Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»

(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)

КАФЕДРА «Информационная безопасность» (ИУ8)

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

Современные методы

алгебраического криптоанализа

Студент ИУ8-94 (Группа) _____ (Подпись, дата) А.Д. Полухина (И.О. Фамилия)

Научный руководитель _____ (Подпись, дата) П.Г. Ключарев (И.О. Фамилия)

2019 г.

РЕФЕРАТ

Отчет содержит 16 стр., 2 рис., 2 источн., 2 прил.

Это пример каркаса расчётно-пояснительной записки, желательный к использованию в РПЗ проекта по курсу РСОИ .

Данный опус, как и более новые версии этого документа, можно взять по адресу (`https://github.com/latex-g7-32/latex-g7-32`).

Текст в документе носит совершенно абстрактный характер.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

API — test

MAX — максимум

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ТЕСТ — Logical Volume Manager

ВВЕДЕНИЕ

Целью работы является создание всякой всячины. Для достижения поставленной цели необходимо решить следующие задачи:

— проанализировать существующую всячину;

— спроектировать свою, новую всячину;

— изготовить всякую всячину;

— проверить её работоспособность.

Проверяем как у нас работают сокращения, обозначения и определения — MAX API API ТЕСТ с обратным прокси.

ОСНОВНАЯ ЧАСТЬ

1 Понятие идеала в кольце многочленов

В первой части научно-исследовательской работы даются базовые определения и понятия, которые будут использоваться на протяжении всей расчетно-пояснительной записки.
Пусть R - коммутативное кольцо с единицей 1.

1.1 Понятие идеала

Непустое подмножество I кольца R называется идеалом в R (записывается $I \lhd R$), если:

1) для любых элементов a,$b \in I$ элемент $a + b \in I$;

2)для любых $a \in I, c \in R$ элемент $ac \in I$.

Идеал I кольца R называется главным, если существует такой элемент $a \in I$, что $I = (a)$. Элемент a называется порождающим(или образующим) для идеала I.

Кольцо R называется кольцом главных идеалов, если каждый идеал кольца R является главным.

1.2 Базис идеала

Обобщим по понятие главного идеала I кольца R. Пусть $a_1, ..., a_k$ - произвольные элементы кольца R.

Если множество

$$(a_1, ..., a_k) = \{a_1r_1 + ... + a_kr_k; r_1, ..., r_k \in R\}$$

есть идеал I кольца R, тогда говорят, что элементы $a_1, ..., a_k$ составляют базис идеала I. Обозначается $I = (a_1, ..., a_k)$.

Можно заметить, что при определении базиса идеала нет требования на минимальное количество базисных элементов. Это связано с тем, что при

добавлении к базису произвольного элемента идеала, мы получаем тот же самый базис.

Для любого элемента $a \in (a_1, ..., a_k)$:

$$(a_1, .., a_k, a) = (a_1, ...,a_k)$$

Легко убедиться в достоверности этого утверждения. По определению $(a_1, ..., a_k, a) = \{a_1r_1 + ... + a_kr_k + ar; r_1, ..., r_k, r \in R\}$. По определению идеала I кольца R, если $a \in I, r \in R$, то элемент $ar \in I$. Тогда $ar = a_1r'_1 + ... + a_kr'_k; r'_1, ..., r'_k, \in R$. Подставим это выражение в определение базиса $(a_1, ..., a_k, a) = \{a_1r_1 + ... + a_kr_k + a_1r'_1 + ... + a_kr'_k; r_1, r'_1, ..., r_k, r'_k \in R\} = \{a_1(r_1 + r'_1) + ... + a_k(r_k + r'_k); r_1, r'_1, ..., r_k, r'_k \in R\}$. Таким образом, при добавлении нового базисного элемента, который принадлежит идеалу, базис не изменится.

1.3 Идеал в кольцах многочленов

Пусть $K[x_1, ..., x_n]$ - кольцо многочленов от переменных $x_1, ...,x_n$ над полем $\mathcal{K}$. Рассмотрим идеалы в кольцах многочленов.

Легко убедиться в том, что кольцо многочленов от нескольких переменных не является кольцом главных идеалов. В кольце многочленов $K[x_1, ..., x_n]$ выделим множество многочленов, у которых свободных член равен 0. Данное множество образует идеал в этом кольце, обозначим его I_0. Пусть $I_0 = (f), f \in K[x_1, ..., x_n]$. Поскольку $x_1 \in I_0$, значит f - либо ненулевая константа (тогда $I_0 = K[x_1, ..., x_n]$, что является противоречием условия), либо $f = ax, a \in \mathcal{K}, a \neq 0$. Но $x_2 \in I_0$, значит f делит x_2. Возникает противоречие.

Раз кольцо многочленов от нескольких переменных не является кольцом главных идеалов, значит имеет место понятие базиса идеала. В следующем параграфе будут подробно рассмотрены базисы идеала в кольце многочленов от нескольких переменных и выведены некоторые утверждения.

2 Мономиальные базисы идеалов в кольцах многочленов

В данном разделе будут подробно рассмотрены мономиальные базисы идеалов в кольцах многочленов от нескольких переменных и введено понятие базиса Гребнера.

2.1 Мономиальный порядок и его свойства

Пусть M_n - множество мономов. Мономиальным упорядочением $\prec$ на M_n называется линейный порядок, удовлетворяющий свойствам:

1) $M \prec N \Rightarrow MP \prec NP, \forall M, N, P \in M_n$

2)$1 \preceq M, \forall M \in M_n$

Пусть $M = x_1^{a_1}...x_n^{a_n}$, $N = x_1^{b_1}...x_n^{b_n}$ - произвольные мономы из M_n. Приведем несколько примеров бинарных отношений на M_n, которые являются мономиальными упорядочениями:

1. Лексикографическое упорядочение (lex):

$$M \prec_{lex} N \Leftrightarrow (a_1, ..., a_n) \prec_{lex} (b_1, ..., b_n)$$

2. Сначала по степени, затем лексикографическое упорядочение (deglex):

$$M \prec_{deglex} N \Leftrightarrow (deg(M), a_1, ..., a_n) \prec_{lex} (deg(N), b_1, ..., b_n)$$

3. Сначала по степени, затем обратное лексикографическое упорядочение (degrevlex):

$$M \prec_{degrevlex} N \Leftrightarrow (deg(M), b_n, ..., b_1) \prec_{lex} (deg(N), a_n, ..., a_1)$$

Далее введем несколько обозначений, которые понадобятся нам в дальнейшем.

Пусть $f = \sum_a p_a x^a$ - ненулевой полином в $K[x_1, ..., x_n]$, и пусть $\prec$ - мономиальное упорядочение.

1. Мультистепень полинома f определяется так:

$$multideg(f) = max(a \in Z^n_{\geqslant 0} : p_a \neq 0)$$

2. Старший коэффициент полинома f:

$$LC(f) = p_{multideg}(f)$$

3. Старший моном полинома f:

$$LM(f) = x^{multideg}(f)$$

(с коэффициентом 1)

4. Старший член полинома f:

$$LT(f) = LC(f)LM(f)$$

2.2 Мономиальные идеалы

Введем понятие мономиального идеала в кольцое многочленов от нескольких переменных.

Идеал $I \lhd K[x_1, ..., x_n]$ называется мономиальным, если существует подмножество $A \in Z^n_{\geqslant 0}$ (которое может быть бесконечым), такое, что I состоит из всех конечных сумм вида $\sum_{a \in A} h_a x^a$, где $h_a \in K[x_1, ..., x_n]$. Такой идеал будем обозначать $(x^a : a \in A)$.

Лемма Диксона. *Любой мономиальный идеал $I = (x^a : a \in A)$ может быть представлен в виде $I = (x^{a(1)}, ..., x^{a(s)}$, где $a(1), ..., a(s) \in A$. В частности, I имеет конечный базис.*

2.3 Теорема Гильберта о базисе

В предыдущем параграфе было показано, что любой мономиальный идеал кольца многочленов от нескольких переменных иметь конечный базис. В этом разделе будет доказано, что любой идеал в кольце многочленов(не только мономиальный) имеет конечный базис.

Теорема Гильберта о базисе. *Каждый идеал $I \lhd K[x_1, ..., x_n]$ является конечно порожденным, то есть $I = (g_1, ..., g_s)$, где $g_1, ..., g_s \in I$.*

Доказательство. Пусть $I \lhd K[x_1, ..., x_n]$. Обозначим через a_t множество элементов $a \in \mathcal{K}$, которое содержит в себе $LC(f)$, где $f \in I$ и

$multideg(f) = t$. Легко видно, что a_i является идеалом в $\mathcal{K}$. (Если a,$b \in a_i$, то $a \pm b \in a_i$, это легко увидеть, достаточно взять сумму или разность соответсвующих многочленов. Если $c \in \mathcal{K}$, то $ca \in a_i$, это можно увидеть при умножении соответсвующего многочлена на c.) Кроме того, имеем

$$a_0 \subset a_1 \subset a_2...$$

другими словами последовательность идеалов $[a_i]$ возрастающая.
Пусть последовательность идеалов стабилизируется на a_r:

$$a_0 \subset a_1 \subset a_2... \subset a_r = a_{r+1} = ...$$

Пусть

$$a_0 = (a_{01}, a_{02}, ..., a_{0n_0})$$

$$a_r = (a_{r1}, a_{r2}, ..., a_{rn_0})$$

Для каждого $i = 0, ..., r$ и $j = 0, ..., n_i$ пусть f_{ij} - многочлен из I степени i со старшим коэффициентом a_{ij}. Покажем, что многочлены f_{ij} образуют базис для I.
Пусть f - многочлен степени d из I. Индукцией по d докажем, что f лежит в идеале, порожденном f_{ij}.
Если $d > r$, то заметим, что старшие коэффициенты многочленов

$$X^{d-r} f_{r1}, ..., X^{d-r} f_{rn_r}$$

порождают a_d. Значит, существуют $c_1, ..., c_{n_r} \in \mathcal{K}$, такие, что многочлен

$$f - c_1 X^{d-r} f_{r1} - ... - c_{n_r} X^{d-r} f_{rn_r}$$

имеет степень $< d$. Этот многочлен лежит в I. Если $d \leqslant r$, мы можем получить многочлен степени $< d$, лежащий в I, вычитая некоторую линейную комбинацию

$$f - c_1 f_{d1} - ... - c_{n_r} f_{dn_r}$$

По индукции мы можем найти такой многочлен $g \in I$, который порожден f_{ij} и $f - g = 0$, доказав таким образом теорему.

2.4 Базис Гребнера

В предыдущем параграфе была приведена и доказана фундаментальная теорема, связанная с базисом идеалов в кольцах многочленов. Далее будет введено понятие базиса Гребнера и описаны его особенности.

Пусть задано мономиальное упорядочение. Конечное подмножество $G = g_1, ..., g_s$ элементов идеала I называется его базисом Гребнера, если

$$(LT(g_1), ..., LT(g_s)) = (LT(I))$$

Стоит отметить, что любой $I \lhd K[x_1, ..., x_n]$ имеет базис Гребнера. Это легко увидеть из доказательства теоремы Гильберта о базисе.

Базис Гребнера является очень важным элементом в алгебраическом криптоанализе. Он помогает упрощать и решать алгебраические системы уравнений, выявлять различные особенности, связанные с той или иной системой алгебраических уравнений (например, существует эффективный критерий несовместимости системы). Поэтому, нахождение базиса Гребнера является одной из важных математических задач на данный момент. Далее будут рассмотрены три алгоритма нахождения базиса Гребнера (алгоритм Бухбергера, алгоритм $F4$ и алгоритм $F5$).

ЗАКЛЮЧЕНИЕ

В результате проделанной работы стало ясно, что ничего не ясно...

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Пупкин Василий, Эйнштейн А. LaTeXдля «чайников». — М., 2009. — 299 с.

2. Wikipedia. Типографика — Википедия. — 2012. — Режим доступа: https://ru.wikipedia.org/wiki/%D0%A2%D0%B8%D0%BF%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%BA%D0%B0 (дата обращения: 25.01.2012).

ПРИЛОЖЕНИЕ А

КАРТИНКИ

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Рисунок А.1 — Картинка в приложении. Страшная и ужасная.

ПРИЛОЖЕНИЕ Б

ЕЩЕ КАРТИНКИ

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Рисунок Б.1 — Еще одна картинка, ничем не лучше предыдущей. Но надо же как-то заполнить место.