Analysis of The Computer-Mathematics Research System ELIMINO

Iyad A. Ajwa*
Department of Mathematics and Computer Science
Ashland University
Ashland, OH 44805, USA

Abstract

This paper presents an analysis of ELIMINO, a computer-mathematics research system that has been developed at the Chinese Academy of Sciences. Also presented are ideas to improve the performance of ELIMINO and an overview of the Characteristic Sets Method.

1 Introduction

The origins of algorithms in mathematics date back to more than two thousand years ago, as can be seen from the fact that one of the most important known algorithms bears the name of the Greek mathematician Euclid. However, the word "algorithm" as well as the key word "algebra" come from the ninth-century scientist Muhammad ibn Mûsâ al-Khawârizmî (770 - 840), who was born in what is now Uzbekistan and worked in Baghdad at the court of Harun Al-Rashid's son. His parents migrated to Baghdad when he was a child. He was apparently a genius, and as a young man was invited to be a scholar at a government-sponsored institution called *Bayt Al-Hikmah* or the House of Wisdom [1].

The word "algorithm" is actually a westernization of al-Khawârizmî's name while "algebra" derives from "al-jabr," a term that appears in the title of his book *kitab al-jabr wa'l muqabala* which translates into *The Compendious Book on Calculation by Completion and Balancing*, where he discusses symbolic methods for solving polynomial equations [1]. This close connection between algebra and algorithms lasted roughly up to the beginning of this century; until then, the primary goal of algebra was the design of constructive methods for solving equations by means of symbolic transformations.

With the development of computers, the central role of algebraic algorithms has been recognized. Recent advances in computer technology coupled with the long-standing interest in algebraic algorithms have made it necessary to study computer related topics to algorithms, such as their efficiency, implementation, hardware/software needs, and so on. This has lead to the establishment of *Computer Algebra*, a field of study that extends deeply into both mathematics and computer science.

Over the years, new concepts and results have developed in the area of computer algebra and computer algebraists have made significant contributions to the fields of Mathematics and Computer Science. Among these contributions, an outstanding example is the theory and algorithm for computing Characteristic Sets.

*Work reported herein has been supported by Ashland University under a Study/Writing Grant

2 The Characteristic Sets Method

Developed from Ritt's work on differential algebra, the Characteristic Setsmethod was discovered independently by the Chinese mathematician Wen-tsün Wu (hence, the name Wu's Method) in 1978 [5]. The two mathematicians had different goals. J. F. Ritt laid the foundations of the Characteristic Sets method in the context of his work on differential algebra. He was interested in studying differential equations from an algebraic standpoint. On the other hand, Wu rediscovered the Characteristic Sets Method in the context of his work on mechanical geometry theorem proving. He developed Ritt's work for the algebraization of geometry and introduced a powerful algebraic algorithm to compute the Characteristic Sets for a set of multivariate polynomials [2].

It is easy to explain the main ideas behind the Characteristic Sets method to a reader with some background in abstract algebra. Given a set F of multivariate polynomials over a field K, the *ideal* generated by F is the set of all polynomials P such that either P is divisible by some polynomial in F or P is a sum of polynomials each is divisible by some polynomial in F. The *Characteristic Set* of F is a well-defined triangular form of F that possesses wonderful properties and makes answering a number of important questions in commutative algebra and algebraic geometry easy. The algorithm depcited in Figure 1 computes the Characteristic Set of a given set of polynomials F.

Input: A set of multivariate polynomials F
Output: A Characteristic Set, CS
Method:
$QS := F$;
$RS := F$;
Repeat
  $CS := BasicSet(QS)$;
  IF CS is contradictory then
    $RS := \phi$
  ELSE
    $RS := \{r \mid r = \text{PseudoRemainder}(q, CS), r \neq 0, q \in QS - CS\}$;
    $QS := QS \bigcup RS$;
Until $RS = \phi$

Figure 1: The Characteristic Sets Method

The Characteristic Sets Method has a wide variety of applications including mechanical geometry theorem proving, theoretical physics, CAGD, robotics, and automated reasoning. The method has been extensively studied in China and abroad and has developed very fast during the past two decades. Several geometry provers have been written and the algorithm has been implemented on most computer algebra systems including Maple and Mathematica. However, no computer algebra system provides the user with a friendly environment to use the Characteristic Sets Method. Such situation partly hindered the further development of the Characteristic Sets Method [4]. ELIMINO is an effort to construct a software system for the Characteristic Sets Method that is independent of any existing mathematical software system [4].

3 The ELIMINO System

ELIMINO is a computer-mathematics research system that is developed at the Mathematics Mechanization Research Center (MMRC) of the Chinese Academy of Sciences as part of the "Mathematics Mechanization and its Applications" project [4]. A long-standing goal at MMRC is to automate Wu's method independent of existing computer algebra systems. ELIMINO is designed to focus on the implementation of Wu's method. However, in order to support Wu's method, ELIMINO also has very general computational capabilities for numbers, polynomials, and Characteristic Sets. Hence, it provides researchers with several kinds of mathematical objects and data structures to perform sophisticated mathematical computations.

3.1 Organization

ELIMINO consists of several components, that are distributed in layers, including the frontend, kernel, task manager, memory manager, and data manager. Each layer is an independent module, written in ANSI standard C/C++, providing a collection of closely-related and tightly organized services. A lower layer never calls functions in an upper layer.

From the user viewpoint, ELIMINO consists of the following three parts:

- Kernel. The kernel part is the heart of the system. It contains implementations of number system, polynomial manipulation system, and the Characteristic Sets Method.
- Applications. The applications part consists of packages that are developed using the ELIMINO library. Examples include the polynomial system solver and the geometry theorem prover.
- Front-end. The front-end part is the interface between the system and user. It handles I/O between the user and the system.

3.2 Analysis

ELIMINO has been designed from the beginning to be an open and flexible research platform. It's open architecture is enhanced by Object-Oriented Design (OOD) and Object-Oriented Programming (OOP) techniques. The system is organized into modules and has a clear separation of the kernel and the user levels. Users can write ELIMINO programs following the simple and efficient *User API* either interactively or by loading saved files. Currently, ELIMINO has the following features:

- Object-Oriented Design - The system has been developed following the Object-Oriented (OO) method of Coad and Yourdan and is written in C++ [4]. It is a collection of objects and each object has an associated datatype (property of the object). The datatype of an object determines the operations that are applicable to the object and clearly separates the various kinds of objects in the system.
- Expandable - The system allows easy integration of new methods or research achievements into the system. Thus, the system is expandable, a package may be built-in or loaded into ELIMINO on demand.
- Interactive - The system provides an interactive interpretation environment: read input expression from the user, evaluate the expression, and display the results back to the user.

- Arithmetic - The ELIMINO arithmetic packages support computations with integers, rational numbers, floating-point numbers, and modular numbers. Where appropriate, these can be combined in the same computation because the system knows how to convert between these types of numbers automatically. The sizes of these numbers are only bounded by the amount of memory. For approximations, floating-point computations can be performed with any desired number of digits.

- Polynomial Computations - Polynomials play a central role in ELIMINO. Many basic polynomial operations have been implemented to support Wu's Method. In addition, ELIMINO supports polynomial factorization over algebraic extension fields with adjoining polynomials in ascending sets.

- Wu's Method - The system is designed to focus on Wu's Method which is implemented in the kernel part of ELIMINO. In addition, ELIMINO provides an interactive environment for Mechanical Geometric Theorem Proving based on Wu's Method.

- Linear Algebra - ELIMINO provides functions for basic operations on vectors and matrices.

- Programming Language - ELIMINO provides an embedded programming language with limited control constructs such as selection and interaction controls.

4 Improving ELIMINO

ELIMINO is already a very useful system for research. But, its power and applicability can be significantly increased by implementing more algorithms, making it an open-source community development software, and by providing good organization.

4.1 Make It Open-Source

ELIMINO provides a good base upon which to build a powerful system through the open source community software process. As an open source and community development software, OpenElimino will become an evolving system as researchers and developers can easily make contributions in it. Algorithmic mathematics researchers may make their contributions by adding their new algorithm implementations into the ELIMINO kernel. Other researchers may add their domain specific modules into ELIMINO so that other researchers may develop higher level applications on them. The open-source ELIMINO should become a useful research tool

- for those who want to do research in algorithmic mathematics and its applications and, hence, need access to all details of the implementations of algorithms; and also

- for those who want to apply these algorithms as a black box, possibly as subalgorithms in larger implementations, and need high efficiency.

4.2 Implement More Algorithms

Addition kernel support needs to be identified and implemented to make it easier for everyone to develop new algorithms and functionalities. One important addition to the kernel would be the implementation of the Gröbner Bases Algorithm [2]. In addition, the frontend of ELIMINO

can be enhanced by adding a new GUI component in addition to the existing text only interface. Moreover, more applications can be implemented in the applications layer of ELIMINO.

4.3 Provide Better Organization

Currently, ELIMINO does not have a good software organization. The source code of all functions implemented are in one directory. The organization can be improved by

- Using a well-defined structure of separate directories including bin (for binary files), doc (for a user's guide and other documentation), examples (for the source code of examples on how to use ELIMINO), include (for all header files included in the source code), lib (for libraries and archives), src (for source code files), etc.
- Providing good documentation. Currently, the system is documented using the Chinese language. In order to make the system easily accessible to international researchers, documentation in English should be provided. This documentation include a user's guide, README files, and API documentation.

References

[1] I. Ajwa, *Parallel Algorithms and Implementations for the Gröbner Bases Algorithm and the Characteristic Sets Method,*" Ph.D. Dissertation, Kent State University, Kent, Ohio, December 1998.

[2] I. Ajwa, Z. Liu, and P. Wang. *On the Characteristic Sets Method.* ICM Technical Reports Series, Kent State University, Kent, Ohio, USA (1996).

[3] I. Ajwa, Z. Liu, and P. Wang, *The Gröbner Bases Algorithm*, ICM Technical Reports (ICM-199502-00), Kent State University, Kent, Ohio, USA, 1995. Prentice Hall (1990).

[4] D. Lin, J. Liu and Z. Liu. *Mathematical Research Software: ELIMINO.* Proceedings of ASCM'98. pp. 107 - 116, Lanzhou University, China (1998).

[5] W-T. Wu, "Basic Principles of Mechanical Theorem Proving in Elementary Geometries," Journal of Sys. Sci. and Math. Scis. 4, pp. 207-235, 1984. (Also in: Journal of Automated Reasoning 2, pp. 221-252, 1986.)