An example of a thesis on the subject of your degree

by

Stuart Arthur Dent

M.Sc., Wossamotta University, 1963
B.Sc., Unseen University, 1836

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy

in the
Department of Inadvisably Applied Mathematics
Faculty of Example Names

SIMON FRASER UNIVERSITY
Fall 2021

Declaration of Committee

Name:	**Stuart Arthur Dent**
Degree:	**Doctor of Philosophy**
Thesis title:	**An example of a thesis on the subject of your degree**
Committee:	**Chair:** Pamela Isely Assistant Professor, Computing Science
	Emmett Brown Supervisor Professor, Computing Science
	Bonnibel Bubblegum Committee Member Associate Professor, Computing Science
	James Moriarty Committee Member Adjunct Professor, Computing Science
	Kaylee Frye Examiner Assistant Professor, Engineering Science
	Hubert J. Farnsworth External Examiner Professor Department of Quantum Fields Mars University

Abstract

Abstract paragraphs should be unindented. Master's abstracts are limited to 150 words; the limit is 350 words for doctoral abstracts. Abstract text must fit on a single page.

Keywords: thesis template; Simon Fraser University; LaTeX time travel paradoxes

Dedication

This is an optional page. Use your choice of paragraph style for text on this page.

Acknowledgements

This is an optional page. Use your choice of paragraph style for text on this page.

Table of Contents

Declaration of Committee **ii**

Abstract **iii**

Dedication **iv**

Acknowledgements **v**

Table of Contents **vi**

List of Tables **vii**

List of Figures **viii**

1 Introduction **1**

1.1 Blackboxes and Evaluation homomorphism 1

1.1.1 Blackboxes 1

1.1.2 Evaluation homomorphism 1

2 Maximal Quotient Rational Function Reconstruction **2**

2.1 Univariate Rational function reconstruction 2

2.1.1 Interpolation 2

2.1.2 Extended Euclidean Algorithm 2

2.1.3 Chinese Remainder Theorem 3

2.1.4 Chinese remainder theorem and evaluating black box for polynomials 3

2.1.5 Main idea 4

3 Ben-Or and Tiwari's Multivariate Polynomial Interpolation **6**

3.1 Introduction 6

Bibliography **7**

Appendix A Code **8**

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Blackboxes and Evaluation homomorphism

1.1.1 Blackboxes

Definition 1.1.1. *A blackbox is a function that takes an input and produces an output. The internal workings of the function are not known to the user. The user can only interact with the blackbox by providing inputs and observing the outputs.*

1.1.2 Evaluation homomorphism

Definition 1.1.2. *Let K be a field and $K[x] \in K(x)$ be the ring of polynomials and field of rational functions respectively. Let $\alpha \in K$ be a point in the field. The evaluation homomorphism is a map*

$$\begin{array}{rrcl} \phi: & K[x] & \longrightarrow & K[x]/(x-\alpha) \cong K \\ & f(x) & \longmapsto & f(\alpha) \end{array}$$

Chapter 2

Maximal Quotient Rational Function Reconstruction

2.1 Univariate Rational function reconstruction

We are given a black box for a rational function $F(x) = \frac{f(x)}{g(x)} \in K(x)$ where $f(x), g(x) \in K[x]$ and $g(x) \neq 0$. We need to recover the polynomials $f(x), g(x)$ upto a constant factor. We can evaluate the black box at n distinct points $\alpha_1, \ldots, \alpha_n$ to gets the values $y_1, \ldots, y_n$.

2.1.1 Interpolation

Given a set of points

2.1.2 Extended Euclidean Algorithm

Algorithm 1 Extended Euclidean Algorithm

$r_0 \leftarrow f, \quad s_0 \leftarrow 1, \quad t_0 \leftarrow 0$
$r_1 \leftarrow g, \quad s_1 \leftarrow 0, \quad t_1 \leftarrow 1$
i=1
while $r_i \neq 0$ **do** do
    $q_i \leftarrow r_{i-1}/r_i$
    $r_{i+1} \leftarrow r_{i-1} - q_i r_i$
    $s_{i+1} \leftarrow s_{i-1} - q_i s_i$
    $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
    $i \leftarrow i + 1$
end while
$l \leftarrow i - 1$
return $r_l, s_l, t_l \in K[x]$

$$\begin{array}{r} \frac{f}{g} = \quad g^{-1}f \\ g) \overline{\quad f} \\ \underline{-f} \\ 0 \end{array}$$

Theorem 2.1.1. *Bezout's identity*

$$\text{Let } f, g \in K[x] \text{ such that } f, g \neq 0$$

$$\text{Let } d = gcd(f, g) \text{ then } \exists s, t \in K[x] \text{ such that}$$

$$s_i f + t_i g = d$$

$$\text{when } gcd(f, g) = 1 \implies s_l f + t_l g = 1$$

$$\implies t_l g \equiv 1 \mod f \implies t_l = \frac{1}{g} \mod f$$

2.1.3 Chinese Remainder Theorem

Theorem 2.1.2. *[1] Let $I_1, I_2, .., I_k$ be ideals in a ring R. The map*

$$\begin{array}{rccl} \phi: & R & \longrightarrow & R/I_1 \times R/I_2 \times \cdots \times R/I_k \\ & r & \longmapsto & (r + I_1, r + I_2, \ldots, r + I_k) \end{array}$$

is a ring homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$,the ideals I_i, I_j are called comaximal and the map ϕ is surjective. Moreover,

$$I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \ldots I_k$$

$$\implies R/(I_1 I_2 \ldots I_k) = R/(I_1 \cap I_2 \cap \cdots \cap I_k) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

2.1.4 Chinese remainder theorem and evaluating black box for polynomials

We know the following result from algebra that,

Theorem 2.1.3. *Let $K[x]$ be a polynomial ring over a field K and let $I \subset K[x]$ be an ideal of the ring then $K[x]/I$ is a field if and only if I is a maximal ideal.*

Given a black box B for a polynomial $f(x) \in K[x]$ and $x = \alpha \in K$ we can evaluate $f(\alpha)$ by querying the black box B at α.

$$\begin{array}{rccl} \phi: & K[x] & \longrightarrow & K[x]/(x - \alpha) \\ & f(x) & \longmapsto & f(\alpha) \end{array}$$

Thus, evaluating the polynomial at n points is querying the black box at n points $\alpha_1, \ldots, \alpha_n$ is the following homomorphism.

$$\begin{array}{rccl} \phi: & K[x] & \longrightarrow & K[x]/(x-\alpha_1) \times K[x]/(x-\alpha_2) \times \cdots \times K[x]/(x-\alpha_n) \\ & f(x) & \longmapsto & (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \end{array}$$

From the Chinese remainder theorem, we know that

$$K[x]/(x-\alpha_1) \times K[x]/(x-\alpha_2) \times \cdots \times K[x]/(x-\alpha_n) \cong K[x]/((x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n))$$

$$\text{Let } \left[\alpha_1, \ldots, \alpha_n\right] \in K^n$$

such that

$$\alpha_i \neq \alpha_j \forall i \neq j \text{ and } n > 0.$$

$$\text{Let } F(x) = \frac{f(x)}{g(x)} \in K(x), \text{ where } f(x), g(x) \in K[x],$$

$$\text{Let } y_i = F(\alpha_i) = \frac{f(\alpha_i)}{g(\alpha_i)}, \forall 1 \leq i \leq n, \text{ such that } g(\alpha_i) \neq 0.$$

$$\exists!\ u(x) \in K[x] \text{ of degree} < n \text{ such that } u(\alpha_i) = y_i$$

$$\implies u(x) \equiv y_i \mod (x-\alpha_i)$$

$$\implies F(x) = \frac{f(x)}{g(x)} \equiv u(x) \mod (x-\alpha_i)$$

$$\text{Let } \overline{m}(x) = \prod_{i=1}^{n}(x-\alpha_i)$$

2.1.5 Main idea

1. We are given the black box of rational polynomial $F(x) \in K(x)$. We have the option to choose n distinct points $\alpha_1, \ldots, \alpha_n$,such that $n > degree_numerator + degree_denominator$ and evaluate the black box at these points to get $y_1, \ldots, y_n$.

2. Construct two polynomials m, u out of these two sets of points.

3. $m(x) = \prod_{i=1}^{n}(x-\alpha_i)$ is the Chinese remainder theorem polynomial.

4. $u(x) = Interpolation(\alpha_i, y_i)$. Note that the degree of $u(x) = n-1$ and the degree of $m(x) = n$.

5. We take these two polynomials m, u and apply the extended euclidean algorithm to get $f(x), g(x) \implies f, g$ appear as remainder and coefficient in the division algorithm.

6. We can think of any rational function $\frac{f}{g}$as members of an equivalence class.(localization?) with other elements.

7. What MQRFR says is that the $f = r_i$nd $g = t_i$ for the i^{th} iteration of the extended euclidean algorithm such that $deg(q_i)$ is max.

8. There does seem to be some relationship between Univariate rational functions, the interpolated polynomial u the product polynomial m and the extended euclidean algorithm(m,u).

9. CRT from 265 Dummit and Foote.

10.

Chapter 3

Ben-Or and Tiwari's Multivariate Polynomial Interpolation

3.1 Introduction

Ben-Or Tiwari is an multivariate interpolation algorithm that interpolates all the variables of the polynomial simultaneously as opposed to Zippel's multivariate interpolation algorithm which interpolates the variables one by one.

Bibliography

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

[2] Frank Mittelbach and Michel Goossens. *The LaTeX Compation*. Addison-Wesley, 2004.

Appendix A

Code

Appendices should be used for supplemental information that does not form part of the main research. Remember that figures and tables in appendices should not be listed in the List of Figures or List of Tables.