxyxyx+142yxyxyy+69yxyyxx-152yxyyxy+46yxyyyx-150yxyyyy-7yyxxxx+16yyxxxy+80yyxxyx-90yyxxyy-98yyxyxx+156yyxyxy+151yyxyyx+153yyxyyy+100yyyxxx-70yyyxxy+62yyyxyx+69yyyxyy+5yyyyxx-97yyyyxy+42yyyyyx+69yyyyyy-56xxxxx+76xxxxy-76xxyxx-16xxyxy+xxyyx-131xxyyy-117xyxxx+61xyxxy+83xyxyx-48xyxyy+124xyyxx-113xyyxy-37xyyyx+157xyyyy+159yxxxx+153yxxxy+26yxxyx-6yxxyy-49yxyxx+130yxyxy-116yxyyx-98yxyyy-31yyxxx+30yyxxy-59yyxyx-35yyxyy+165yyyxx-39yyyxy-89yyyyx+144yyyyy-35xxxx+52xxxy+96xxyx-5xxyy-58xyxx+18xyxy+74xyyx-143xyyy+131yxxx+13yxxy-34yxyx+29yxyy+141yyxx+92yyxy+27yyyx-50yyyy+70xxx+95xxy+39xyx-112xyy+86yxx+138yxy-43yyx+42yyy+149xx-109xy+108yx+127yy+72x+46y+6,$$

$$yxyxxyxyy+150yxyxyxxyx-86yxyxyxxyy+32yxyxyyyxyx-36yxyxyyyxyy-121yyxxyyyxyx+12yyxxyyyxyy+38yyxyyyxxyx+40yyxyyyxxyy-35yyxyyyxyyy+4yyxyyyyxyx+161yyxyyyyxyy+123yyyyxxyxyy-48yyyyxyxxyx+54yyyyxyxxyy-58yyyyxyyyyy+58xyxxyxyy+132xyxyxxyx+17xyxyxxyy-20xyxyyyxyx-143xyxyyyxyy+30yxxxxxxy-45yxxxyxxyy+151yxxxyxyxx-30yxxxyxyyx+59yxxyxxxxy-97yxyxxxyxx-141yxyxxyxy+4yxyxxyyyx+57yxyxyxxx+152yxyxyxxy-107yxyxyyxx+156yxyxyyxy-137yxyyxxyx-125yxyyxxyy+15yxyyxyyy-29yxyyyyxyx+74yxyyyyxyy+128yyxxxxxy+3yyxxyxyx+2yyxxyxyy+146yyxxyyyxx-52yyxxyyyxy+86yyxyxxxy+163yyxyxxyx-152yyxyxxyy-132yyxyxyxx+5yyxyxyyx-65yyxyyyxxx-63yyxyyyxxy-19yyxyyyxyx-164yyxyyyxyy+28yyxyyyyxx-146yyxyyyyxy-66yyxyyyyyx+156yyxyyyyyy+83yyyyxxxxy+109yyyyxxyxx+140yyyyxxyxy-57yyyyxxyyx-5yyyyxyxxx+97yyyyxyxxy+2yyyyxyxyx+109yyyyxyxyy+6yyyyxyyyx+31yyyyxyyyy+47yyyyyxxyx+68yyyyyxxyy-100yyyyyxyyy+52yyyyyyxyx+107yyyyyyxyy-92yyyyyyyyy+85xxxxxxy+164xxyxxyx+19xxyxxyy+152xxyxyxx-85xxyxyyx-22xxyyyxx-58xxyyyxy+112xyxxxxy+xyxxyxx+97xyxxyxy-99xyxxyyx-69xyxyxxx+147xyxyxxy-74xyxyxyx+132xyxyxyy-140xyxyyxx+68xyxyyxy-144xyyxxyx+52xyyxxyy+114xyyxyyy-148xyyyxyx+xyyyxyy-116xyyyyyy-121yxxxxxx+122yxxxxxy+64yxxyxxx+90yxxyxxy+50yxxyxyx+4yxxxyxyy-23yxxyyxx+65yxyxxxx-29yxyxxxy+142yxyxxyx-126yxyxxyy+14yxyxyxx+127yxyxyyx+34yxyyyxx-104yxyyxxy-148yxyyyxyx-$$

$$36yxyyxyy + 128yxyyyxx - 100yxyyyxy - 44yxyyyyx - 24yxyyyyy - 97yyxxxxx - 106yyxxxxy + 128yyxxyxx + yyxxyxy + 48yyxxyyx + 157yyxyxxx + 119yyxyxxy - 93yyxyxyx + 134yyxyxyy - 8yyxyyxx + 56yyxyyxy + 130yyxyyyx - 118yyxyyyy + 20yyyxxxx - 93yyyxxxy - 102yyyxxyx - 51yyyxxyy - 51yyyxyxx - 162yyyxyxy + 136yyyxyyx + 159yyyxyyy - 2yyyyxxx - 131yyyyxxy + 157yyyyxyx - 47yyyyxyy + 33yyyyyxx + 88yyyyyxy - 118yyyyyyx + 101yyyyyyy - 67xxxxxx + 165xxxxxy - 105xxyxxx - 104xxyxxy - 74xxyxyx - 40xxyxyy - 164xxyyxx + 141xxyyxy + 45xxyyyx + 129xyxxxx + 104xyxxxy - 162xyxxyx - 144xyxxyy - 108xyxyxx - 149xyxyxy + 43xyxyyx - 15xyyxxx + 27xyyxxy - 97xyyxyx - 46xyyxyy - 43xyyyxx + 106xyyyxy - 31xyyyyx + 93xyyyyy + 109yxxxxx - 99yxxxxy - 16yxxyxx + yxxyxy + 80yxxyyx + 114yxyxxx + 78yxyxxy + 42yxyxyx + 144yxyxyy + 122yxyyxx - 42yxyyxy - 150yxyyyx + 16yxyyyy + 28yyxxxx + 18yyxxxy + 96yyxxyx + 153yyxxyy + 153yyxyxx - 155yyxyxy + 20yyxyyx + 132yyxyyy - 113yyyxxx + 112yyyxxy - 70yyyxyx + 98yyyxyy + 118yyyyxx + 44yyyyxy - 38yyyyyx - 5yyyyyy - 18xxxxx + 111xxxxy - 137xxyxx - xxyxy - 154xxyyx + 121xxyyy - 96xyxxx - 95xyxxy + 152xyxyx + 84xyxyy + 87xyyxx - 69xyyxy - 129xyyyx + 17xyyyy - 76yxxxx + 54yxxxy - 51yxxyx + 152yxxyy + 18yxyxx - 108yxyxy + 30yxyyx + 152yxyyy + 110yyxxx - 156yyxxy - 87yyxyx + 142yyxyy - 140yyyxx - 129yyyxy - 132yyyyx - 115yyyyy - 99xxxx + 76xxxy + 150xxyx - 152xxyy - 48xyxx - 156xyxy - 43xyyx + 13xyyy + 80yxxx + 134yxxy - 76yxyx - 71yxyy - 129yyxx + 128yyxy + 103yyyx - 102yyyy + 79xxx - 66xxy + 125xyx - 64xyy + 153yxx - 2yxy + 108yyx + 92yyy + 11xx + 150xy + 47yx - 12yy + 145x + 141y + 36,$$

$$xxyyxyyyy + 89xxyxyyxy - 62xxyyxxyy - 55xxyyxyxy + 51xxyyxyyy - 137xxyyyxyy + 56xyxxyxxy - 152xyxxyxyx + 65xyxxyxyy + 122xyxxyyxy - 98xyxyxxyx + 54xyxyxxyy + 78xyxyyxyy - 39xyyyxxyx + 90xyyxyyyy - 121xyyyyyyy - 7yxxyxxyy - 26yxxyyxyy - 108yxyxxyxy - 73yxyyyxyy - 23yxyyyyxy + 47xxxxxxy - 118xxyxxxy - 115xxyxxyx - 51xxyxxyy + 74xxyxyyx + 55xxyyxxy + 38xxyyxyx + 8xxyyxyy + 123xxyyyxy + 59xyxxxxy - 17xyxxyxx - 109xyxxyxy + 104xyxxyyx - 24xyxyxxx + 67xyxyxxy - 111xyxyxyx - 141xyxyxyy + 104xyxyyxy + 58xyyxxxy + 124xyyxxyx + 99xyyxxyy - 70xyyxyxy + 13xyyxyyy - 17xyyyxyy + 129xyyyyxy - 8xyyyyyy - 152yxxyxxy + 113yxxyxyx + 65yxxyxyy - 18yxxyyxy - 94yxyxxxy - 156yxyxxyx - 7yxyxxyy - 161yxyyxyy - 138yxyyyxy - 165yxyyyyx + 160yxyyyyy - 125yyxxyxy - 76yyxyyyy + 44yyyyxyy + 32yyyyyxy + 82yyyyyyy - 2xxxxxx + 54xxxxxy + 24xxyxxx + 13xxyxxy + 134xxyxyx + 98xxyxyy + 95xxyyxx + 103xxyyxy - 101xxyyyx + 33xyxxxx + 100xyxxxy + 59xyxxyx + 27xyxxyy + 122xyxyxx + 26xyxyxy - 104xyxyyx - 125xyyxxx + 26xyyxxy +$$

$73xyyxyx - 86xyyxyy + 148xyyyxy - 51xyyyyx + 35xyyyyy + 62yxxxxy + 67yxxyxx - 21yxxyxy - 69yxxyyx - 99yxyxxx - 75yxyxxy + 37yxyxyx - 96yxyxyy + 29yxyyxy + yxyyyx - 90yxyyyy + 118yyxxxy + 114yyxxyx - 65yyxxyy + 35yyxyxy - 108yyxyyy + 17yyyxyy + 68yyyyxy - 159yyyyyx - 28yyyyyy - 72xxxxx + 13xxxxy + 142xxyxx - 60xxyxy + 161xxyyx - 154xxyyy + 49xyxxx + 153xyxxy - 103xyxyx - 123xyxyy + 105xyyxx - 163xyyxy + 142xyyyx + 93xyyyy + 82yxxxx - 88yxxxy + 16yxxyx + 126yxxyy + 35yxyxx + 41yxyxy - 42yxyyx - 82yxyyy + 136yyxxx + 108yyxxy - 136yyxyx - 13yyxyy + 59yyyxy - 28yyyyx + 136yyyyy + 62xxxx + 20xxxy + 12xxyx - 38xxyy + 40xyxx - 117xyxy - 141xyyx + 94xyyy - 40yxxx + 128yxxy + 52yxyx + 70yxyy - 35yyxx + 87yyxy + 121yyyx + 18yyyy + 136xxx + 150xxy - 122xyx - 43xyy + 18yxx - 100yxy - 70yyx + 62yyy - 71xx + 85xy + 93yx + 96yy - 157x + 116y - 49,$

$xxyxyyxyx + 123xxyxyyxyy + 110xyxxyyxyx - 41xyxxyyxyy + 128xyxyyxxyx - 21xyxyyxxyy + 26xyxyyxyyy - 123xyyxxyxyy + 164xyyxyxxyx - 19xyyxyxxyy - 94xyyxyyyyy + 78yxxyyxxyy - 128yxxyyxyyy + 38yxyxyxxyx + 40yxyxyxxyy + 3yxyxyyxyx + 38yxyxyyxyy + 46yxyyyxxyx + 51yxyyyxxyy - 148yxyyyxyyy + 129yxyyyyxyx + 68yxyyyyxyy - yyxxyyxyx - 123yyxxyyxyy + 107yyxyyxxyx - 79yyxyyxxyy - 55yyxyyxyyy - 41yyxyyyxyx - 78yyxyyyxyy + 146yyyxxyxyy + 161yyyxyxxyx - 57yyyxyxxyy + 98yyyxyyyyy + 63xxxxxxxy + 19xxyxxxxy - 99xxyxxyxx + 134xxyxxyyx + 7xxyxyyxx + 129xxyxyyxy + 154xxyyxxyy - 53xxyyxyyy - 147xxyyyyxy - 58xxyyyyxy + 4xyxxxxxy + 52xyxxyxyx + 118xyxxyxyy + 108xyxxyyxx - 43xyxxyyxy - 26xyxyxxxy - 54xyxyxxyx - 142xyxyxxyy + 50xyxyxyxx + 78xyxyxyyx - 97xyxyyxxx + 5xyxyyxxy - 75xyxyyxyx - 62xyxyyxyy + 75xyyxxxxy - 69xyyxxyxx + 62xyyxxyxy + 112xyyxxyyx + 155xyyxyxxx - 28xyyxyxxy - 69xyyxyxyx + 114xyyxyxyy + 145xyyxyyyx + 58xyyxyyyy + 120xyyyxxyx + 106xyyyxxyy + 28xyyyxyyy + 73xyyyyyxy - 136xyyyyyxy + 102xyyyyyyy - 142yxxxxxxy + 51yxxyxxxy - 155yxxyxxyy - 61yxxyxyxx + 90yxxyxyyx - 22yxxyyxxy - 124yxxyyxyx - 39yxxyyxyy + 143yxyxxxxy + 22yxyxxyxx - 100yxyxxyxy - 61yxyxxyyx - 65yxyxyxxx - 63yxyxyxxy + 21yxyxyyxx + 56yxyxyyxy + 66yxyyxxyx - 144yxyyxxyy + 61yxyyxyyy - 9yxyyyxxx + 103yxyyyxxy - 25yxyyyxyx - 15yxyyyxyy - 136yxyyyyxx - 50yxyyyyxy + 90yxyyyyyx + 12yyxxxxxy + 149yyxxyxyx - 120yyxxyxyy - 7yyxxyyxx - 129yyxxyyxy - 54yyxyxxxy - 17yyxyxxyx + 163yyxyxxyy + 29yyxyxyxx - 134yyxyxyyx + 87yyxyyxxx - 99yyxyyxxy + 112yyxyyxyx + 26yyxyyxyy + 44yyxyyyxx + 7yyxyyyxy + 152yyxyyyyx + 106yyxyyyyy - 106yyyxxxxy + 124yyyxxyxx - 111yyyxxyxy + 5yyyxxyyx + 134yyyxyxxx - 84yyyxyxxy + 145yyyxyxyx + 124yyyxyxyy + 104yyyxyyyx + 96yyyxyyyy - 132yyyyxxyx - 34yyyyxxyy + 94yyyyxyyy + 151yyyyyyxy -$

$$130yyyyyxyy - 50yyyyyyyy + 110xxxxxxx - 126xxxxxxy + 102xxyxxxx - 22xxyxxxy + 158xxyxxyx + 118xxyxxyy + 16xxyxyxx - 81xxyxyyx + 107xxyyxxy + 115xxyyxyx - 35xxyyxyy - 34xxyyyxx - 63xxyyyxy + 28xyxxxxx - 118xyxxxxy + 97xyxxyxx - 75xyxxyxy - 115xyxxyyx - 24xyxyxxx - 147xyxyxxy - 88xyxyxyx + 71xyxyxyy + 96xyxyyxx - 42xyxyyxy + 42xyyxxxx + 165xyyxxxy - 44xyyxxyx - 70xyyxxyy - 40xyyxyxx + 148xyyxyxy + 46xyyxyyx - 70xyyxyyy - 153xyyyxxx - 38xyyyxxy + 89xyyyxyx + 81xyyyxyy - 59xyyyyxx + 100xyyyyxy + 50xyyyyyx - 91xyyyyyy - yxxxxxx + 79yxxxxxy + 21yxxyxxx + 49yxxyxxy + 156yxxyxyx - 82yxxyxyy - 11yxxyyxx + 111yxxyyxy + 162yxyxxxx - 123yxyxxxy - 151yxyxxyx - 36yxyxxyy - 82yxyxyxx - 50yxyxyyx + 131yxyyxxx - 78yxyyxxy + 95yxyyxyx - 100yxyyxyy + 42yxyyyxx + 68yxyyyxy - 59yxyyyyx + 159yxyyyyy + 84yyxxxxx + 156yyxxxxy - 138yyxxyxx - 14yyxxyxy + 81yyxxyyx + 37yyxyxxx - 57yyxyxxy + 162yyxyxyx - 9yyxyxyy + 82yyxyyxx + 88yyxyyxy + 75yyxyyyx + 84yyxyyyy + 126yyyxxxx + 43yyyxxxy + 53yyyxxyx - 70yyyxxyy + 109yyyxyxx - 160yyyxyxy - 70yyyxyyx - 131yyyxyyy + 69yyyyxxx - 49yyyyxxy - 109yyyyxyx + 43yyyyxyy + 128yyyyyxx + 103yyyyyxy - 136yyyyyyx - 137yyyyyyy + 36xxxxxx + 65xxxxxy - 100xxyxxx - 68xxyxxy - 51xxyxyx + 96xxyxyy + 128xxyyxx - 162xxyyxy - 15xxyyyx - 58xyxxxx + 83xyxxxy - 81xyxxyx - 144xyxxyy - 88xyxyxx - 132xyxyxy - 112xyxyyx + 160xyyxxx + 76xyyxxy + 49xyyxyx + 116xyyxyy - 122xyyyxx - 12xyyyxy - 15xyyyyx - 137xyyyyy - 28yxxxxx + 73yxxyxx - 132yxxyxy + 32yxxyyx + 38yxyxxx - 19yxyxxy + 123yxyxyx + 43yxyxyy - 164yxyyxx - 98yxyyyx - 90yxyyyy + 140yyxxxx + 5yyxxxy + 63yyxxyx + 21yyxxyy - 21yyxyxx - 127yyxyxy + 49yyxyyx - 138yyxyyy + 86yyyxxx + 162yyyxxy - 5yyyxyx - 68yyyxyy - 140yyyyxx + 21yyyyxy + 123yyyyyx - 49yyyyyy - 110xxxxx + 64xxxxy + 84xxyxx - 67xxyxy + 100xxyyx + 127xxyyy - 151xyxxx - 72xyxxy - 33xyxyx - 41xyxyy - 43xyyxx - 113xyyxy + 8xyyyx + 49xyyyy - 143yxxxx + 82yxxxy - 116yxxyx - 152yxxyy + 122yxyxx + 164yxyxy + 66yxyyx - 2yxyyy - 34yyxxx - 2yyxxy + 40yyxyx - 79yyxyy - 29yyyxx - 81yyyxy + 148yyyyx + 148yyyyy - 164xxxx + 44xxxy - 71xxyx + 125xxyy - 140xyxx + 104xyxy + 97xyyx + 144xyyy + 107yxxx + 23yxxy + 8yxyx + 15yxyy + 63yyxx + 129yyxy + 42yyyx - 23yyyy - 92xxx + 62xxy + 145xyx - 81xyy - 45yxx - 23yxy - 92yyx - 95yyy - 17xx - 73xy - 63yx + 91yy - 117x + 44y - 157,$$

$$xxyyyxyyy + 55xyxyyxyyy + 92yxxyyxyyy + 131yxyyyxyyy - 13xxyyxyyy + 105xxyyyxyy + 119xyxxyxyx + 54xyxxyxyy - xyxyxxyx - 123xyxyxxyy + 148xyxyyxyy + 162xyyyxyyy + 61yxxyyxyy - 115yxyyxxyx + 88yxyyxxyy - 42yxyyxyyy - 147yxyyyxyy + 112yyxxyxyx - 109yyxxyxyy + 93yyxyxxyx - 146yyxyxxyy + 25yyxyyyyx + 4yyxyyyyy + 48yyyyxyyy +$$

$$119xxxxxxy - 119xxyxxyx + 50xxyxxyy - 13xxyxyxx + 53xxyxyyx - 41xxyyxyy + 46xxyyyxy - 98xyxxxxy - 110xyxxyxx + 130xyxxyxy - 93xyxxyyx - 7xyxyxxx - 129xyxyxxy - 34xyxyxyx + 5xyxyxyy - 118xyxyyxy - 127xyyxxyx + 59xyyxxyy - 143xyyxyyy + 129xyyyxyy - 110xyyyyyy - 66yxxxxxy + 11yxxyxyx - 146yxxyxyy - 71yxxyyxy + 123yxyxxxy - 119yxyxxyx + 124yxyxxyy + 108yxyxyxx - 55yxyxyyx - 143yxyyxxx + 60yxyyxxy + 112yxyyyxx - 144yxyyyxy + 68yxyyyxy + 92yxyyyyx + 57yxyyyyy - 16yyxxxxy + 16yyxxyxx + 148yyxxyxy - 117yyxxyyx - 11yyxyxxx + 81yyxyxxy + 159yyxyxyx - 3yyxyxyy + 160yyxyyyx + 19yyxyyyy + 143yyyxxyx + 140yyyxxyy+67yyyxyyy+75yyyyxyy−6yyyyyyx+52yyyyyyy−160xxxxxx+138xxxxxy+ 69xxyxxx+58xxyxxy−34xxyxyx−152xxyxyy+162xxyyxx+64xxyyxy−106xxyyyx− 5xyxxxx − 30xyxxxy − 43xyxxyx + 29xyxxyy − 133xyxyxx − 161xyxyxy + 40xyxyyx + 104xyyxxx + 70xyyxxy − 18xyyxyx + 76xyyxyy − 161xyyyxy + 47xyyyyx − 10xyyyyy − 131yxxxxx+36yxxxxy−130yxxyxx−60yxxyxy−117yxxyyx+122yxyxxx+21yxyxxy+ 85yxyxyx − 85yxyxyy − 117yxyyxx − 74yxyyxy + 56yxyyyx − 19yxyyyy + 139yyxxxx + 159yyxxxy + 3yyxxyx − 106yyxxyy + 22yyxyxx − 7yyxyxy + 45yyxyyx − 120yyxyyy + 8yyyxxx − 144yyyxxy − 129yyyxyx + 59yyyxyy − 109yyyyxy − 48yyyyyx + 2yyyyyy + 52xxxxx−26xxxxy+57xxyxx+14xxyxy−54xxyyx+90xxyyy+11xyxxx−107xyxxy− 143xyxyx − 165xyxyy + 89xyyxx − 131xyyxy − 45xyyyx − 122xyyyy + 111yxxxx − 92yxxxy − 116yxxyx − 143yxxyy + 158yxyxx − 57yxyxy + 141yxyyx + 73yxyyy − 52yyxxx − 49yyxxy − 140yyxyx + 77yyxyy + 58yyyxx + 12yyyxy − 17yyyyx − 41yyyyy + 25xxxx + 124xxxy + 5xxyx − 3xxyy − xyxx − 67xyxy − 11xyyx + 141xyyy + 83yxxx − 2yxxy − 70yxyx + 131yxyy + 4yyxx − 159yyxy − 114yyyx − 141yyyy − 164xxx − 138xxy + 92xyx−88xyy−19yxx+163yxy+143yyx−159yyy−80xx+54yx+149yy−102x+95y−76,$$

$$xxyxyxxy - 55xxyxyyxy - 91xxyyyxyy + 98xyxxyxxy - 146xyxxyxyx - 84xyxxyxyy - 103xyxxyyxy−68xyxyxxyx−111xyxyxxyy−40xyxyyxyy−88xyyxxyxy+163xyyxyyyy− 134xyyyyyyy + 63yxxyxxyy - 97yxxyyxyy + 8yxyxxyxy - 5yxyyyxyy + 63yxyyyyxy - 92xxxxxxy + 7xxyxxxy - 74xxyxxyx + 14xxyxxyy + 131xxyxyxx + 77xxyxyyx + 13xxyyxxy - 141xxyyxyy + 87xxyyyxy - 89xyxxxxy - 100xyxxyxx - 89xyxxyxy - 165xyxxyyx - 145xyxyxxx + 49xyxyxxy + 33xyxyxyx + 40xyxyxyy - 22xyxyyxy + 46xyyxxxy - 157xyyxxyx + 140xyyxxyy + 123xyyxyxy - 120xyyxyyy + 153xyyyxyy - 97xyyyyxy - 35xyyyyyy - 95yxxyxxy + 19yxxyxyx + 160yxxyxyy + 148yxxyyxy + 56yxyxxxy + 62yxyxxyx - 108yxyxxyy + 125yxyyxyy - 104yxyyyxy + 106yxyyyyx + 104yxyyyyy - 99yyxxyxy + 33yyxyyyy - 65yyyyxyy + 157yyyyyxy - 87yyyyyyy + 18xxxxxx−113xxxxxy+68xxyxxx−114xxyxxy−140xxyxyx+104xxyxyy+48xxyyxx−$$

$$158xxyyxy+42xxyyyx+36xyxxxx+133xyxxxy+160xyxxyx-110xyxxyy+88xyxyxx+122xyxyxy+126xyxyyx-106xyyxxx-78xyyxxy+59xyyxyx-159xyyxyy-116xyyyxy-54xyyyyx-2xyyyyy+104yxxxxy+39yxxyxx-91yxxyxy-94yxxyyx+103yxyxxx+95yxyxxy-135yxyxyx-110yxyxyy-13yxyyxy+19yxyyyx-60yxyyyy-31yyxxxy-107yyxxyx+65yyxxyy-136yyxyxy+136yyxyyy-153yyyxyy-40yyyyxy+54yyyyyx+56yyyyyy-51xxxxx+67xxxxy-164xxyxx+150xxyxy-23xxyyx-61xxyyy-22xyxxx-127xyxxy+106xyxyx-97xyxyy-42xyyxx-21xyyxy+45xyyyx+42xyyyy-146yxxxx+105yxxxy+159yxxyx+143yxxyy+159yxyxx-5yxyxy-72yxyyx+68yxyyy-87yyxxx+89yyxxy+151yyxyx-114yyxyy+12yyyxy+2yyyyx+35yyyyy+4xxxx+26xxxy+84xxyx+160xxyy+90xyxx+66xyxy-100xyyx+111xyyy+80yxxx-114yxxy-88yxyx+146yxyy-157yyxx-155yyxy+76yyyx-20yyyy-129xxx-108xxy+67xyx+52xyy+57yxx+52yxy+53yyx-16yyy-110xx+78xy+107yx-94yy-88x+154y+144,$$

$$xxyyyxxyx-105xyxyyxxyx-159xyxyyxxyy+42xyxyyxyyy-93xyyyxxyxyx+34xyyyxxyxyy+31xyyyxyyyyx+99xyyyxyyyyy+88yxxyyxxyy+47yxxyyxyyy-157yxyxxyxyx+157yxyxyxxyx+113yxyxyxxyy+7yxyxyyyxyx-132yxyxyyyxyy-85yxyyyyxxyx-3yxyyyyxxyy+80yxyyyyxyyy-128yxyyyyyxyx-146yxyyyyyxyy+108yyyxxyyyxyx+44yyyxxyyyxyy+29yyyxyyyxxyx-74yyyxyyxxyy-18yyyxyyxyyy+125yyyxyyyyxyx+149yyyxyyyyxyy+120yyyyxxyxyy+155yyyyxyxxyx-133yyyyxyxxyy+8yyyyxyyyyy+126xxyyyxxyy-143xxyyyxyyy+7xxyyyyxxx-62xxyyyyxxy-71xxyyyyxyy+72xyxxyxyx+12xyxxyxyy+135xyxyxxxy+32xyxyxxyx-123xyxyxxyy+46xyxyxyxx-108xyxyxyyx-73xyxyyyxx-52xyxyyyxy-73xyxyyyxy-41xyxyyyyy-101xyyyxxyxx-120xyyyxxyxy-124xyyyxxyyx-70xyyyxyxyx+119xyyyxyxyy+5xyyyxyyyx+162xyyyxyyyy+164xyyyyxxyx+68xyyyyxxyy-150xyyyyxyyy-75xyyyyyxyx-39xyyyyyxyy+72xyyyyyyyx-37xyyyyyyyy+110yxxxxxxy+71yxxyxxxy-143yxxyxxyy+18yxxyxyxx-90yxxyxyyx-21yxxyyyxy-37yxxyyyxyx+122yxxyyyxyy-104yxyxxxxy+123yxyxxxyxx-20yxyxxxyxy+102yxyxxxyyx+106yxyxyxxx+62yxyxyxxy+49yxyxyyxx-90yxyxyyxy+20yxyyxxyx-23yxyyxxyy+9yxyyxyyy+67yxyyyxxx-46yxyyyxxy-80yxyyyxyx+81yxyyyxyy+97yxyyyyxx-140yxyyyyxy-9yxyyyyyx+28yyyxxxxy+73yyyxxyxx-96yyyxxyxyy+94yyyxxyyxx+30yyyxxyyxy-126yyyxyxxxy-70yyyxyxxyx-151yyyxyxyy-153yyyxyxyxx-92yyyxyxyyx-128yyyxyyxxx+100yyyxyyxxy+151yyyxyyxyx-160yyyxyyxyy-118yyyxyyyxx-94yyyxyyyxy-45yyyxyyyyx+152yyyxyyyyy-137yyyyxxxxy-152yyyyxxyxx+72yyyyxxyxy+122yyyyxxyyx+92yyyyxyxxx+135yyyyxyxxy-103yyyyxyxyx-152yyyyxyxyy+22yyyyxyyyx-107yyyyxyyyy-50yyyyyxxyx+100yyyyyxxyy-99yyyyyxyyy-39yyyyyyxyx+39yyyyyyxyy+104yyyyyyyyy-21xxxxxxy+31xxyxxxy-79xxyxxyx-118xxyxxyy-$$

$$128xxyxyxx + 99xxyxyyx + 156xxyyxxy + 136xxyyxyx + 95xxyyxyy + 148xxyyyxx + 43xxyyyxy - 106xyxxxxy + 12xyxxyxx + 73xyxxyxy + 140xyxxyyx - 164xyxyxxx + 146xyxyxxy - 44xyxyxyx - 61xyxyxyy + 26xyxyyxx + 115xyxyyxy - 122xyyxxxx - 142xyyxxxy - 129xyyxxyx - 110xyyxxyy - 71xyyxyxx + 48xyyxyxy - 43xyyxyyx - 104xyyxyyy + 155xyyyxxx - 111xyyyxxy - 159xyyyxyx - 91xyyyxyy + 137xyyyyxx - 51xyyyyxy - 80xyyyyyx - 127xyyyyyy + 108yxxxxxx + 49yxxxxxy - 39yxxyxxx - 131yxxyxxy + 157yxxyxyx + 96yxxyxyy + 150yxxyyxx - 90yxxyyxy - 118yxyxxxx + 116yxyxxxy - 40yxyxxyx + yxyxxyy - 74yxyxyxx - 73yxyxyyx + 140yxyyxxx + 81yxyyxxy + 161yxyyxyx - 154yxyyxyy + 107yxyyyxx - 67yxyyyxy - 15yxyyyyx + 34yxyyyyy - 135yyxxxxx + 5yyxxxxy - 95yyxxyxx + 138yyxxyxy - 45yyxxyyx - 126yyxyxxx - 74yyxyxxy - 155yyxyxyx + 122yyxyxyy + 81yyxyyxx + 95yyxyyxy + 6yyxyyyx + 119yyxyyyy - 37yyyxxxx - 10yyyxxxy - 128yyyxxyx - 57yyyxxyy + 144yyyxyxx + 68yyyxyxy - 53yyyxyyx - 152yyyxyyy - 19yyyyxxx + 25yyyyxxy - 78yyyyxyx + 141yyyyxyy + 58yyyyyxx - 63yyyyyxy - 85yyyyyyx + 96yyyyyyy - 147xxxxxx - 101xxxxxy + 92xxyxxx + 154xxyxxy + 122xxyxyx - 40xxyxyy + 164xxyyxx - 140xxyyxy - 9xxyyyx + 117xyxxxx - 125xyxxxy - xyxxyx + 100xyxxyy + 28xyxyxx + 27xyxyxy + 99xyxyyx + 70xyyxxx - 118xyyxxy + 90xyyxyx - 139xyyxyy + 75xyyyxx - 67xyyyxy - 36xyyyyx + 89xyyyyy + 149yxxxxx - 114yxxxxy - 162yxxyxx + 85yxxyxy - 159yxxyyx - 129yxyxxx - 78yxyxxy + 40yxyxyx + 113yxyxyy - 141yxyyxx - 11yxyyxy + 138yxyyyx - 119yxyyyy - 158yyxxxx + 58yyxxxy - 157yyxxyx - 165yyxxyy + 110yyxyxx - 126yyxyxy - 140yyxyyx + 126yyxyyy + 94yyyxxx + 6yyyxxy - 44yyyxyx + 143yyyxyy - 106yyyyxx + 30yyyyxy - 74yyyyyx - 130yyyyyy - 20xxxxx - 56xxxxy + 21xxyxx + 28xxyxy + 76xxyyx + 111xxyyy - 153xyxxx - 44xyxxy - 3xyxyx + 113xyxyy - 153xyyxx + 91xyyxy + 131xyyyx - 64xyyyy - 140yxxxx + 27yxxxy + 82yxxyx - 116yxxyy - 37yxyxx + 15yxyxy + 80yxyyx - 140yxyyy - 102yyxxx - 138yyxxy - 136yyxyx + 59yyxyy - 98yyyxx - 57yyyxy + 81yyyyx + 137yyyyy - 96xxxx - 5xxxy + 66xxyx + 165xxyy + 77xyxx - 22xyxy - 127xyyx + 140xyyy - 100yxxx - 103yxxy - 73yxyx + 79yxyy - 42yyxx + 25yyxy - 161yyyx + 119yyyy - 14xxx - 141xxy - 42xyx - 81xyy - 72yxx - 159yxy + 72yyx - 2yyy + 102xx - 76xy - 49yx + 15yy + 19x + 30y - 91,$$

$$xxyxxyxxy - 99xxyxxyyxy - 6xxyxyyxyy - xyxxyxxyy - 41xyxxyyxyy - 110xyxyxxyxy + 64xyxyxyxxy + 121xyxyxyyxy - 43xyxyyxxyx + 25xyxyyxxyy + 63xyxyyxyyy - 76xyyxxyxyx - 58xyyxxyxyy - 85xyyxyyyyx - 70xyyxyyyyy + 78xyyyyyyyy + 76yxxyyxxyy + 62yxxyyxyyy + 120yxyxxyxxy + 36yxyxxyyxy - 33yxyxyxxyx + 136yxyxyxxyy + 119yxyxyyxyx - 3yxyxyyxyy - 74yxyyyxxyx - 154yxyyyxxyy +$$

$$51yxyyyxyyy + 165yxyyyyxxy - 136yxyyyyxyx - 98yxyyyyxyy - 138yxyyyyyxy - 112yyxxyxxyy - 150yyxxyyxyx + yyxxyyxyy + 59yyxyxxyxy + 162yyxyyxxyx + 66yyxyyxxyy + 25yyxyyxyyy + 139yyxyyyyxy + 41yyxyyyxyy + 32yyxyyyyxy + 54yyyxxyxyy - 13yyyxyxxyx + 56yyyxyxxyy + 136yyyxyyyyy - 82xxxxxxxy - 66xxyxxxxy + 131xxyxxyxx - 60xxyxxyyx - 6xxyxyyxy - 69xxyyxxyy + 116xxyyxyxy + 48xxyyxyyy + 71xxyyyxxy - 56xxyyyxyy - 121xyxxyxxy - 44xyxxyxyx - 158xyxxyxyy - 9xyxxyyxy - 156xyxyxxxy + 3xyxyxxyx + 2xyxyxxyy + 111xyxyxyxx + 131xyxyxyyx + 30xyxyyxxx + 32xyxyyyxy + 43xyxyyyxx - 134xyxyyyyy + 10xyyxxyxx - 85xyyxxyxy + 9xyyxxyyx - 161xyyxyxxy - 48xyyxyxyx + 133xyyxyxyy - 82xyyxyyxy + 29xyyxyyyx + 4xyyxyyyy + 22xyyyxxyx - 101xyyyxxyy + 36xyyyxyyy + xyyyyxxy - 59xyyyyxyx - 142xyyyyxyy - 55xyyyyyxy - 112xyyyyyyx + 62xyyyyyyy - 26yxxxxxxy + 160yxxyxxxy - 90yxxyxxyy - 45yxxyxyxx + 100yxxyxyyx + 3yxxyyxxy - 56yxxyyxyx - 63yxxyyxyy - 37yxyxxxxy - 40yxyxxxyx + 92yxyxxyxy + 63yxyxxyyx + 100yxyxyxxx + 76yxyxyxxy - 160yxyxyyxx + 72yxyxyyxy - 125yxyyxxyx - 46yxyyxxyy + 18yxyyxyxy + 78yxyyxyyy + 144yxyyyxxx - 122yxyyyxxy + 125yxyyyxyx + 135yxyyyxyy + 141yxyyyyxx + 157yxyyyyxy + 14yxyyyyyx + 145yyxxxxxy + 135yyxxyxxy + 157yyxxyxyx - 118yyxxyxyy - 57yyxxyyxx - 94yyxxyyxy - 74yyxyxxxy + 132yyxyxxyx + 71yyxyxxyy + 47yyxyxyxx + 91yyxyxyyx + 141yyxyyxxx + 45yyxyyxxy - 81yyxyyxyx - 20yyxyyyxx + 147yyxyyyxy - yyxyyyyx + 6yyxyyyyy - 12yyyxxxxy + 64yyyxxyxx + 63yyyxxyxy + 88yyyxxyyx - 91yyyxyxxx - 22yyyxyxxy - 96yyyxyxyx + 64yyyxyxyy + 43yyyxyyyx + 86yyyxyyyy + 92yyyyxxyx + 30yyyyxxyy - 164yyyyxyyy + 159yyyyyxxy + 39yyyyyxyx - 79yyyyyxyy - 54yyyyyyxy + 134yyyyyyyy + 88xxxxxxx + 69xxxxxxy + 75xxyxxxx + 81xxyxxxy + 155xxyxxyx + 149xxyxxyy - 140xxyxyxx - 108xxyxyyx - 128xxyyxxy + 71xxyyxyx + 151xxyyxyy - 4xxyyyxx + 90xxyyyxy - 86xyxxxxy + 53xyxxyxx + 127xyxxyxy + 121xyxxyyx + 52xyxyxxx + 51xyxyxxy + 31xyxyxyx + 105xyxyxyy + 38xyxyyxx + 74xyxyyxy + 153xyyxxxx - 117xyyxxxy + 49xyyxxyx + 143xyyxxyy + 135xyyxyxx - 44xyyxyxy + 84xyyxyyx + 7xyyxyyy + 154xyyyxxx + 125xyyyxxy - 38xyyyxyx + 21xyyyxyy + 49xyyyyxx - 115xyyyyxy - 133xyyyyyx + 124xyyyyyy + 149yxxxxxx + 126yxxxxxy + 21yxxyxxx - 25yxxyxxy - 66yxxyxyx + 5yxxyxyy + 39yxxyyxx + 100yxxyyxy - 130yxyxxxx + 162yxyxxxy + 13yxyxxyx + 129yxyxxyy + 136yxyxyxx - 6yxyxyyx + 118yxyyxxx + 145yxyyxxy + 9yxyyxyx + 83yxyyxyy + 139yxyyyxx + 3yxyyyxy + 116yxyyyyx + 129yxyyyyy + 22yyxxxxx - 154yyxxxxy + 77yyxxyxx + 143yyxxyxy - 108yyxxyyx + 161yyxyxxx - 136yyxyxxy - 77yyxyxyx + 48yyxyxyy + 53yyxyyxx + 9yyxyyxy - 150yyxyyyx + 112yyxyyyy + 33yyyxxxx -$$

$$22yyyxxxy + 145yyyxxyx + 56yyyxxyy + 131yyyxyxx - 93yyyxyxy + 92yyyxyyx - 145yyyxyyy - 18yyyyxxx + 121yyyyxxy + 8yyyyxyx + 19yyyyxyy - 82yyyyyxx + 132yyyyyxy + 66yyyyyyx - 59yyyyyyy + 92xxxxxx + 69xxxxxy + 93xxyxxx + 24xxyxxy - 15xxyxyx + 140xxyxyy + 106xxyyxx - 8xxyyxy - 48xxyyyx + 113xyxxxx - 21xyxxxy + 148xyxxyx + 148xyxxyy - 54xyxyxx - 88xyxyxy + 92xyxyyx - 3xyyxxx - 6xyyxxy - 5xyyxyx + 61xyyxyy - 147xyyyxx - 58xyyyxy - 86xyyyyx - 141xyyyyy + 122yxxxxx - 44yxxxxy + 69yxxyxx - 116yxxyxy - 25yxxyyx - 153yxyxxx - 75yxyxxy - 10yxyxyx + 60yxyxyy - 100yxyyxx + 131yxyyxy - 125yxyyyx - 95yxyyyy + 13yyxxxx + 33yyxxxy + 140yyxxyx + 108yyxxyy - 69yyxyxx + 64yyxyxy + 123yyxyyx + 86yyxyyy - 29yyyxxx + 40yyyxxy + 78yyyxyx + 86yyyxyy + 165yyyyxx + 140yyyyxy - 86yyyyyx + 77yyyyyy + 42xxxxx + 22xxxxy - 48xxyxx + 16xxyxy - 106xxyyx + 79xxyyy - 13xyxxx - 149xyxxy - 50xyxyx + 123xyxyy + 85xyyxx + 102xyyxy + 72xyyyx - 158xyyyy - 6yxxxx - 31yxxxy - 110yxxyx + 50yxxyy + 83yxyxx + 4yxyxy + 21yxyyx + 45yxyyy - 104yyxxx - 128yyxxy - 91yyxyx + 91yyxyy + 85yyyxx + 162yyyxy + 165yyyyx + 73yyyyy - 20xxxx - 105xxxy - 154xxyx + 126xxyy - 11xyxx - 25xyxy - 10xyyx + 101xyyy + 101yxxx + 57yxxy - 12yxyx + 85yxyy + 12yyxx - 106yyxy + 111yyyx - 94yyyy + 25xxx + 13xxy - 35xyx + 36xyy - 132yxx + 53yxy - 70yyx - 145yyy + 37xx + 65xy + 30yx + 165yy - 97x + 75y - 129,$$

$$xxyyyxxyy + 51xyxyyxxyx + 91xyxyyxxyy + 159xyxyyxyyy - 71xyyxxyxyx + 30xyyxxyxyy + 134xyyxyyyyx - 10xyyxyyyyy + 30yxxyyxxyy - 32yxxyyxyyy - 38yxyxxyxyx - 136yxyxyxxyx + 153yxyxyxxyy - 139yxyxyyyxyx + 115yxyxyyyxyy - 49yxyyyxxyx - 150yxyyyxxyy - 60yxyyyxyyy - 34yxyyyyyxyx + 164yxyyyyyxyy - 64yyxxyyyxyx + 72yyxxyyyxyy - 103yyxyyyxxyx - 91yyxyyyxxyy + 121yyxyyyxyyy + 24yyxyyyyxyx - 27yyxyyyyxyy + 76yyyxxyxyy + 43yyyxyxxyx - 7yyyxyxxyy - 17yyyxyyyyy + 105xxyyyxxyy + 131xxyyyxyyy - 117xxyyyyxxy + 82xxyyyyxyy - 43xyxxyxyx + 108xyxxyxyy + 22xyxyxxxy - 107xyxyxxyx - 59xyxyxxyy + 28xyxyxyxx + 35xyxyxyyx + 26xyxyyxxx + 61xyxyyxxy - 116xyxyyxyx + 128xyxyyxyy + 140xyyxxyxx - 131xyyxxyxy + 126xyyxxyyx - 83xyyxyxyx - 136xyyxyxyy + 75xyyxyyyx + 28xyyxyyyy + 94xyyyxxyx + 81xyyyxxyy - 139xyyyxyyy + 68xyyyyxyx + 3xyyyyxyy + 87xyyyyyyx - 130xyyyyyyy - 151yxxxxxxy + 77yxxyxxxy - 159yxxyxxyy - 81yxxyxyxx - 7yxxyxyyx + 134yxxyyxxy - 57yxxyyxyx - 106yxxyyxyy - 144yxyxxxxy + 116yxyxxyxx + 77yxyxxyxy - 127yxyxxyyx + 41yxyxyxxx - yxyxyxxy + 20yxyxyyxx - 57yxyxyyxy - 160yxyyxxyx + 100yxyyxxyy + 46yxyyxyyy - 12yxyyyxxx - 121yxyyyxxy + 31yxyyyxyx - 42yxyyyxyy + 93yxyyyyxx + 96yxyyyyxy - 111yxyyyyyx + 106yyxxxxxy - 102yyxxyxyx - 139yyxxyxyy - 117yyxxyyxx + 19yyxxyyxy - 146yyxyxxxy + 79yyxyxxyx + 58yyxyxxyy -$$

$$130yyyxyxyxx + 30yyyxyxyyx - 59yyyxyyxxx - 47yyyxyyxxy - 114yyyxyyxyx + 9yyyxyyxyy - 163yyyxyyyxx + 117yyyxyyyxy - 147yyyxyyyyx - 13yyyxyyyyy - 164yyyyxxxxy - 8yyyyxxyxx - 153yyyyxxyxy - 11yyyyxxyyx - 30yyyyxyxxx - 80yyyyxyxxy + 12yyyyxyxyx - 8yyyyxyxyy + 36yyyyxyyyx - 145yyyyxyyyy - 24yyyyyxxyx + 113yyyyyxxyy - 56yyyyyxyyy - 130yyyyyyxyx + 126yyyyyyxyy + 110yyyyyyyyy + 111xxxxxxy + 34xxyxxxy - 50xxyxxyx + 49xxyxxyy + 57xxyxyxx + 12xxyxyyx - 164xxyyyxy - 148xxyyyxyx - 62xxyyyxyy + 125xxyyyyx - 47xxyyyyy - 23xyxxxxy - 87xyxxyxx + 156xyxxyxy - 152xyxxyyx - 68xyxyxxx + 140xyxyxxy - 19xyxyxyx - 59xyxyxyy + 46xyxyyxx - 136xyxyyxy + 156xyyxxxx - 114xyyxxxy - 145xyyxxyx - 74xyyxxyy + 77xyyxyxx - 63xyyxyxy + 10xyyxyyx - 8xyyxyyy - 4xyyyxxx - 50xyyyxxy + 59xyyyxyx - 83xyyyxyy + 145xyyyyxx + 139xyyyyxy + 76xyyyyyx - 58xyyyyyy - 64yxxxxxx - 72yxxxxxy - 28yxxyxxx - 164yxxyxxy + 134yxxyxyx - 121yxxyxyy + 2yxxyyxx + 20yxxyyxy + 11yxyxxxx - 135yxyxxxy + 153yxyxxyx + 147yxyxxyy + 122yxyxyxx - 35yxyxyyx - 127yxyyxxx + 54yxyyxxy - 144yxyyxyx + 67yxyyxyy + 48yxyyyxx - 159yxyyyxy + 7yxyyyyx + 86yxyyyyy + 80yyxxxxx - 40yyxxxxy - 57yyxxyxx - 134yyxxyxy + 135yyxxyyx - 55yyxyxxx - 69yyxyxxy + 111yyxyxyx - 133yyxyxyy - 48yyxyyxx + 5yyxyyxy - 27yyxyyyx + 30yyxyyyy + 120yyyxxxx + 104yyyxxxy + 154yyyxxyx - 3yyyxxyy + 25yyyxyxx + 21yyyxyxy + 154yyyxyyx + 31yyyxyyy + 163yyyyxxx - 42yyyyxxy - 71yyyyxyx - 152yyyyxyy + 83yyyyyxx + 121yyyyyxy + 93yyyyyyx - 146yyyyyyy + 115xxxxxx + 70xxxxxy - 44xxyxxx - 10xxyxxy - 19xxyxyx - 72xxyxyy + 32xxyyxx + 39xxyyxy + 31xxyyyx + 13xyxxxx - 141xyxxxy - 32xyxxyx - 22xyxxyy + 24xyxyxx - 155xyxyxy - 110xyxyyx + 62xyyxxx - 85xyyxxy - 42xyyxyx - 103xyyxyy + 29xyyyxx + 42xyyyxy + 8xyyyyx - 101xyyyyy - 9yxxxxx + 11yxxxxy + 103yxxyxx - 142yxxyxy + 96yxxyyx + 51yxyxxx - 85yxyxxy + 152yxyxyx + 64yxyxyy + 41yxyyxx - 93yxyyxy + 97yxyyyx - 57yxyyyy + 142yyxxxx + 102yyxxxy - 142yyxxyx + 94yyxxyy + 124yyxyxx + 66yyxyxy - 93yyxyyx + 156yyxyyy + 50yyyxxx + 48yyyxxy + 122yyyxyx - 74yyyxyy + 26yyyyxx + 124yyyyxy - 124yyyyyx + 85yyyyyy - 115xxxxx - 71xxxxy - 19xxyxx + 121xxyxy - 109xxyyx + 161xxyyy + 52xyxxx - 99xyxxy + 136xyxyx - 121xyxyy + 133xyyxx + 153xyyxy + 63xyyyx + 158xyyyy - 30yxxxx + 45yxxxy - 16yxxyx - 27yxxyy + 147yxyxx - 144yxyxy - 77yxyyx + 36yxyyy + 57yyxxx - 94yyxxy - 19yyxyx + 44yyxyy + 106yyyxx + 126yyyxy + 106yyyyx + 37yyyyy + 38xxxx + 135xxxy + 74xxyx - 49xxyy - 41xyxx - 163xyxy - 12xyyx - 50xyyy - 42yxxx + 127yxxy - 52yxyx - 134yxyy + 68yyxx - 41yyxy + 43yyyx - 25yyyy - 129xxx + 150xxy - 8xyx + 123xyy - 165yxx + 29yxy + 45yyx - 124yyy - 53xx + 137xy + 151yx + 142yy + 145x + 20y + 161,$$

$$xyyyyxyyx + 118xyxxyxyxx - 50xyxxyxyyx - 109xyxxyyyxyx + 164xyxxyyxyy - 72xyxyxxyxx - 130xyxyxxyxy - 137xyxyxxyyx + 61xyxyyyxxyx - 79xyxyyyxxyy + 55xyxyyyxyyx - 118xyxyyyxyyy + 121xyyyxxyxyx - 61xyyyxxyxyy - 8xyyyxyxxyx + 9xyyyxyxxyy - 100xyyyxyyyyx + 126xyyyxyyyyy - 64xyyyyyyyyx + 72xyyyyyyyyy - 128yxxxyxxyyx - 53yxxyyyxxyy + 92yxxyyyxyyx + 70yxxyyyxyyy - 11yxyxxyxyx - 26yxyxyxxyx + 112yxyxyxxyy + 42yxyxyyyxyx - 130yxyxyyyxyy + 130yxyyyyxxyx + 29yxyyyyxxyy + 131yxyyyyxyyx + 143yxyyyyxyyy - 152yxyyyyyxyx - 117yxyyyyyxyy - 14yyxxyyyxyx - 67yyxxyyyxyy - 157yyxyyyxxyx - 113yyyxyyxxyy - 108yyyxyyyxyyy + 88yyyxyyyyxyx - 99yyyxyyyyxyy + 58yyyyxxyxyy - 63yyyyxyxxyx - 136yyyyxyxxyy + 48yyyyxyyyyy-89xxxxxxxy+108xxyxxxxy-162xxyxxyxx+125xxyxxyyyx-5xxyxyxxx-56xxyxyyxx-42xxyyxxyy-13xxyyxyyx-152xxyyxyyy-142xxyyyyxy+117xxyyyyxyy-89xyxxxxxy+5xyxxyxxx+103xyxxyxyx+89xyxxyxyy-38xyxxyyxx-159xyxxyyxy+158xyxyxxxx-50xyxyxxxy-66xyxyxxyx-2xyxyxxyy-90xyxyxyxx-9xyxyxyyx+96xyxyyyxx-83xyxyyyxy-149xyxyyyxyx-142xyxyyyxyy+69xyyyxxxxy-28xyyyxxyxx-34xyyyxxyxy+129xyyyxxyyx-56xyyyxyxxx-39xyyyxyxxy-165xyyyxyxyx-63xyyyxyxyy-165xyyyxyyyx+44xyyyxyyyy-150xyyyyxxyx+43xyyyyxxyy+162xyyyyxyyx-149xyyyyxyyy+140xyyyyyxyx-78xyyyyyxyy-76xyyyyyyyx+116xyyyyyyyy-2yxxxxxxy+29yxxyxxxy+120yxxyxxyy+16yxxyxyxx+71yxxyxyyx-19yxxyyyxy+94yxxyyyxyx-114yxxyyyxyy+112yxyxxxxy + 142yxyxxyxx + 152yxyxxxyx + 144yxyxxyyx + 149yxyxyxxx - 44yxyxyxxy-37yxyxyyxx+122yxyxyyxy+9yxyyxxyx+142yxyyxxyy+35yxyyxyyx+65yxyyxyyy-83yxyyyxxx+104yxyyyxxy+39yxyyyxyx+83yxyyyxyy-65yxyyyyxx+64yxyyyyxy-36yxyyyyyx-163yyxxxxxy-10yyxxyxyx-72yyxxyxyy-98yyxxyyxx-151yyxxyyxy-94yyxyxxxy+49yyxyxxyx-151yyxyxxyy+75yyxyxyxx+110yyxyxyyx-106yyxyyxxx-62yyxyyxxy-87yyxyyyxx+33yyxyyyxy-46yyxyyyxx+98yyxyyyxy-124yyxyyyyx+51yyxyyyyy-160yyyxxxxy+81yyyxxyxx+101yyyxxyxy+70yyyxxyyx-110yyyxyxxx+148yyyxyxxy+44yyyxyxyx+81yyyxyxyy+132yyyxyyyx+20yyyxyyyy+76yyyyxxyx-113yyyyxxyy+48yyyyxyyx-10yyyyxyyy+161yyyyyxyx-160yyyyyxyy+161yyyyyyyx - 95yyyyyyyy + 39xxxxxxx - 73xxxxxxy - 82xxyxxxx - 130xxyxxxy - 82xxyxxyx + 21xxyxxyy - 43xxyxyxx - 100xxyxyyx - 65xxyyxxx - 24xxyyxxy + 83xxyyxyx - 163xxyyxyy + 122xxyyyxx - 25xxyyyxy - 81xyxxxxx - 131xyxxxxy + 11xyxxyxx + 138xyxxyxy + 106xyxxyyx + 14xyxyxxx + 82xyxyxxy + 106xyxyxyx + 156xyxyxyy + 28xyxyyxx - 162xyxyyxy - 15xyyxxxx + 111xyyxxxy - 142xyyxxyx - xyyxxyy - 40xyyxyxx + 100xyyxyxy + 133xyyxyyx - 89xyyxyyy - 57xyyyxxx + 12xyyyxxy + 132xyyyxyx + 18xyyyxyy + 161xyyyyxx - 100xyyyyxy + 50xyyyyyx -$$

$$31xyyyyyy - 14yxxxxxx + 79yxxxxxy + 2yxxyxxx + 107yxxyxxy + 39yxxyxyx - 12yxxyxyy - 96yxxyyxx - 101yxxyyxy - 16yxyxxxy - 16yxyxxyx + 74yxyxxyy + 163yxyxyxx - 151yxyxyyx + 63yxyyxxx + 27yxyyxxy - 49yxyyxyx + 52yxyyxyy - 9yxyyyxx + 119yxyyyxy + 85yxyyyyx + 36yxyyyyy - 148yyxxxxx + 81yyxxxxy - 23yyxxyxx - 92yyxxyxy + 6yyxxyyx - 121yyxyxxx + 146yyxyxxy + 54yyxyxyx - 90yyxyxyy + 155yyxyyxx - 92yyxyyxy + 108yyxyyyx - 144yyxyyyy + 109yyyxxxx - 60yyyxxxy + 165yyyxxyx + 141yyyxxyy - 129yyyxyxx + 77yyyxyxy - 149yyyxyyx + 144yyyxyyy - 130yyyyxxx + 125yyyyxxy + 86yyyyxyx + 136yyyyxyy - 119yyyyyxx + 120yyyyyxy + 146yyyyyyx - 84yyyyyyy - 11xxxxxx + 51xxxxxy - 12xxyxxx - 161xxyxxy - 132xxyxyx - 148xxyxyy + 116xxyyxx + 35xxyyxy - 54xxyyyx - 16xyxxxx + 142xyxxxy - 110xyxxyx - 5xyxxyy - 51xyxyxx + 14xyxyxy + 41xyxyyx + 13xyyxxx - 42xyyxxy - 112xyyxyx + 20xyyxyy + 145xyyyxx - 108xyyyxy - 74xyyyyx + 140xyyyyy - 35yxxxxx + 165yxxxxy - 94yxxyxx - 134yxxyxy + 106yxxyyx + 88yxyxxx - 126yxyxxy - 129yxyxyx - 59yxyxyy + 36yxyyxx - 135yxyyxy - 62yxyyyx + 47yxyyyy + 34yyxxxx - 19yyxxxy + 23yyxxyx + 65yyxxyy + 126yyxyxx + 155yyxyxy - 40yyxyyx - 90yyxyyy + 144yyyxxx + 101yyyxxy - 159yyyxyx + 7yyyxyy - 25yyyyxx - 130yyyyxy + 126yyyyyx - 85yyyyyy - 38xxxxx - 80xxxxy - 110xxyxx + 9xxyxy + 43xxyyx - 162xxyyy + 60xyxxx + 69xyxxy - 24xyxyx - 76xyxyy + 49xyyxx - 147xyyxy + 36xyyyx + 96xyyyy + 97yxxxx + 57yxxxy + 119yxxyx - 21yxxyy + 76yxyxx + 30yxyxy + 86yxyyx + 123yxyyy + 18yyxxx + 35yyxxy - 61yyxyx + 39yyxyy - 35yyyxx - 110yyyxy - 87yyyyx + 11yyyyy + 113xxxx - 115xxxy + 46xxyx + 65xxyy + 120xyxx - 33xyxy - xyyx + 103xyyy - 96yxxx - 70yxxy + 30yxyx - 165yxyy - 106yyxx + 120yyxy + 145yyyx - 159yyyy + 162xxx - 101xxy - 46xyx - 20xyy + 120yxx - 23yxy + 32yyx - 107yyy + 82xx + 159xy + 79yx - 43yy + 94x - 99y - 53,$$

$$yxyxyxxyxy + 62yxyxyyxyxy - 131yyxxyyxyxy - 75yyxyyyxyxy - 38yyyxyxxyxy + 72yyyxyyyyxy - 158xyxyxxyxy + 44xyxyyxyxy - 34yxyxxyxyx + 7yxyxyxxxy - 89yxyxyxxyx - 76yxyxyxxyy + 103yxyxyyxxy + 57yxyxyyxyx + 146yxyxyyxyy + 130yxyyyxyxy - 8yyxxyxxyy + 76yyxxyyxxy - 19yyxxyyxyx - 159yyxxyyxyy + 83yyxyxxyxy - 121yyxyxyxxy + 35yyxyxyyxy + 36yyxyyxxyx + 125yyxyyxxyy - 111yyxyyxyxy - 68yyxyyxyyy + 137yyxyyyxxy - 117yyxyyyxyx + 101yyxyyyxyy + 71yyxyyyyxy + 58yyyxxyxxy + 12yyyxxyxyy - 115yyyxxyyxy + 65yyyxyxxxy - 145yyyxyxxyx - 75yyyxyxxyy - 128yyyxyyyxy + 158yyyxyyyyx + 74yyyxyyyyy + 35yyyyxxyxy - 79yyyyxyyyy + 18yyyyyxyxy - 57yyyyyyyxy - 84xxyyxyxy + 14xyxxyxyx - 113xyxyxxxy - 150xyxyxxyx + 27xyxyxxyy - 23xyxyyxxy - 77xyxyyxyx + 157xyxyyxyy - 42xyyxxyxy + 33xyyxyyyy + 127xyyyxyxy + 76xyyyyyyy - 10yxxxxxxy - 114yxxyxxyy -$$

$$52yxxyxyxx - 119yxxyxyyx + 95yxyxxxxy - 38yxyxxyxx + 53yxyxxyxy - 51yxyxxyyx +$$
$$39yxyxyxxx + 88yxyxyxxy + 68yxyxyyxx - 75yxyxyyxy + 79yxyyxxyx - 98yxyyxxyy -$$
$$26yxyyxyxy - 128yxyyxyyy - 83yxyyyxxy - 62yxyyyxyx - 153yxyyyxyy + 91yxyyyyxy +$$
$$56yyxxxxxy + 70yyxxyxxy - 100yyxxyxyx + 80yyxxyxyy - 133yyxxyyxx - 136yyxxyyxy -$$
$$80yyxyxxxy - 110yyxyxxyx - 64yyxyxxyy - 62yyxyxyxx + 143yyxyxyyx - 79yyxyyxxx -$$
$$23yyxyyxxy + 75yyxyyxyx - 17yyxyyxyy - 157yyxyyyxx - 130yyxyyyxy + 14yyxyyyyx +$$
$$117yyxyyyyy + 124yyyxxxxy - 24yyyxxxyx - 25yyyxxyxy + 89yyyxxyyx - 22yyyxyxxx +$$
$$146yyyxyxxy - 113yyyxyxyx - 33yyyxyxyy + 140yyyxyyxy - 161yyyxyyyx - yyyxyyyy -$$
$$86yyyyxxxy + 97yyyyxxyx + 117yyyyxxyy - 165yyyyxyxy - 50yyyyxyyy + 126yyyyyxxy +$$
$$134yyyyyxyx - 11yyyyyxyy + 119yyyyyyxy + 68yyyyyyyx - 65yyyyyyyy + 82xxxxxxy +$$
$$107xxyxxyx - 65xxyxxyy - 37xxyxyxx + 49xxyxyyx + 74xxyyxxy + 147xxyyxyx -$$
$$59xxyyxyy + 100xxyyyxy - 117xyxxxxy + 113xyxxyxx + 110xyxxyxy + 21xyxxyyx -$$
$$57xyxyxxx - 113xyxyxxy + 127xyxyxyx + 154xyxyxyy + 123xyxyyxx - 89xyxyyxy +$$
$$37xyyxxxy - xyyxxyx + 160xyyxxyy - 79xyyxyxy - 119xyyxyyy - 104xyyyxxy +$$
$$26xyyyxyx - 96xyyyxyy - 19xyyyyxy + 27xyyyyyy - 70yxxxxxx - 32yxxxxxy -$$
$$33yxxyxxx + 75yxxyxxy + 16yxxyxyx + 31yxxyxyy - 14yxxyyxx - 87yxxyyxy +$$
$$79yxyxxxx - 111yxyxxxy + 112yxyxxyx + 38yxyxxyy - 36yxyxyxx - 135yxyxyyx -$$
$$109yxyyxxx + 32yxyyxxy + 158yxyyxyx + 146yxyyxyy - 103yxyyyxx - 100yxyyyxy -$$
$$34yxyyyyx + 61yyxxxxx + 83yyxxxxy + 90yyxxyxx + 40yyxxyxy - 39yyxxyyx +$$
$$98yyxyxxx + 78yyxyxxy - 151yyxyxyx + 62yyxyxyy + 52yyxyyxx - 101yyxyyxy +$$
$$22yyxyyyx - 121yyxyyyy - 156yyyxxxx + 150yyyxxxy - 34yyyxxyx + 142yyyxxyy -$$
$$24yyyxyxx - 67yyyxyxy - 116yyyxyyx + 59yyyxyyy + 17yyyyxxx - 155yyyyxxy -$$
$$83yyyyxyx - 12yyyyxyy - 55yyyyyxx + 163yyyyyxy + 13yyyyyyx - 164yyyyyyy -$$
$$88xxxxxx + 124xxxxxy + 159xxyxxx + 24xxyxxy - 149xxyxyx - 51xxyxyy - 114xxyyxx -$$
$$80xxyyxy - 162xxyyyx - 52xyxxxx + 119xyxxxy + 133xyxxyx - 119xyxxyy + 78xyxyxx +$$
$$121xyxyxy - 75xyxyyx - 7xyyxxx + 140xyyxxy - 15xyyxyx + 121xyyxyy - 149xyyyxx -$$
$$106xyyyxy - 23xyyyyx + 144xyyyyy - 86yxxxxx - 158yxxxxy + 25yxxyxx - 5yxxyxy +$$
$$94yxxyyx - 19yxyxxx + 136yxyxxy + 36yxyxyx - 47yxyxyy - 110yxyyxx - 33yxyyxy -$$
$$155yxyyyx + 37yxyyyy + 91yyxxxx + 162yyxxxy + 123yyxxyx + 145yyxxyy + 72yyxyxx +$$
$$57yyxyxy + 155yyxyyx + 121yyxyyy - 23yyyxxx - 20yyyxxy + 30yyyxyx + 108yyyxyy +$$
$$73yyyyxx + 147yyyyxy - 80yyyyyx + 18yyyyyy - 65xxxxx + 70xxxxy + 155xxyxx -$$
$$50xxyxy - 154xxyyx - 30xxyyy + 77xyxxx + 136xyxxy + 61xyxyx - 47xyxyy + 33xyyxx +$$
$$18xyyxy + 37xyyyx + 97xyyyy - 106yxxxx + 73yxxxy - 120yxxyx + 102yxxyy + 42yxyxx +$$
$$28yxyxy + 27yxyyx + 12yxyyy + 149yyxxx + 37yyxxy + 33yyxyx + 20yyxyy + 103yyyxx +$$

$$127yyyxy + 67yyyyx - 68yyyyy - 3xxxx + 48xxxy - 28xxyx + 152xxyy - 109xyxx - 69xyxy - 154xyyx + 119xyyy + 44yxxx - 62yxxy + 77yxyx - 143yxyy - 145yyxx + 143yyxy + 50yyyx - 131yyyy + 10xxx - 150xxy + 148xyx + 22xyy + 10yxx + 104yxy - 104yyx - 148yyy + 50xx - 43xy - 134yx - 87yy - 64x + 160y + 77,$$

$$yxyxyyxyyy + 110yyxxyyxyyy - 124yyxyyyxyyy - 42xyxyyxyyy - 52yxyxxyxyx - 51yxyxyxxyx + 16yxyxyxxyy + 107yxyxyyxyx + 26yxyxyyxyy - 94yxyyyxyyy - 146yyxxyyyxyx - 119yyxxyyyxyy + 93yyxyyxxyx - 146yyxyyxxyy - 165yyxyyyxyyy - 28yyxyyyyxyx + 86yyxyyyyxyy - 10yyyxxyxyx + 124yyyxxyxyy + 109yyyyxyxxyx - 164yyyyxyxxyy - 150yyyxyyyyx + 51yyyxyyyyy + 43yyyyyxyyy + 20xxyyxyyy - 59xyxxyxyx + 6xyxxyxyy + 114xyxyxxyx + 120xyxyxxyy + 140xyxyyxyx - 99xyxyyxyy - 46xyyyxyyy + 69yxxxxxxy - 92yxxyxxyy + 14yxxyxyxx - 108yxxyxyyx - 156yxyxxxxy + 15yxyxxyxx - 124yxyxxxyx - 132yxyxxyyx - 26yxyxyxxx + 41yxyxyxxy + 87yxyxyyxx - 53yxyxyyxy - 102yxyyxxyx + 48yxyyxxyy - 82yxyyxyyy - 128yxyyyxyx - 127yxyyyxyy + 162yyxxxxxy + 2yyxxyxyx - 8yyxxyxyy - 29yyxxyyxx + 128yyxxyyxy - 16yyxyxxxy - 58yyxyxxyx + 29yyxyxxyy - 55yyxyxyxx - 36yyxyxyyx - 11yyxyyxxx + 81yyxyyxxy + 123yyxyyxyx + 26yyxyyxyy + 135yyxyyyxx - 48yyxyyyxy + 80yyxyyyyx + 55yyxyyyyy - 154yyyxxxxy + 134yyyxxyxx + 118yyyxxyxy + 108yyyxxyyx + 101yyyxyxxx + 159yyyxyxxy + 25yyyxyxyx - 83yyyxyxyy - 9yyyxyyyx + 137yyyyxxyx + 8yyyyxxyy + 106yyyyxyyy - 33yyyyyxyx + 125yyyyyxyy + 36yyyyyyyx + yyyyyyyy + 30xxxxxy + 138xxyxxyx + 53xxyxxyy + 150xxyxyxx + 25xxyxyyx + 154xxyyxyx - 142xxyyxyy - 60xyxxxxy + 54xyxxyxx - 54xyxxyxy + 2xyxxyyx + 136xyxyxxx + 142xyxyxxy + xyxyxyx + 152xyxyxyy - 13xyxyyxx - 91xyxyyxy + 139xyyxxyx + 138xyyxxyy + 68xyyxyyy + 43xyyyxyx + 128xyyyxyy + 61xyyyyyy + 152yxxxxxx + 103yxxxxxy + 98yxxyxxx - 73yxxyxxy + 59yxxyxyx - 132yxxyxyy - 149yxxyyxx - 94yxyxxxx - 154yxyxxxy - 82yxyxxyx + 47yxyxxyy + 156yxyxyxx + 32yxyxyyx - 52yxyyxxx + 151yxyyxxy - 124yxyyxyx - 113yxyyxyy + 97yxyyyxx + 17yxyyyxy + 38yxyyyyx - 97yxyyyyy + 141yyxxxxx - 50yyxxxxy + 104yyxxyxx - 24yyxxyxy + 93yyxxyyx + 90yyxyxxx - 29yyxyxxy + 155yyxyxyx - 80yyxyxyy + 96yyxyyxx + 52yyxyyxy + 100yyxyyyx + 131yyxyyyy + 19yyyxxxx + 28yyyxxxy - 16yyyxxyx - 46yyyxxyy - 106yyyxyxx - 148yyyxyxy + 102yyyxyyx - 86yyyxyyy - 34yyyyxxx + 126yyyyxxy + 6yyyyxyx + 6yyyyxyy + 100yyyyyxx + 38yyyyyxy + 14yyyyyyx + 128yyyyyyy - 121xxxxxx + 152xxxxxy + 30xxyxxx - 3xxyxxy + 118xxyxyx + 52xxyxyy + 49xxyyxx - 67xxyyxy + 70xxyyyx - 130xyxxxx + 11xyxxxy + 49xyxxyx + 12xyxxyy - 111xyxyxx - 160xyxyxy - 40xyxyyx - 20xyyxxx - 16xyyxxy + 83xyyxyx - 43xyyxyy - 30xyyyxx + 121xyyyxy + 60xyyyyx - 101xyyyyy - 165yxxxxx + 77yxxxxy -$$

$$143yxxyxx+128yxxyxy+85yxxyyx-146yxyxxx+83yxyxxy+30yxyxyx-105yxyxyy+5yxyyxx+119yxyyxy+102yxyyyx-46yxyyyy-102yyxxxx-57yyxxxy-106yyxxyx-143yyxxyy+135yyxyxx+137yyxyxy-6yyxyyx-87yyxyyy+91yyyxxx-yyyxxy-108yyyxyx-123yyyxyy+150yyyyxx+56yyyyxy+119yyyyyx+116yyyyyy-12xxxxx+150xxxxy-49xxyxx+19xxyxy+150xxyyx+72xxyyy-99xyxxx+57xyxxy+35xyxyx+109xyxyy+134xyyxx+14xyyxy-128xyyyx+12xyyyy+24yxxxx+133yxxxy+160yxxyx+69yxxyy-43yxyxx-150yxyxy-130yxyyx+112yxyyy-124yyxxx+91yyxxy-130yyxyx+31yyxyy-27yyyxx+134yyyxy+69yyyyx+161yyyyy+14xxxx+137xxxy+156xxyx+88xxyy+18xyxx+24xyxy+31xyyx+152xyyy-98yxxx+8yxxy+104yxyx+76yxyy+108yyxx-82yyxy+27yyyx+88yyyy+47xxx+111xxy+94xyx+100xyy-157yxx-152yxy+149yyx-126yyy+129xx-21xy+30yx+158yy-68x-93y-36\}$$

Example 4.2:- Let $K = \mathbb{Z}_{331},\ K\langle x,y\rangle = \mathbb{Z}_{331}\langle x,y\rangle$.

Let $g = xy + 7x + 13y + 11 \in K\langle x,y\rangle$ be the private key.

Let $f_1 = xx + 170xy + 295yx + 61x + y + 274,\ h_1 = yy + 116x + 133y + 9$
$f_2 = xx + 248xy + 182yx + 316x + 17y + 1,\ h_2 = yy + 196x + 128y - 232$
$f_3 = xx + 9xy + 83yx + 94x + 282y + 177,\ h_3 = yy + 252x + 83y + 44$
$f_4 = xx + 105xy + 40yx + 23x + 219y + 47,\ h_4 = yy + 73x + 7y + 38$
$f_5 = xx + 93xy + 176yx + 301x + 58y + 302,\ h_5 = yy + 75x + 181y + 43.$

Then, we have:

$q_1 = f_1gh_1 = xxxyyy - 161xyxyyy - 36yxxyyy + 116xxxyx + 140xxxyy + 74xxyyy - 140xyxyx - 32xyxyy - 107xyyyy + 127yxxyx - 75yxxyy - 136yxyyy + 150xxxx - 53xxxy - 22xxyx + 19xxyy + 13xyxx - 73xyxy - 165xyyx - 40xyyy - 104yxxx - 78yxxy + 112yxyx + 59yxyy + 13yyyy - 103xxx + 2xxy - 120xyx + 12xyy - 59yxx - 1yxy - 147yyx + 6yyy + 77xx + 50xy - 135yx + 45yy - 112x + 71y - 16,$

$q_2 = f_2gh_2 = xxxyyy - 83xyxyyy - 149yxxyyy - 135xxxyx + 135xxxyy - 2xxyyy - 49xyxyx + 49xyxyy - 86xyyyy - 76yxxyx + 76yxxyy + 66yxyyy + 48xxxx + 2xxxy - 61xxyx - 19xxyy - 12xyxx + 165xyxy + 25xyyx + 132xyyy + 130yxxx + 33yxxy + 27yxyx - 23yxyy - 110yyyy + 143xxx + 17xxy - 92xyx - 94xyy - 5yxx - 18yxy - 45yyx + 22yyy + 108xx - 65xy - 64yx + 157yy + 85x + 24y + 96$

$q_3 = f_3gh_3 = xxxyyy + 9xyxyyy + 83yxxyyy - 79xxxyx + 90xxxyy + 107xxyyy - 49xyxyx + 148xyxyy + 117xyyyy + 63yxxyx - 143yxxyy + 37yxyyy + 109xxxx - 37xxxy + 153xxyx - 49xxyy - 12xyxx - 2xyxy + 25xyyx - 45xyyy + 110yxxx - 92yxxy + 56yxyx + 25yyyy + 86xxx - 7xxy - 51xyx + 17xyy + 63yxx - 50yxy + 11yyx - 135yyy + 143xx + 32xy + 77yx + 12yy + 152x + 147y - 61$

$q_4 = f_4gh_4 = xxxyyy + 105xyxyyy + 40yxxyyy + 73xxxyx + 14xxxyy + 36xxyyy + 52xyxyx + 146xyxyy + 41xyyyy - 59yxxyx - 102yxxyy + 77yxyyy - 151xxxx + 87xxxy - 20xxyx + 93xxyy + 33xyxx - 133xyxy + 14xyyx + 133xyyy - 82yxxx - 161yxxy - 6yxyx - 136yxyy - 132yyyy - 87xxx - 76xxy + 138xyx + 69xyy + 92yxx - 144yxy - 37yyx + 110yyy + 34xx - 123xy - 149yx + 91yy - 54x - 119y + 117$

$q_5 = f_5gh_5 = xxxyyy + 93xyxyyy - 155yxxyyy + 75xxxyx - 143xxxyy - 17xxyyy + 24xyxyx - 59xyxyy - 115xyyyy - 40yxxyx - 12yxxyy + 29yxyyy - 137xxxx - 14xxxy + 49xxyx + 34xxyy - 163xyxx + 22xyxy - 19xyyx - 20xyyy + 51yxxx - 147yxxy - 142yxyx - 22yxyy + 92yyyy - 60xxx - 9xxy + 142xyx - 88xyy - 95yxx + 145yxy - 51yyx + 32yyy + 125xx + 2xy + 128yx - 96yy + 158x + 155y - 146$

Set $B = \{q_1, q_2, q_3, q_4, q_5\}$ as the public key. Note that this is the same set described in example 3.5.2.

To encrypt a message, we create a polynomial, p, as follows:

Let $F_1 = xxx - 98,\ H_1 = yyy + 97$

$F_2 = xxx + 79,\ H_2 = yyy + 9$

$F_3 = xxx + 1,\ H_3 = yyy - 5$

$F_4 = xxx + 59,\ H_4 = yyy - 160$

$F_5 = xxx + 47,\ H_5 = yyy + 33$

Then, $p = F_1q_1H_1 + F_2q_2H_2 + F_3q_3H_3 + F_4q_4H_4 + F_5q_5H_5$

$= 5xxxxxxyyyyyy - 37xxxxyxyyyyyy + 114xxxyxxyyyyyy + 50xxxxxxyxyyy - 95xxxxxxyyyyy - 133xxxxxyyyyyy - 162xxxxyxyxyyy - 79xxxxyxyyyyy - 150xxxxyyyyyyy+15xxxyxxyxyyy+75xxxyxxyyyyy+73xxxyxyyyyyy+19xxxxxxxyyy-15xxxxxxyyyy + 99xxxxxyxyyy + 78xxxxxyyyyy - 141xxxxyxxyyy - 21xxxxyxyyyy - 120xxxxyyxyyy+160xxxxyyyyyy+105xxxyxxxyyy-114xxxyxxyyyy+47xxxyxyxyyy-122xxxyxyyyyy - 112xxxyyyyyyy + 35xxxxxxyyy - 73xxxxxyyyy + 143xxxxyxyyy - 84xxxxyyyyy + 143xxxyxxyyy - 68xxxyxyyyy + 62xxxyyxyyy + 133xxxyyyyyy + 26xyxyyyyyy-8yxxyyyyyy+87xxxxxxyx-80xxxxxxyy-35xxxxxyyy+165xxxxyxyx+133xxxxyxyy-121xxxxyyyy-32xxxyxxyx+61xxxyxxyy+146xxxyxyyy-138xxxyyyyy+57xxyyyyyy - 65xyxyxyyy - 88xyxyyyyy + 7xyyyyyyy + 52yxxyxyyy - 97yxxyyyyy + 30yxyyyyyy - 53xxxxxxx + 42xxxxxxy + 8xxxxxyx - 159xxxxxyy + 162xxxxyxx + 160xxxxyxy + 159xxxxyyx - 15xxxxyyy + 107xxxyxxx - 75xxxyxxy + 47xxxyxyx - 161xxxyxyy + 155xxxyyyy + 143xxyxyyy - 127xxyyyyy - 124xyxxyyy + 114xyxyyyy + 148xyyxyyy - 93xyyyyyy + 33yxxxyyy + 113yxxyyyy - 29yxyxyyy - 107yxyyyyy + 87yyyyyyy-32xxxxxx+68xxxxxy-79xxxxyx+96xxxxyy+146xxxyxx-140xxxyxy+61xxxyyx+96xxxyyy+135xxyyyy+147xyxyyy+126xyyyyy+50yxxyyy+86yxyyyy+103yyxyyy+46yyyyyy+41xxxxx-15xxxxy-127xxxyx-94xxxyy-83xxyyy+4xyxyx+106xyxyy - 135xyyyy - 68yxxyx + 36yxxyy - 52yxyyy + 45yyyyy + 54xxxx + 15xxxy - 155xxyx-63xxyy+28xyxx-112xyxy+52xyyx-122xyyy-145yxxx-17yxxy+103yxyx-125yxyy+159yyyy+55xxx+89xxy+93xyx-82xyy+133yxx+117yxy-78yyx+155yyy-137xx + 93xy + 154yx + 137yy - 63x - 28y - 85.$

Reducing p by the public key, B, yields the remainder:

$$2yxyyyyxyyyyy + 149yxyyyyyyyyyy - 55xxyxxyxyxyy + 56xxyxyxxyxyy +$$
$$21xxyxyxyxyxy + 105xxyxyyyxxyxy + 36xxyxyyyxyyyy + 103xxyyyxyyyyyy +$$
$$66xxyyyyxxyxyy + 23xxyyyyxyxyxy + 131xxyyyyxyyyyy - 13xyxxyxyxyxy -$$
$$65xyxxyyyxxyxy - 158xyxxyyyxyyyy - 82xyxyxxyxyxy - 63xyxyxyxxyxy +$$
$$131xyxyxyxyxyy - 57xyxyyyxxyxyy - 59xyxyyyxyxyxy - 141xyxyyyxyyyyy -$$
$$161xyyyxyyyyyyy - 4xyyyyyxyyyyy + 33xyyyyyyyyyyy + 35yxxyxxyxyxy + 81yxxyxyxxyxy +$$
$$144yxxyxyxyxyy - 133yxxyyyxxyxyy + 152yxxyyyxyxyxy - 127yxxyyyxyyyyy +$$
$$77yxyyyyxxyxyy + 34yxyyyyxyxyxy - 102yxyyyyxyyyyy + 91yxyyyyyxxyxy + 24yxyyyyyxyxyy -$$
$$25yxyyyyyxyyyy + 152yxyyyyyyyyyy - 117yyxyyyyyyyyy + 26yyyyyyxyyyyy - 49yyyyyyyyyyyy -$$
$$54xxyxxyxxyy - 155xxyxxyxyxy - 53xxyxxyyxyy - 128xxyxyxxyxy + 147xxyxyxyxxy -$$
$$104xxyxyxyxyx + 97xxyxyxyxyy - 141xxyxyxyyxy + 73xxyxyyxxxy + 28xxyxyyxxyx +$$
$$33xxyxyyxxyy + 40xxyxyyxyxy - 132xxyxyyxyyy + 159xxyyxxyxyx + 113xxyyxxyxyy +$$
$$133xxyyxyxxyx + 140xxyyxyxxyy - 129xxyyxyxyxy - 54xxyyxyyyyy - 35xxyyyxxyxy +$$
$$161xxyyyxyxxy + 37xxyyyxyxyx + 144xxyyyxyxyy - 32xxyyyxyyxy + 129xxyyyxyyyy -$$
$$118xyxxyxxyxy - 91xyxxyxyxxy + 129xyxxyxyxyx - 75xyxxyxyxyy + 29xyxxyxyyxy -$$
$$124xyxxyyxxxy - 129xyxxyyxxyx + 30xyxxyyxxyy + 77xyxxyyxyxy + 143xyxxyyxyyy +$$
$$88xyxyxxyxxy + 81xyxyxxyxyx - 4xyxyxxyxyy - 73xyxyxxyyxy - 110xyxyxyxxxy -$$
$$126xyxyxyxxyx + 78xyxyxyxxyy - 78xyxyxyxyxy + 48xyxyxyyxyy + 45xyxyyxxyxy -$$
$$82xyxyyxyxxy - 39xyxyyxyxyx + 113xyxyyxyxyy - 105xyxyyxyyxy + 139xyxyyxyyyy +$$
$$7xyyxxyxyxy - 44xyyxyxxyxy + xyyxyxyxyy + 69xyyxyyyyxy - 117xyyxyyyyyy -$$
$$89xyyyxxyxyy + 85xyyyxyxyxy + 140xyyyxyyyyy + 149xyyyyxxyxy - 48xyyyyxyxyy +$$
$$52xyyyyxyyyy - 112xyyyyyyyyy - 86yxxyxxyxxy + 157yxxyxxyxyx - 120yxxyxxyxyy +$$
$$124yxxyxxyyxy - 95yxxyxyxxxy + 148yxxyxyxxyx + 163yxxyxyxxyy + 56yxxyxyxyxy -$$
$$114yxxyxyyxyy + 71yxxyyxyxxy + 12yxxyyxyxyx + 92yxxyyxyxyy - 10yxxyyxyyxy -$$
$$120yxxyyxyyyy + 51yxyxxyxyxy + 147yxyxyxxyxy - 124yxyxyxyxyy - 103yxyxyyxyxy +$$
$$159yxyyxxyxyy - 151yxyyxyxyxy - 120yxyyxyyyyy - 15yxyyyxxyxy - 93yxyyyxyxxy -$$
$$76yxyyyxyxyx + 90yxyyyxyxyy + 111yxyyyxyyxy + 97yxyyyxyyyy - 25yxyyyyxxxy -$$
$$97yxyyyyxxyx + 8yxyyyyxxyy + 108yxyyyyxyxy + 152yxyyyyxyyy - 19yxyyyyyxyy -$$
$$162yxyyyyyyxy + 123yxyyyyyyyy + 5yyxxyxxyxy - 124yyxxyxyxyy - 76yyxxyyxyxy +$$
$$21yyxyxxyxyy - 137yyxyyyxyxy + 110yyxyyyyxyy + 115yyxyyyyyyy - 68yyyxyyyyyy +$$
$$8yyyyxxyxyy + 111yyyyxyxyxy + 117yyyyxyyyyy - 141yyyyyxxyxy - 19yyyyyxyxyy +$$
$$6yyyyyxyyyy - 113yyyyyyyyyy + 44xxyxxyxy - 61xxyxxyxyx - 165xxyxxyxyy -$$
$$160xxyxxyyxy - 11xxyxyxxxy - 158xxyxyxxyx + 82xxyxyxxyy - 66xxyxyxyxx +$$
$$150xxyxyxyxy - 45xxyxyxyyx - 135xxyxyyxxx + 141xxyxyyyxy + 15xxyxyyyxx -$$

$$82xxyxyyxyy - 30xxyyxxxxy + 120xxyyxxyxx - 28xxyyxxyxy + 81xxyyxxyyx - 62xxyyxyxxx + 35xxyyxyxxy - 20xxyyxyxyx - 114xxyyxyxyy - 108xxyyxyyxy - 159xxyyxyyyy - 49xxyyyyxxy + 61xxyyyyxxyx + 71xxyyyyxxyy - 72xxyyyyxyxx + 125xxyyyyxyxy + 150xxyyyyxyyx + 164xxyyyyxyyy - 107xyxxyxxxy - 127xyxxyxxyx - 161xyxxyxxyy - 90xyxxyxyxx + 164xyxxyxyxy - 85xyxxyxyyx + 90xyxxyyxxx + 28xyxxyyxxy - 58xyxxyyxyx - 82xyxxyyxyy - 96xyxyxxxxy - 95xyxyxxyxx + 99xyxyxxyxy + 60xyxyxxyyx + 111xyxyxyxxx - 150xyxyxyxxy - 47xyxyxyxyx - 106xyxyxyxyy + 89xyxyxyyxy - 74xyxyyxxxy - 29xyxyyxxyx + 91xyxyyxxyy + 58xyxyyxyxx - 29xyxyyxyxy + 155xyxyyxyyx - 53xyxyyxyyy + 50xyyxxyxxy + 102xyyxxyxyx - 129xyyxxyxyy - 14xyyxxyyxy + 23xyyxyxxxy - 74xyyxyxxyx + 104xyyxyxxyy - 49xyyxyxyxy + 13xyyxyyxyy + 65xyyxyyyxy - 9xyyxyyyyx + 163xyyxyyyyy + 95xyyyxxyxy - 67xyyyxyxxy + 63xyyyxyxyx + 156xyyyxyxyy + 112xyyyxyyxy + 108xyyyxyyyy + 50xyyyyxxxy - 104xyyyyxxyx + 115xyyyyxyxy - 60xyyyyxyyy + 38xyyyyyxyy - 103xyyyyyyxy + 34xyyyyyyyy - 43yxxyxxxxy + 106yxxyxxyxx + 103yxxyxxyxy + 55yxxyxxyyx + 43yxxyxyxxx + 116yxxyxyxxy - 113yxxyxyxyx + 65yxxyxyxyy - 81yxxyxyyxy + 56yxxyyxxxy + 50yxxyyxxyx + 112yxxyyxxyy + 84yxxyyxyxx + 154yxxyyxyxy + 156yxxyyxyyx - 53yxxyyxyyy + 91yxyxxyxxy - 69yxyxxyxyx - 160yxyxxyxyy + 52yxyxxyyxy + 36yxyxyxxxy + 164yxyxyxxyx + 45yxyxyxxyy + 142yxyxyxyxy - 59yxyxyyxxy - 14yxyxyyxyx - 80yxyxyyxyy + 9yxyyxxyxy - 64yxyyxyxxy + 109yxyyxyxyx - 102yxyyxyxyy + 23yxyyxyyxy - 118yxyyxyyyy + 66yxyyyxxxy + 114yxyyyxxyx + 19yxyyyxxyy + 130yxyyyxyxx-116yxyyyxyxy+5yxyyyxyyx-82yxyyyxyyy-yxyyyyxxx+92yxyyyyxxy+ 23yxyyyyxyx + 114yxyyyyxyy + 64yxyyyyyxy - 93yxyyyyyyx + 56yxyyyyyyy + 35yyxxyxxxy - 160yyxxyxxyx - 42yyxxyxxyy - 71yyxxyxyxy + 130yyxxyyxxy + 115yyxxyyxyx + 148yyxxyyxyy - 8yyxyxxyxy - 12yyxyxyxyx + 4yyxyxyxyy + 14yyxyyxxyx - 80yyxyyxxyy + 115yyxyyxyxy - 45yyxyyxyyy + 34yyxyyyxxy + 81yyxyyyxyx + 101yyxyyyxyy - 58yyxyyyyxy + 31yyxyyyyyy - 154yyyxxyxyx + 29yyyxxyxyy - 108yyyxyxxyx - 44yyyxyxxyy + 71yyyxyxyxy + 148yyyxyyyyy - 109yyyyxxyxy + 115yyyyxyxxy + 5yyyyxyxyx - 50yyyyxyxyy + 119yyyyxyyxy + 31yyyyxyyyy + 6yyyyyxxxy + 63yyyyyxxyx + 104yyyyyxxyy - 46yyyyyxyxy - 10yyyyyxyyy - 141yyyyyyxyy - 120yyyyyyyxy + 43yyyyyyyyy + 149xxxxxxxy - 53xxyxxxxy-116xxyxxyxx-8xxyxxyxy-102xxyxxyyx+134xxyxyxxx+140xxyxyxxy- 153xxyxyxyx-64xxyxyxyy+122xxyxyyxx+123xxyxyyxy+121xxyyxxxx-52xxyyxxxy+ 131xxyyxxyx+163xxyyxxyy-151xxyyxyxx+81xxyyxyxy-119xxyyxyyx-30xxyyxyyy-$$

$$57xxyyyxxx+137xxyyyyxxy+21xxyyyyxyx+159xxyyyyxyy-96xyxxxxxy-159xyxxyxxx-$$
$$137xyxxyxxy-132xyxxyxyx+65xyxxyxyy-88xyxxyyxx+78xyxxyyxy-10xyxyxxxx-$$
$$3xyxyxxxy-128xyxyxxyx+61xyxyxxyy-47xyxyxyxx-53xyxyxyxy+81xyxyxyyx+$$
$$31xyxyyxxx+87xyxyyxxy-23xyxyyxyx-58xyxyyxyy-85xyyxxxxy-12xyyxxyxx+$$
$$139xyyxxyxy-62xyyxxyyx+144xyyxyxxx-43xyyxyxxy-125xyyxyxyx-68xyyxyxyy-$$
$$5xyyxyyxy-15xyyxyyyx-132xyyxyyyy+62xyyyxxxy-41xyyyxxyx-xyyyxxyy+$$
$$110xyyyxyxx-31xyyyxyxy+157xyyyxyyx-122xyyyxyyy-66xyyyyxxx+16xyyyyxxy-$$
$$145xyyyyxyx-160xyyyyxyy-101xyyyyyxy+69xyyyyyyx+31xyyyyyyy+30yxxyxxxx-$$
$$102yxxyxxxy+84yxxyxxyx+37yxxyxxyy-56yxxyxyxx-50yxxyxyxy+13yxxyxyyx+$$
$$139yxxyyxxx-104yxxyyxxy+24yxxyyxyx-133yxxyyxyy-37yxyxxxxy-35yxyxxxyx+$$
$$114yxyxxxyy-77yxyxxyyx+155yxyxyxxx-80yxyxyxxy+10yxyxyxyx-32yxyxyxyy-$$
$$98yxyxyyxx+145yxyxyyxy-145yxyyxxxy+13yxyyxxyx-84yxyyxxyy+101yxyyxyxx+$$
$$151yxyyxyxy+93yxyyxyyx-140yxyyxyyy-60yxyyyxxx-87yxyyyxxy+91yxyyyxyx+$$
$$38yxyyyxyy-59yxyyyyxx-6yxyyyyxy-141yxyyyyyx-152yxyyyyyy-127yyxxyxxx-$$
$$50yyxxyxxy-152yyxxyxyx-163yyxxyxyy+143yyxxyyxx-60yyxxyyxy+162yyxyxxxy+$$
$$123yyxyxxyx-129yyxyxxyy-84yyxyxyxx-111yyxyxyxy-156yyxyxyyx+98yyxyyxxx+$$
$$132yyxyyxxy+85yyxyyxyx+59yyxyyxyy-95yyxyyyxx-49yyxyyyxy+30yyxyyyyx+$$
$$88yyxyyyyy+104yyyyxxxy-85yyyyxxyx-164yyyyxxyy-16yyyyxyyx-94yyyyxyxx+$$
$$136yyyyxyxy+138yyyyxyyx-155yyyyxyyy-70yyyyyyxy-111yyyyyyyy+136yyyyyxxy-$$
$$82yyyyyxyx+93yyyyyxyy+35yyyyyyxx-108yyyyyyxy+65yyyyyyyx-103yyyyyyyy+$$
$$110yyyyyyxx-17yyyyyyxy+28yyyyyyyx-19yyyyyyyy+38yyyyyyyy+115yyyyyyyyx-$$
$$105yyyyyyyy+50xxxxxxx-132xxxxxxy+107xxyxxxx+84xxyxxxy-160xxyxxyx-$$
$$127xxyxxyy-37xxyxyxx-34xxyxyxy+136xxyxyyx+58xxyyxxx+47xxyyxxy+$$
$$67xxyyxyx+42xxyyxyy+95xxyyyxx-23xxyyyxy-10xyxxxxx+25xyxxxxy-70xyxxyxx-$$
$$165xyxxyxy-125xyxxyyx+24xyxyxxx+109xyxyxxy+125xyxyxyx+120xyxyxyy+$$
$$79xyxyyxx+11xyxyyxy-99xyyxxxx+32xyyxxxy-82xyyxxyx+81xyyxxyy+106xyyxyxx-$$
$$10xyyxyxy+62xyyxyyx+162xyyxyyy+51xyyyxxx-145xyyyxxy+55xyyyxyx+$$
$$134xyyyxyy+49xyyyyxx+4xyyyyxy-109xyyyyyx-71xyyyyyy-162yxxxxxy-$$
$$122yxxyxxx-80yxxyxxy-158yxxyxyx-26yxxyxyy+67yxxyyxx+45yxxyyxy+$$
$$23yxyxxxx-79yxyxxxy-111yxyxxyx+136yxyxxyy+77yxyxyxx-37yxyxyxy-$$
$$140yxyxyyx-119yxyyxxx+8yxyyxxy-93yxyyxyx+101yxyyxyy-129yxyyyxx+$$
$$71yxyyyxy-136yxyyyyx-79yxyyyyy+116yyxxxxy+28yyxxyxx-125yyxxyxy-$$
$$154yyxxyyx-9yyxyxxx-82yyxyxxy-127yyxyxyx+124yyxyxyy+8yyxyyxx+$$
$$129yyxyyxy+154yyxyyyx-122yyxyyyy+66yyyxxxx-69yyyxxxy+15yyyxxyx-$$

$158yyyxxyy - 33yyyxyxx - 72yyyxyxy - 145yyyxyyx - 103yyyxyyy - 143yyyyxxx + 119yyyyxxy - 77yyyyxyx - 87yyyyxyy - 16yyyyyxx + 23yyyyyxy + 140yyyyyyx + 156yyyyyyy + 65xxxxxx + 93xxxxxy + 24xxyxxx - 127xxyxxy - 17xxyxyx + 89xxyxyy + 115xxyyxx + 66xxyyxy - 160xxyyyx + 24xyxxxx - 55xyxxxy + xyxxyx - 7xyxxyy + 122xyxyxx - 119xyxyxy - 102xyxyyx - 127xyyxxx - 8xyyxxy - 90xyyxyx + 137xyyxyy - 77xyyyxx - 104xyyyxy + 92xyyyyx - 51xyyyyy - 132yxxxxx - 87yxxxxy - 33yxxyxx - 87yxxyxy + 44yxxyyx + 132yxyxxx - 10yxyxxy - 3yxyxyx - 40yxyxyy + 151yxyyxx - 66yxyyxy + 71yxyyyx + 46yxyyyy + 136yyxxxx + 156yyxxxy + 151yyxxyx + 25yyxxyy + 28yyxyxx - 22yyxyxy + 165yyxyyx - 86yyxyyy - 41yyyxxx - 8yyyxxy + 33yyyxyx - 66yyyyxx - 66yyyyxy - 47yyyyyx - 30yyyyyy + 154xxxxx + 68xxxxy - 132xxyxx + 41xxyxy + 42xxyyx - 116xxyyy + 143xyxxx - 145xyxxy - 82xyxyx - 10xyxyy - 144xyyxx + 29xyyxy - 106xyyyx - 18xyyyy - 35yxxxx + 60yxxxy + 97yxxyx + 105yxxyy + 163yxyxx + 10yxyxy - 84yxyyx + 84yxyyy - 152yyxxx + 98yyxxy + 136yyxyx + 24yyxyy - 44yyyxx + 122yyyxy + 73yyyyx - 6yyyyy + 31xxxx + 23xxxy - 123xxyx - 119xxyy + 76xyxx - 139xyxy - 100xyyx + 25xyyy - 99yxxx + 101yxxy + 88yxyx + 90yxyy + 80yyxx - 158yyxy + 67yyyx - 90yyyy + 118xxx + 131xxy + 130xyx + 52xyy - 74yxx - 111yxy - 150yyx - 122yyy - 38xx - 11xy - 95yx + 44yy - 14x - 139y - 160$

So a message, m, that is encrypted as $c = p + m$ cannot be found by reducing c with respect to the public key.

Reducing p by the partial Gröbner basis of $\langle B \rangle$ that was displayed in example 3.5.1 yields the remainder:

$33xxyyyxyxxyxy + 79xyxyxyyyxyxy + 84xyyyxxyyyxyxy + 93xyyyxyxyxxyx - 146xyyyxyxyxxyy + 139xyyyxyxyyyxx - 115xyyyxyxyyyxy + 134xyyyxyyyxyxy + 56xyyyxyyyyxyy + 64xyyyyxxyyyxx - 72xyyyyxxyyxyy + 37xyyyyxyxxyxy + 103xyyyyxyyxxyx + 91xyyyyxyyxxyy - 121xyyyyxyyxyyy - 24xyyyyxyyyxyx + 27xyyyyxyyyxyy + 17xyyyyxyyyyxy - 76xyyyyyxxyxyy - 43xyyyyyxyxxyx + 7xyyyyyxyxxyy + 17xyyyyyxyyyyy - 125xyyyyyyyyyy - 17yxxyxyyyxyyy - 106yxyxxyyyxyxy + 116yxyxxyyyxyyy - 48yxyxyxxyxxy + 82yxyxyxxyyyxy - 147yxyxyyyxyxxy + 86yxyxyyyxyxyx + 37yxyxyyyxyxyy - 111yxyxyyyxyyxy - 163yxyyyxxyxxyy - 122yxyyyxxyyyxx - 149yxyyyxxyyxyy - 157yxyyyxyxxyxy + 145yxyyyxyyxxyx - 39yxyyyxyyxxyy - 90yxyyyxyyxyyy - 37yxyyyxyyyxyx - 151yxyyyxyyyxyy + 56yxyyyyxxyxyy + 113yxyyyyxyxxyx - 3yxyyyyxyxxyy - 28yxyyyyxyyyyy + 140yxyyyyyxxyxy - 87yxyyyyyxyxyy - 101yxyyyyyxyyyy - 85yyyxxyxxyyxy + 56yyyxxyxyyxyy + 49yyyxxyyxyxxy - 139yyyxxyyyxyxx + 98yyyxxyyyxyyy + 37yyyxxyyyyyxy - 95yyyxyxxyxxyy -$

$$138yyxyxxyxyxx - 52yyxyxxyyxyx + 30yyxyxxyyxyy + 20yyxyxyxxyxx + 95yyxyxyxxyyx - 128yyxyxyyxxyx + 80yyxyxyyxxyy - 3yyxyxyyxyxx - 136yyxyxyyxyxy - 35yyxyxyyxyyx + 53yyxyyxxyxxy - 101yyxyyxxyyxy + 18yyxyyxyxxyx - 103yyxyyxyxxyy + 47yyxyyxyyyxy - 114yyxyyyyxxyx + 23yyxyyyyxyxy - 72yyxyyyyxyyx + 46yyxyyyyxyyy - 138yyxyyyyyyxy + 38yyxyyyyxyyy + 91yyxyyyyyxyx - 130yyxyyyyyxyy + 99yyxyyyyyxyy - 39yyxyyyyyyyy + 28yyxyyyyyyyx + 159yyxyyyyyyyy - 13yyyyxxyxxyyx + 128yyyyxxyxyyxy + 24yyyyxxyyxxyy + yyyyxxyyxyxx - 65yyyyxxyyxyxy + 122yyyyxxyyxyyx + 146yyyyxxyyxyyy + 55yyyyxyxxyxxy + 53yyyyxyxxyxyx + 145yyyyxyxxyyxy + 86yyyyxyxyxxyx - 14yyyyxyxyxxyy - 26yyyyxyxyyxyx + 112yyyyxyxyyxyy - 107yyyyxyyxxyxx + 79yyyyxyyxxyyx + 55yyyyxyyxyyyx + 116yyyyxyyyxxyx + 143yyyyxyyyxxyy + 41yyyyxyyyxyxx - 17yyyyxyyyxyxy + 37yyyyxyyyxyyx + 95yyyyxyyyxyyy + 115yyyyxyyyyyxx + 66yyyyxyyyyxyy + 163yyyyxyyyyyxy - 146yyyyyxxyxyyx + 119yyyyyxxyyyxx + 73yyyyyxxyyxyy - 161yyyyyxyxxyxx + 62yyyyyxyxxyxy + 57yyyyyxyxxyyx - 155yyyyyxyyxxyx + 133yyyyyxyyxxyy - 75yyyyyxyyxyyy - 86yyyyyxyyyxyx + 14yyyyyxyyyxyy + 109yyyyyxyyyyxy - 98yyyyyxyyyyyx - 162yyyyyyxxyxyy + 39yyyyyyxyxxyx + 163yyyyyyxyxxyy - 77yyyyyyxyyyyy + 133xxyxxyyyxyx + 73xxyxxyyxyyy + 157xxyxyyxxyx + 156xxyxyyxxyy + 10xxyxyyxyyy + 37xxyyyxxyyxy - 100xxyyyxyxxxy - 158xxyyyxyxxyx + 35xxyyyxyxxyy + 143xxyyyxyyyxy - 129xyxxxyxyyxy + 79xyxxxyyxxyy + 76xyxxxyyxyxy + 42xyxxxyyxyyy + 72xyxyxxxyxxy + 72xyxyxxxyxyx + 37xyxyxxyyxy + 152xyxyxyxxyx + 128xyxyxyxxyy - 109xyxyxyyyxxy + 91xyxyxyyyxyx - 110xyxyxyyyxyy - 115xyxyyyxyxxy + 29xyxyyyxyxyx - 114xyxyyyxyxyy + 28xyxyyyxyyxy + 151xyyyxxxxxxy - 79xyyyxxyxxyy + 87xyyyxxyxyxx - 151xyyyxxyxyyx - 74xyyyxxyyxxy - 35xyyyxxyyxyx + 32xyyyxxyyxyy - 23xyyyxyxxxxy - 80xyyyxyxxyxx + 98xyyyxyxxyxy - 24xyyyxyxxyyx - 11xyyyxyxyxxx + 103xyyyxyxyxxy - 20xyyyxyxyyxx - 160xyyyxyxyyxy + 141xyyyxyyxxyx + 26xyyyxyyxxyy - 40xyyyxyyxyxy + 156xyyyxyyxyyy - 55xyyyxyyyxxy + 63xyyyxyyyxyx - 143xyyyxyyyxyy + 7xyyyxyyyyxy - 106xyyyyxxxxxy - 161xyyyyxxyxxy + 107xyyyyxxyxyx - 6xyyyyxxyxyy + 117xyyyyxxyyxx + 32xyyyyxxyyxy + 74xyyyyxyxxxy + 94xyyyyxyxxyx + 148xyyyyxyxxyy + 130xyyyyxyxyxx - 30xyyyyxyxyyx + 59xyyyyxyyxxx + 47xyyyyxyyxxy + 114xyyyyxyyxyx - 9xyyyyxyyxyy + 163xyyyyxyyyxx + 147xyyyyxyyyxy + 125xyyyyxyyyyx + 29xyyyyxyyyyy + 164xyyyyyxxxxy + 8xyyyyyxxyxx - 13xyyyyyxxyxy + 11xyyyyyxxyyx + 30xyyyyyxyxxx + 80xyyyyyxyxxy - 12xyyyyyxyxyx - 149xyyyyyxyxyy - 36xyyyyyxyyyx - 100xyyyyyxyyyy + 49xyyyyyyxxyx - 77xyyyyyyxxyy + 87xyyyyyxyxy - 62xyyyyyxyyy + 19xyyyyyyyxyx + 86xyyyyyyyxyy + 60xyyyyyyyyxy - 105xyyyyyyyyyy - 149yxxyxxyyxy - 141yxxyxyxxxy + 142yxxyxyyxxy + 45yxxyxyyxyy -$$

$$103yxxyyyxyxyy + 84yxyxxxxxxy + 84yxyxxxyxxxy - 50yxyxxxyxxyy - 16yxyxxxyxyxx -$$
$$121yxyxxyyyxxy - 139yxyxxyyyxyx - 35yxyxxyyyxyy + 3yxyxyxxxxy - 82yxyxyxxyxx -$$
$$94yxyxyxxyyyx - 36yxyxyyyxxxy + 52yxyxyyyxxyx + 155yxyxyyyxxyy - 57yxyxyyyxyxx -$$
$$100yxyxyyyxyxy - 161yxyxyyyxyyx + 140yxyyyxxxxxy + 110yxyyyxxyxxy + 139yxyyyxxyyxx +$$
$$101yxyyyxxyyxy - 74yxyyyxyxxxy + 46yxyyyxyxxyx - 30yxyyyxyxxyy - 103yxyyyxyxyxx -$$
$$129yxyyyxyxyyx + 22yxyyyxyyxxx - 162yxyyyxyyxxy - 31yxyyyxyyxyx - 99yxyyyxyyxyy +$$
$$72yxyyyxyyyxx - 62yxyyyxyyyxy - 23yxyyyyxxxxy - 98yxyyyyxxyxx - 20yxyyyyxxyxy -$$
$$52yxyyyyxxyyx + 129yxyyyyxyxxx - 71yxyyyyxyxxy + 132yxyyyyxyxyx + 113yxyyyyxyxyy -$$
$$158yxyyyyxyyxy + 110yxyyyyxyyyx - 6yxyyyyxyyyy - 13yxyyyyyxxxy - 45yxyyyyyxxyx -$$
$$105yxyyyyyxxyy - 140yxyyyyyxyxy - 148yxyyyyyxyyy - 90yxyyyyyyxyx + 135yxyyyyyyxyy -$$
$$57yyxxxxxxxxy - 96yyxxxyxxxxy - 20yyxxxyxxyyx - 100yyxxxyxyxxx - 127yyxxxyxyyxx +$$
$$123yyxxxyxyyxy + 12yyxxxyyxxxy + 25yyxxxyyxxyy + 61yyxxxyyxyxx - 165yyxxxyyxyxy -$$
$$8yyxxxyyxyyx - 162yyxxxyyxyyy - 48yyxyxxxxxxy + 157yyxyxxxyxxx + 132yyxyxxxyxxy -$$
$$159yyxyxxxyxyx - 133yyxyxxxyyxx + 8yyxyxxxyyxy + 140yyxyxyxxxxx + 142yyxyxyxxxxy -$$
$$64yyxyxyxxxyx - 39yyxyxyxxyyy + 76yyxyxyyyxxx - 140yyxyxyyyxxy - 19yyxyxyyyxyx +$$
$$53yyxyxyyyxyy + 133yyxyyyxxxxy - 159yyxyyyxxyxx + 66yyxyyyxxyyx + 126yyxyyyxyxxx +$$
$$144yyxyyyxyxxy + 24yyxyyyxyxyx + 87yyxyyyxyxyy + 81yyxyyyxyyxy - 134yyxyyyxyyyx +$$
$$25yyxyyyyxxxy - 127yyxyyyyxxyx - 143yyxyyyyxxyy + 135yyxyyyyxyxx + 66yyxyyyyxyxy -$$
$$17yyxyyyyxyyx + 139yyxyyyyxyyy - 25yyxyyyyyxxx + 122yyxyyyyyxxy + 113yyxyyyyyxyx +$$
$$121yyxyyyyyxyy - 135yyxyyyyyyxx - 31yyxyyyyyyxy + 17yyyyxxxxxxy + 25yyyyxxyxxxy -$$
$$162yyyyxxyxxyy + 91yyyyxxyxyxx + 21yyyyxxyxyyx + 7yyyyxxyyxxx + 108yyyyxxyyxxy +$$
$$119yyyyxxyyxyx - 48yyyyxxyyxyy - 106yyyyxyxxxxy - 156yyyyxyxxyxx - 2yyyyxyxxyxy -$$
$$52yyyyxyxxyyx - 89yyyyxyxyxxx - 134yyyyxyxyxxy - 48yyyyxyxyyxx - 132yyyyxyxyyxy -$$
$$87yyyyxyyxxxx - 114yyyyxyyxxyx - 11yyyyxyyxxyy - 112yyyyxyyxyxx + 94yyyyxyyxyxy +$$
$$6yyyyxyyxyyx - 59yyyyxyyxyyy + 106yyyyxyyyxxx - 91yyyyxyyyxxy - 93yyyyxyyyxyx -$$
$$60yyyyxyyyxyy + 122yyyyxyyyyxx - 48yyyyxyyyyxy + 22yyyyxyyyyyx - 104yyyyyxxxxxy -$$
$$124yyyyyxxyxxx + 119yyyyyxxyxxy + 116yyyyyxxyxyx + 3yyyyyxxyxyy - 165yyyyyxxyyxx -$$
$$150yyyyyxxyyxy - 134yyyyyxyxxxx - 91yyyyyxyxxxy - 156yyyyyxyxxyx + 68yyyyyxyxxyy +$$
$$45yyyyyxyxyxx - 66yyyyyxyxyyx - 92yyyyyxyyxxx - 135yyyyyxyyxxy - 88yyyyyxyyxyx -$$
$$115yyyyyxyyxyy - 44yyyyyxyyyxx + 90yyyyyxyyyxy - 147yyyyyxyyyyx - 124yyyyyxyyyyy +$$
$$36yyyyyyxxxxy - 124yyyyyyxxyxx + 6yyyyyyxxyxy + 102yyyyyyxxyyx - 58yyyyyyxyxxx +$$
$$34yyyyyyxyxxy + 14yyyyyyxyxyx - 63yyyyyyxyxyy - 139yyyyyyxyyxy - 161yyyyyyxyyyx -$$
$$111yyyyyyxyyyy - 140yyyyyyyxxyx + 31yyyyyyyxxyy - 129yyyyyyyxyxx + 73yyyyyyyxyxy +$$
$$150yyyyyyyxyyx - 101yyyyyyyxyyy + 79yyyyyyyyxyx + 128yyyyyyyyxyy - 105yyyyyyyyyxy +$$

$$50yyyyyyyyyx + 22yyyyyyyyyy + 19xxxxxxxxy - 163xxyxxxxxy - 62xxyxxyyxx + 134xxyxxyyxy - 135xxyxyxxxy + 106xxyxyyxxx + 80xxyxyyxxy + 71xxyxyyxyy + 61xxyyxxxxy - 15xxyyxxyyx - 113xxyyxyxxx + 36xxyyxyxxy - 88xxyyxyxyx + 124xxyyxyxyy - 109xxyyxyyxy - 6xxyyxyyyx - 123xxyyyyxxy - 80xyxxxxxxy + 103xyxxxyxxy + 23xyxxxyxyy - 163xyxxxyxyx + 51xyxxxyyyx - 124xyxxyyyxy - 139xyxxyyyxx + 125xyxxyyyyy + 106xyxyxxxxy + 108xyxyxxxyx + 13xyxyxxyxy - 26xyxyxxyyx + 71xyxyxyxxx - 57xyxyxyxxy - 25xyxyxyyxx - 68xyxyxyyxy + 43xyxyyxxxy + 30xyxyyxxyx - 58xyxyyxxyy + 73xyxyyxyxx + 130xyxyyxyxy - 15xyxyyxyyx - 33xyxyyxyyy + 64xyyxxxxxx - 40xyyxxxxxy - 53xyyxxyxxx + 60xyyxxyxxy - 81xyyxxyxyx - 28xyyxxyxyy - 107xyyxxyyxx - 92xyyxxyyxy - 59xyyxyxxxx - 102xyyxyxxxy - 132xyyxyxxyx - 120xyyxyxxyy - 113xyyxyxyxx - 28xyyxyxyyx - 6xyyxyyxxx - 165xyyxyyxxy - 95xyyxyyxyx - 56xyyxyyxyy + 110xyyxyyyxx + 155xyyxyyyxy + 76xyyxyyyyx - 17xyyxyyyyy - 80xyyyxxxxx + 88xyyyxxxxy + 63xyyyxxyxx - 129xyyyxxyxy + 135xyyyxxyyx - 58xyyyxyxxx + 53xyyyxyxxy + 21xyyyxyxyx - 73xyyyxyxyy + 48xyyyxyyxx - 70xyyyxyyxy - 85xyyyxyyyx + 145xyyyxyyyy - 120xyyyyxxxx + 58xyyyyxxxy + xyyyyxxyx + 17xyyyyxxyy - 25xyyyyxyxx - 108xyyyyxyxy - 154xyyyyxyyx - 137xyyyyxyyy + 12xyyyyyxxx + 71xyyyyyxxy - 122xyyyyyxyx - 16xyyyyyxyy + 133xyyyyyyxx + 33xyyyyyyxy - 163xyyyyyyyx - 61xyyyyyyyy + 16yxxxxxxxy - 119yxxyxxxxy - 21yxxyxxyyx + 114yxxyxyxxx + 19yxxyxyyxx + 101yxxyxyyxy + 91yxxyyxxxy + 26yxxyyxxyy - 60yxxyyxyxx - 78yxxyyxyxy - 38yxxyyxyyx + 141yxxyyxyyy - 74yxyxxxxxx - 12yxyxxxxxy + 137yxyxxyxxx + 121yxyxxyxxy - 149yxyxxyxyx - 14yxyxxyyxx - 147yxyxxyyxy + 144yxyxyxxxx - 69yxyxyxxxy - 162yxyxyxxyx + 155yxyxyxxyy + 54yxyxyyxxx - 44yxyxyyxxy + 98yxyxyyxyx + 111yxyxyyxyy - 13yxyyxxxxx + 97yxyyxxxxy - 73yxyyxxyxx - 89yxyyxxyyx + 156yxyyxyxxx + 70yxyyxyxxy + 151yxyyxyxyx + 46yxyyxyxyy - 132yxyyxyyxx - 130yxyyxyyxy + 7yxyyxyyyx + 146yxyyyxxxx + 159yxyyyxxxy + 128yxyyyxxyx + 37yxyyyxxyy + 68yxyyyxyxx + 44yxyyyxyxy + 52yxyyyxyyx + 66yxyyyxyyy + 16yxyyyyxxx + 118yxyyyyxxy + 48yxyyyyxyx - 25yxyyyyxyy + 32yxyyyyyxx - 41yxyyyyyxy - 68yyxxxxxxx + 149yyxxxxxxy - 48yyxxyxxxx + 14yyxxyxxxy + 73yyxxyxxyy - 125yyxxyxyxx - 99yyxxyxyyx - 20yyxxyyxxx - 126yyxxyyxxy + 157yyxxyyxyx - 88yyxyxxxxx + 101yyxyxxxxy - 8yyxyxxyxx + 3yyxyxxyxy + 114yyxyxxyyx - 135yyxyxyxxx - 133yyxyxyxxy - 131yyxyxyyxx - 14yyxyxyyxy - 131yyxyyxxxx + 28yyxyyxxxy + 165yyxyyxxyx + 24yyxyyxxyy + 28yyxyyxyxx + 109yyxyyxyxy -$$

$$63yyxyyxyyx - 143yyxyyxyyy - 57yyxyyyxxx - 103yyxyyyxxy + 72yyxyyyxyx - 151yyxyyyxyy + 65yyxyyyyxx + 29yyxyyyyxy - 83yyxyyyyyx + 119yyyxxxxxx + 8yyyxxxxxy - 52yyyxxyxxx + 66yyyxxyxxy + 80yyyxxyxyx - 19yyyxxyxyy + 141yyyxxyyxx + 4yyyxxyyxy - 47yyyxyxxxx + 108yyyxyxxxy - 79yyyxyxxyx - 69yyyxyxxyy + 65yyyxyxyxx - 66yyyxyxyyx + 82yyyxyyxxx - 135yyyxyyxxy - 143yyyxyyxyx + 5yyyxyyxyy - 52yyyxyyyxx + 77yyyxyyyxy + 159yyyxyyyyx + 21yyyxyyyyy + 59yyyyxxxxx + 93yyyyxxxxy + 79yyyyxxyxx + 94yyyyxxyxy - 84yyyyxxyyx - 162yyyyxyxxx + 127yyyyxyxxy - 104yyyyxyxyx + 154yyyyxyxyy - 89yyyyxyyxx - 39yyyyxyyxy - yyyyxyyyx - 85yyyyxyyyy + 46yyyyyxxxx - 117yyyyyxxxy - 44yyyyyxxyx + 47yyyyyxxyy + 50yyyyyxyxx - 38yyyyyxyxy + 49yyyyyxyyx + 37yyyyyxyyy + 103yyyyyyxxx + 75yyyyyyxxy - 35yyyyyyxyx + 150yyyyyyxyy - 79yyyyyyyxx + 123yyyyyyyxy + 123yyyyyyyyx - 5yyyyyyyyy + 133xxxxxxxx-71xxxxxxxy-148xxyxxxxx-32xxyxxxxy-97xxyxxyxx+108xxyxxyyx-103xxyxyxxx-106xxyxyyxx-92xxyxyyxy+96xxyyxxxx+60xxyyxxxy+139xxyyxxyy+83xxyyxyxx-101xxyyxyxy+47xxyyxyyx-72xxyyxyyy+132xxyyyxxx+106xxyyyxxy-102xxyyyxyy+102xyxxxxxx-17xyxxxxxy-61xyxxxyxx-163xyxxxyxy+22xyxxxyyx+147xyxxxyyy+53xyxxyyxx+37xyxxyyxy+69xyxyxxxx+52xyxyxxxy-90xyxyxxyx-92xyxyxxyy-15xyxyxyxx+85xyxyxyyx-60xyxyyxxx-75xyxyyxxy+161xyxyyyxx+48xyxyyyxy-113xyyxxxxx+77xyyxxxxy-95xyyxxyxx-145xyyxxyxy-100xyyxxyyx+133xyyxyxxx+130xyyxyxxy-16xyyxyxyx+107xyyxyxyy-60xyyxyyxx+14xyyxyyxy-106xyyxyyyx-161xyyxyyyy-64xyyyxxxx-103xyyyxxxy-162xyyyxxyx-67xyyyxxyy-97xyyyxyxx + 8xyyyxyxy - 67xyyyxyyx - 124xyyyxyyy + 42xyyyyxxx + 53xyyyyxxy - 151xyyyyxyx-27xyyyyxyy+67xyyyyyxx-128xyyyyyxy-149xyyyyyyx+35xyyyyyyy+112yxxxxxxx-67yxxxxxxy-77yxxxyxxx+119yxxxyxxy-84yxxxyxyy-77yxxyxyxx+86yxxyxyyx-34yxxyyxxx-117yxxyyxxy-93yxxyyxyx-114yxxyyxyy+91yxyxxxxx+144yxyxxxxy-10yxyxxyxx-33yxyxxyxy+88yxyxxyyx+89yxyxyxxx+35yxyxyxxy-152yxyxyyxx+110yxyxyyxy+158yxyyxxxx-96yxyyxxxy-105yxyyxxyx+82yxyyxxyy-27yxyyyxxx-37yxyyyxxy-78yxyyyxyx-128yxyyyxyy+159yxyyyyxx-136yxyyyyxy-72yxyyyyxx-156yxyyyyxy+157yxyyyyyx-110yxyyyyyy-156yxyyyyyx-24yyxxxxxx-38yyxxxxxy-148yyxxyxxx+60yyxxyxxy-110yyxxyxyx-130yyxxyxyy-162yyxxyyxx+44yyxxyyxy - 30yyxyxxxx + 137yyxyxxxy - yyxyxxyx + 52yyxyxxyy - yyxyxyxx - 157yyxyxyyx + 84yyxyyxxx + 7yyxyyxxy - 37yyxyyyxx + 11yyxyyyxy + 9yyxyyyyx + 149yyxyyyxy-76yyxyyyyx-56yyxyyyyy+105yyyxxxxx+111yyyxxxxy-140yyyxxyxx+123yyyxxyxy-52yyyxxyyx+22yyyxyxxx-155yyyxyxxy+12yyyxyxyx+42yyyxyxyy+$$

$$12yyyxyyyx + 148yyyxyyxy + 39yyyxyyyx + 136yyyxyyyy - 64yyyyxxxx - 92yyyyxxxy - 50yyyyxxyx + 28yyyyxxyy + 152yyyyxyxx - 128yyyyxyxy - 165yyyyxyyx - 142yyyyxyyy + 159yyyyyxxx + 26yyyyyxxy - 77yyyyyxyx - 85yyyyyxyy + 88yyyyyyxx - 17yyyyyyxy + 109yyyyyyyx + 91yyyyyyyy - 31xxxxxxx - 55xxxxxxy + 157xxyxxxx + 30xxyxxxy + 82xxyxxyx - 81xxyxxyy - 28xxyxyxx - xxyxyyx - 82xxyyxxx + 97xxyyxxy + 67xxyyxyx + 132xxyyxyy + 143xxyyyxx - 15xxyyyxy - 143xyxxxxx - 35xyxxxxy - 56xyxxyxx + 39xyxxyxy - 116xyxxyyx - 111xyxyxxx - 93xyxyxxy + 139xyxyxyx + 98xyxyxyy - 93xyxyyxx - 11xyxyyxy + 86xyyxxxx - 76xyyxxxy - 78xyyxxyx + 68xyyxxyy + 4xyyxyxx - 78xyyxyxy - 46xyyxyyx - 70xyyxyyy + 131xyyyxxx + 147xyyyxxy + 130xyyyxyx + 92xyyyxyy - 71xyyyyxx - 102xyyyyxy + 36xyyyyyx + 8xyyyyyy - 94yxxxxxx + 32yxxxxxy - 116yxxyxxx - 60yxxyxxy - 47yxxyxyx + 30yxxyxyy - 5yxxyyxx - 18yxxyyxy - 118yxyxxxx - 80yxyxxxy - 132yxyxxyx + 102yxyxxyy + 160yxyxyxx - 111yxyxyyx - 117yxyyxxx + 109yxyyxxy - 80yxyyxyx + 35yxyyxyy + 160yxyyyxx - 164yxyyyxy - 148yxyyyyx - 47yxyyyyy + 159yyxxxxx + 53yyxxxxy - 121yyxxyxx - 14yyxxyxy + 39yyxxyyx - 78yyxyxxx + 24yyxyxxy + 56yyxyxyx - 148yyxyxyy + 72yyxyyxx + 154yyxyyxy - 111yyxyyyx - 16yyxyyyy - 53yyyxxxx - 89yyyxxxy - 162yyyxxyx - 48yyyxxyy - 152yyyxyxx - 57yyyxyxy - 87yyyxyyx - 146yyyxyyy + 8yyyyxxx + 11yyyyxxy + 19yyyyxyx + 56yyyyxyy + 164yyyyyxx - 42yyyyyxy - 157yyyyyyx + 3yyyyyyy - 101xxxxxx - 83xxxxxy - 3xxyxxx - 23xxyxxy + 17xxyxyx + 27xxyxyy + 107xxyyxx - 92xxyyxy + 85xxyyyx + 129xyxxxx - 35xyxxxy - xyxxyx + 35xyxxyy + 12xyxyxx + 51xyxyxy + 137xyxyyx + 118xyyxxx - 58xyyxxy - 55xyyxyx - 163xyyxyy + 161xyyyxx + 79xyyyxy + 93xyyyyx - 43xyyyyy - 142yxxxxx + 76yxxxxy - 28yxxyxx - 147yxxyxy - 149yxxyyx - 149yxyxxx + 61yxyxxy - 24yxyxyx - 44yxyxyy + 141yxyyxx - 30yxyyxy + 60yxyyyx - 43yxyyyy - 60yyxxxx - 65yyxxxy + 83yyxxyx - 113yyxxyy - 9yyxyxx - 47yyxyxy + 125yyxyyx + 85yyxyyy + 158yyyxxx + 150yyyxxy + 101yyyxyx - 65yyyxyy - 76yyyyxx - 83yyyyxy + 93yyyyyx - 21yyyyyy + 75xxxxx - 34xxxxy + 92xxyxx + 102xxyxy + 68xxyyx - 66xxyyy - 15xyxxx - 104xyxxy + 153xyxyx + 51xyxyy - 137xyyxx - 139xyyxy - 60xyyyx + 62xyyyy + 138yxxxx + 18yxxxy - 123yxxyx - 136yxxyy - 89yxyxx + 61yxyxy - 111yxyyx - 131yxyyy - 155yyxxx - 144yyxxy - 69yyxyx + 161yyxyy + 61yyyxx - 49yyyxy + 18yyyyx - 85yyyyy - 45xxxx + 157xxxy + 72xxyx - 12xxyy - 122xyxx + 128xyxy - 57xyyx + 105xyyy - 24yxxx - 77yxxy - 61yxyx - 120yxyy - 33yyxx - 142yyxy - 86yyyx - 69yyyy - 97xxx + 35xxy + 110xyx + 67xyy - 82yxx - 87yxy - 131yyx + 5yyy - 78xx + 74xy - 67yx + 139yy + 62x - 89y + 107$$

Bibliography

[AdLo] W. Adams and P. Loustaunau: An Introduction to Gröbner Bases. Amer. Math. Soc., Providence, 1994.

[BeWe] T. Becker and V. Weispfenning: Gröbner Basis: A Computational Approach to Commutative Algebra. Springer-Verlag, New York, 1993.

[Berg] G. Bergman: The diamond lemma for ring theory, Adv. Math. 29, 1978, pp 178 - 218.

[BoOt] R. Book and F. Otto: String-Rewriting Systems. Springer-Verlag, 1993.

[Bucb1] B. Buchberger: An algorithm for finding a basis for the residue class ring of a zero-dimensional ideal, Ph.D. Thesis, University of Innsbruck, 1965.

[Bucb2] B. Buchberger: Gröbner bases: an algorithmic method in polynomial ideal theory. In N. K.Bose, editor, Multidimensional Systems Theory, Mathematics and its Applications, pages 184-232. D. Reidel Publishing Company, Dordrecht, Holland, 1985.

[Bucm] J. Buchmann: Introduction to Cryptography. Springer, New York, 2001.

[CLOs] D. Cox, J. Little and D. O'Shea: Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra, 2nd ed. Springer, 1997

[Cram] R. Cramer: An introduction to Crypto-Systems Secure Against Active Attacks. Lecture Notes, Part II of Cryptographic Protocol Theory (CPT), Comp. Sc. Dept. Aarhus University, Spring 2001.

[Di] L. Dickson: Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. Amer. J. Math., 35, 1913, pp 413 - 426.

[DiHe] W. Diffie and M. Hellman: New Directions in Cryptography. IEEE Trans. Information Theory 22, 1976, pp 644 - 654.

[FeKo] M. Fellows and N. Koblitz: Combinatorial cryptosystems galore! Contemporary Math. 168, 1994, 51 - 61.

[EGSt] R. Endsuleit, W. Geiselmann and R. Steinwandt: Attacking a polynomial-based cryptosystem: Polly Cracker. Int. Jour. Information Security, 1, 2002, pp 143 - 148.

[GeSt] W. Geiselmann and R. Steinwandt: Cryptanalysis of Polly Cracker. IEEE Trans. Information Theory, 48, 2002, pp 2990 - 2991.

[Gi] M. Giutsi: Some effectivity problems in polynomial ideal theory, EUROSAM 84; Proc. intern. symp. on Symbolic and Algebraic Computation, Cambridge, England, Springer-Verlag, 1984, 159 - 171.

[GoMi1] S. Goldwasser and S. Micali: Probabilistic encryption and how to play mental poker keeping secret all partial information. Proc. 14th ACM Symp.Theory of Computing, 1982, pp 365 - 377.

[GoMi1] S. Goldwasser and S. Micali: Probabilistic encryption. J.Comput. System Sci. 28, 1984, pp 270 - 299.

[Gr1] E. Green: Noncommutative Gröbner bases, and projective resolutions. Computational methods for representations of groups and algebras. Papers from the First Euroconference held at the University of Essen. Basel, 1999, P. Dräxler, G. O. Michler, and C. M. Ringel, Eds., no. 173 in Progress in Math., Birkhäuser Verlag, pp. 29-60.

[Gr2] E. Green: Multiplicative bases, Gröbner bases, and right Gröbner bases. Jour. Symb. Comput., 2000.

[GHKO] E. Green, L. S. Heath and B. J. Keller: Opal: A system for computing noncommutative Gröbner bases (system description). Eighth International Conference on Rewriting Techniques and Applications (RTA-97), 1997, pp. 331- 334.

[GMTU] E. Green, T. Mora and V. Ufnarovski: The non-commutative Gröbner freaks, Progress in Comp. Sci. and App. Logic, vol. 15, Birkhäuser Verlag Basel, 1998.

[HoSt] D.Hofheinz, and R. Steinwandt: A "Differential" Attack on Polly Cracker. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, 2002, pp 211.

[Ja] M. Jantzen: Confluent String Rewriting, Springer-Verlag, Berlin, New York, 1988.

[No] P. Nordbeck: On the finiteness of Gröbner bases computation in quotients of free algebras. AAECC, 11, 2001, pp 157 - 160.

[Ko] N. Koblitz: Algebraic aspects of cryptography, Algorithms and computations in Math., vol. 3, Springer, 1997.

[Ly] L. Van Ly: Polly Two — A Public Key Cryptosystem based on Polly Cracker. Ph.D. Dissertation, Rhur Universität Bochum, Germany, 2002.

[MVoV] A. Menezes, P. van Oorschot, and S. Vanstone: Handbook of applied cryptography. CRC Press, Boca Raton, 1997.

[MF] F. Mora: Gröbner basis for non-commutative polynomial rings. Proc. AAECC3, LNCS 229. Springer-Verlag, Berlin, New York, 1986.

[MT] T. Mora: An introduction to commutative and non-commutative Gr"obner bases. Theoretical Comp. Sci., 134:131-173, 1994.

[MTea] T. Mora et al: [pseudonyms Boo Barkee, Deh Cac Can, Julia Ecks, Theo Moriarty, R.F. Ree] Why you cannot even hope to use Gröbner bases in public key cryptology: An open letter to a scientist who failed and a challenge to those who have not yet failed, Jour. Symb. Comput., vol. 18, 1994, pp 497 - 501.

[Pa] J. Patarin: Asymmetric cryptography with a hidden monomial. Advances in Cryptology — Crypto '96, Springer-Verlag, 1996, pp 33 - 48.

[Sc] B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, 2nd ed. Wiley, New York, 1996.

[St] D. Stinson: Cryptography: theory and practice. Chapman & Hall/CRC, Boca Raton, 2002.

[WaTr] L. Washington and W. Trappe: Introduction to Cryptography with Coding Theory. Prentice Hall, New Jersey, 2002.

Curriculum Vitae

Tapan S. Rai

Education

Ph. D. (Mathematics),	Virginia Tech, Blacksburg, Virginia.	2004
M. S. (Mathematics),	Virginia Tech, Blacksburg, Virginia.	1988
B. Sc. (Mathematics),	University of Bombay, Bombay, India.	1986

Employment History

Professor,	Centennial College, Toronto, Ontario.	1999 - present
Sessional Professor,	Seneca College, Toronto, Ontario.	1997 - 1999
Instructor,	Virginia Tech, Blacksburg, VA.	1993 - 1997
Visiting Lecturer,	Narsee Monjee College, Bombay, India.	1993
G. T. A.,	Virginia Tech, Blacksburg, Virginia.	1987 - 1992

Other Scholarly and Professional Activities

Visiting Scholar,	Virginia Tech, Blacksburg, VA.	2002 - 2003
Presenter/Participant,	Algebra Seminar, Centennial College.	2002, 2003
Honorary Visitor,	T. I. F. R., Bombay, India.	1992 - 1993
Member,	American Mathematical Society.	