The South African Institute of Computer Science and Information Technology

The 1997 National Research and Development Conference

Riverside Sun
Vanderbijlpark
13 & 14 November

Hosted by

Potchefstroomse Universiteit vir Christelike Hoër Onderwys

The Department of Computer Science and Information Systems
Potchefstroom University for Christian Higher Education
Vaal Triangle Campus

PROCEEDINGS

Edited by L.M. Venter & R.R. Lombard
The South African Institute of Computer Science and Information Technology

Proceedings
of the
The 1997 National Research and Development Conference
Towards 2000

Riverside Sun
Vanderbijlpark
13 & 14 November

Edited by
L.M. Venter
R.R. Lombard
Foreword

This book contains a collection of papers presented at a Research and Development conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT). The conference was held on 13 & 14 November 1997 at the Riverside Sun, Vanderbijlpark. Most of the organization for the conference was done by the Department of Computer Science and Information Technology of the Vaal Triangle Campus, Potchefstroom University for Christian Higher Education.

The programming committee accepted a wide selection of papers for the conference. The papers range from detailed technical research work to reports of work in progress. The papers originate mainly from Academia, but also describe work done in and for Industry. It is hoped that the papers give a true reflection of the current research scene in Computer Science and Information Technology in South Africa. Since one of the aims of the conference is Research development, the papers were not subjected to a refereeing process.

A number of people spent numerous hours helping with the organization of this conference. In this regard, we wish to thank the members of the Organizing committee, and the Programming committee who had very little time to screen the abstracts and compile the program. A special thanks goes to the secretary of the department, Mrs Helei Jooste, whose very able work was interrupted by the birth of her first child.
Organizing Committee

Conference General Chairs
Prof. J.M. Hattingh (PU for CHE)

Organizing Chair
Prof. Lucas Venter (PU for CHE)

Organizing Committee
Mrs. S. Gilliland
Mr. J.P. Jooste
Mr. R.R. Lombard
Mrs. M. Huisman

Secretariat
Mrs. H. Jooste

Program Chair
Prof A de Waal (PU for CHE)

Program Committee
Prof. D. Kourie (UP)
Prof. C. Bornman (UNISA)
Prof. L.M. Venter (PU for CHE)
# Table of Contents

Foreword

Organizing Committee

List of Contributors

*Software Objects Change: Problems and Solution*
S.A. Ajila 1

*Liming-like Curve Constructions*
M.L. Baart and R. McLeod 26

*A Model for Evaluating Information Security*
L. Barnard and R. von Solms 27

* Integrating Spatial Data Management and Object Store Technology*
S. Berman, S. Buffler and E. Voges 31

*Metamodelling in Automated Software Engineering*
S. Berman and R. Figueira 32

*Using Multimedia Technology for Social Upliftment in Deprived Communities of Southern Africa*
L. Bester and E. de Preez 33

*Extending the Client-Server Model for Web-based Execution of Applications*
L. Botha, J.M. Bishop and N.B. Serbedzija 36

*Access Control Needs in an Electronic Workflow Environment*
R.A. Botha 45

*The Use of the Internet in an Academic Environment to Commercially Supply and Support Software Products*
B. Braude and A.J. Walker 51

*Explanation Facilities in Expert Systems Using Hypertext Technology*
T. Breetzke and T. Thomas 63

*Theoretical Computer Science: What is it all about, and is it of any relevance to us?*
C. Brink 75

*Representing Quadrics on a Computer*
M.A. Coetzee and M.L. Baart 76
The Generation of Pre-Interpretations for Detecting Unsolvable Planning Problems
D.A. de Waal, M. Denecker, M. Bruynooghe and M. Thielscher

The Emerging Role of the Chief Information Officer in South Africa
B. Dekenah

A Java-Implemented Remote Respiratory Disease Diagnosis System on a High Bandwidth Network
A. Foster

Early Results of a Comparative Evaluation of ISO 9001 and ISO/IEC 15504 Assessment Methods Applied to a Software Project
C. Gee and A.J. Walker

A Neural Network Model of a Fluidised Bed
M. Hajek

The Effects of Virtual Banking on the South African Banking Industry
M.L. Hart and M. Dunley-Owen

Linear Response Surface Analysis and Some Applications
J.M. Hattingh

Model Checking Software with Symbolic Trajectory Evaluation
A. Hazelhurst

A Risk Model to Allocate Resources to Different Computerized Systems
H.A. Kruger and J.M. Hattingh

Returns on the Stock Exchange
J.W. Kruger

Cardinality Constrained 0-1 Knapsack Problems
M.F. Kruger, J.M. Hattingh and T. Steyn

An Investigation in Software Process Improvement in the Software Development of a large Electricity Utility
M. Lang and A.J. Walker

Design and Implementation of a C++ Package for Two-Dimensional Numerical Integration
D.P. Laurie, L Pluym and Ronald Cools

Algebraic Factorization of Integers Using BDE’s
H. Messerschmidt and J. Robertson
Global Optimization of Routes after the Process of Recovery
M. Mphahlele and J. Roos

Using a Lattice to Enhance Adaptation Guided Retrieval in Example Based Machine Translation
G.D. Oosthuizen and S.L. Serutla

Information Systems Development and Multi Criteria Decision Making / Systems Thinking
D. Petkov, O. Petkova

The Development of a Tutoring System to Assist Students to Develop Answering Techniques
N. Pillay

Combining Rule-Based Artificial Intelligence with Geographic Information Systems to Plan the Physical Layer of Wireless Networks in Greenfield Areas
K. Prag, P. Premjeeth and K. Sandrasegaran

A Distributed Approach to the Scheduling Problem
V. Ram and P. Warren

More readings than I thought: Quantifier Interaction in Analysing the Temporal Structure of Repeated Eventualities
S. Rock

Ray Guarding Configuration of Adjacent Rectangles
I. Sanders, D. Lubinsky and M. Sears

Developing Soft Skills in Computer Students
C. Schröder, T. Thomas

Information Security Awareness, a Must for Every Organization
M. Thomson and R. von Solms

Pla Va: A Lightweight Persistent Java Virtual Machine
S. Tjasink and S. Berman

Beliefs on Resource-Bounded Agent
E. Viljoen

Object-Orientated Business Modelling and Re-engineering
M. Watzenboeck
On Indexing in Case Based Reasoning Applied to Pre-Transportation Decision Making for Hazardous Waste Handling
K.L. Wortmann, D. Petkov and E Senior

Author Index
List of Contributors

S.A. Ajila
Department of Mathematics and Computer Science
National University of Lesotho
Roma, 180
Lesotho

L. Baart
Department of Mathematics
Vaal Triangle Campus of the PU for CHE
PO Box 1174
Vanderbijlpark, 1900

L. Barnard
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

S. Berman
University of Cape Town
Rondebosch, 7701

L. Bester
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

J.M. Bishop
Computer Science Department
University of Pretoria
Pretoria, 0002

L. Botha
Computer Science Department
University of Pretoria
Pretoria, 0002

R.A. Botha
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

B. Braude
Software Engineering Applications Laboratory,
Electrical Engineering
University of the Witwatersrand
Private Bag 3
Wits, 2050

T. Breetzke
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

C. Brink
University of Cape Town
Rondebosch, 7700

M. Bruynooghe
Departement Computerwetenschappen
Katholieke Universiteit Leuven
Celestijnenlaan 200A
B-3001 Heverlee
Belgium

S. Buffler
University of Capetown
Rondebosch, 7701

M.A. Coetzee
Department of Mathematics
PU for CHE
Private Bag X6001
Potchefstroom, 2520

R. Cools
Katholieke Universiteit Leuven
Celestijnenlaan 200A
B-3001 Heverlee
Belgium

E. de Preez
Faculty of Computer Studies
Port Elizabeth Technikon
Private Bag X6011
Port Elizabeth, 6000

D.A. De Waal
Department of Computer Science and Information Systems
PU for CHE
Private Bag X6001
Potchefstroom, 2531

B. Dekenenah
The Board of Executors

M. Denecker
Departement Computerwetenschappen
Katholieke Universiteit Leuven
Celestijnenlaan 200A
B-3001 Heverlee
Belgium

M. Dunley-Owen
Department of Information Systems
University of Cape Town
Rondebosch, 7700

R. Fiqueira
University of Cape Town
Rondebosch, 7701

A. Foster
Department of Computer Science
University of Cape Town
Rondebosch, 7701

C. Gee
Software Engineering Applications Laboratory,
Electrical Engineering
University of the Witwatersrand
Private Bag 3
Wits 2050
K. Sandrasegaran  
Department of electrical Engineering  
University of Durban-Westville  
Private Bag X54001  
Durban, 4000

C. Schoder  
Faculty of Computer Studies  
Port Elizabeth Technikon  
Private Bag X6011  
Port Elizabeth, 6000

M. Sears  
Department of Mathematics  
University of the Witwatersrand  
Private Bag 3  
Wits, 2050

E. Senior  
International Center for Waste Technology  
University of Natal, Pietermaritzburg  
Private Bag X01  
Scotsville, 3209

N.B. Serbedzija  
GMD FIRST  
Rudower Chausee 5  
D-12489 Berlin  
Germany

S.L. Serutla  
Department of Computer Science  
The University of Pretoria  
Pretoria, 0002

T. Steyn  
PU for CHE  
Private Bag X6001  
Potchefstroom, 2520

M. Thielscher  
Fachgebiet Informatik, Fachgebiet Informatik  
Technische Hochschule Darmstadt  
Alexanderstrasse 10  
D-64283 Darmstadt  
Germany

T. Thomas  
Faculty of Computer Studies  
Port Elizabeth Technikon  
Private Bag X6011  
Port Elizabeth, 6000

M. Thomsen  
Faculty of Computer Studies  
Port Elizabeth Technikon  
Private Bag X6011  
Port Elizabeth, 6000

S. Tjasink  
University of Cape Town  
Rondebosch, 7700

E. Viljoen  
Department of Computer Science and  
Information Systems  
University of South Africa  
PO Box 302  
Pretoria, 0001

E. Voges  
University of Cape Town  
Rondebosch, 7701

R. Von Solms  
Faculty of Computer Studies  
Port Elizabeth Technikon  
Private Bag X6011  
Port Elizabeth, 6000

A.J. Walker  
Software Engineering Applications Laboratory,  
Electrical Engineering  
University of the Witwatersrand  
Private Bag 3  
Wits, 2050

P. Warren  
Department of Computer Science  
University of Natal  
Private Bag X01  
Scotsville, 3209

M. Watzenboeck  
University of Botswana  
Private Bag 0022  
Gaborone  
Botswana

K.L. Wortmann  
Department of Computer Science  
University of Natal, Pietermaritzburg  
Private Bag X01  
Scotsville, 3209
Algebraic Factorization of integers using BDE's

H. J. Messerschmidt and J. Robertson
Department of Computer Science and Informatics
University of the Orange Free State
Bloemfontein 9301
South Africa

Email: hans@wwg3.uovs.ac.za

Abstract

This paper outlines a new direct algebraic method for the factorization of integers. It shows how by using a mixed binary-decimal multiplication scheme the multiplication can be reconstructed from the product only. This reconstruction process leads to a set of Diophantine equations in binary variables (BDE's) that have one or both factors as roots.

A programmatic implementation of the algorithm is also discussed.

MR Classification: primary 11A51; secondary 11D72

1. Introduction

From the time of Euclid and Erastostenes man has been fascinated by factorization. More and more algorithms were developed, but factorization has remained a difficult task, so much so that some modern cryptography algorithms rely on the fact that it is practically impossible to factor an integer of 200 or more decimal digits.

Almost all the known algorithms are numeric in nature and use repeated trials to
factor an integer. In trial division one tries division by successive small primes, in
Fermat's methods one tries to write the number to be factored as the difference of
two squares and in Gauss' method one tries to eliminate possible factors by finding
quadratic residues. (Riesel, 1985)

In this paper a more direct method is presented using algebra and Diophantine
Equations in Binary Variables (or BDE's for short).

2. The multiplication process

In order to understand factorization, it is instructive to see how a composite number
is formed during the multiplication of two integers:

\[
\begin{array}{c}
43 \\
x \times 193 \\
\hline \\
387 \\
43 \\
\hline \\
8299
\end{array}
\]

The information on how the product 8299 was arrived at has been discarded. In the
decimal system this information is very difficult to reconstruct. The highlighted 9 in
the intermediate calculation could have been obtained in 4 different ways. The
highlighted 8 has no direct connection to 9 x 4 since the 2 carried from 9 x 3 has
obscured the 6.

In the binary number system things are much simpler. The binary multiplication
table shows

\[
\begin{array}{c|c|c}
\times & 0 & 1 \\
\hline \\
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}
\]

that there is never any multiplicative carry and that 1 can only result from 1 x 1.
Further more if that observation is extended to algebra, it means that if x is a binary
variable \( x = x^2 = x^3 \) etc.

3. A mixed mode multiplication scheme

If a composite odd number \( Z \) (even numbers can be disregarded for factorization without loss of generality) consists of \( \text{NoZ} \) binary digits, it must have at least two factors \( X \) and \( Y \) such that \( X \geq Y > 1 \). Since \( Z \) is odd the larger factor \( X \) can at most have \( \text{NoX} = \text{NoZ} - 1 \) binary digits and the smaller factor \( Y \) at most \( \text{NoY} = (\text{NoZ} + 1) / 2 \) binary digits. (where / represents integer division).

Taking \( 7 \times 13 = 91 = 1011011_2 \) as an example \( \text{NoZ} = 7, \text{NoX} = 6 \) and \( \text{NoY} = 4 \). This gives rise to the following mixed (binary and decimal) mode multiplication scheme:

\[
\begin{array}{cccccccc}
0 & 0 & 1 & 1 & 0 & 1 & X \\
\times & 0 & 1 & 1 & 1 & Y \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & C(arry) \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & \text{XY}_0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & \text{XY}_1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & \text{XY}_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \text{XY}_3 \\
0 & 0 & 1 & 2 & 3 & 3 & 2 & 1 & 1 & \text{T(otal)} \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \text{Z} \\
\end{array}
\]

The variables \( X, Y \) and \( Z \) are binary variables while \( C \) and \( T \) are decimal. The number of columns in the scheme is \( \text{NoC} = \text{NoX} + \text{NoY} - 1 \). The column subscripts count from 0 and from right to left. The \( T_i \) represent the total of the column while the \( C_i \) represent the carry from the previous column.

For factorization the question is if the scheme can be reconstructed given \( Z \) only. Surprisingly the answer is yes. There are a few observations that point the way. Obviously the \( C_i \) are related to the \( T_i \) by \( T_i = 2C_i + Z_i \). The \( Z_i \) determine the parity of the \( T_i \): \( C_0 = 0, T_{\text{NoZ}-1} = 1 \) and both \( C_{\text{NoZ}..\text{NoC}-1} \) and \( T_{\text{NoZ}..\text{NoC}-1} \) are 0. The \( \text{XY}_i \) rows are either all 0 or have the same bit pattern as \( X \).
4. The reconstruction process

The reconstruction process depends on the following two equations:

\[ T_i = C_i + \text{Sum}(X_jY_{j+1}) \quad \text{where } j \text{ goes from } 0 \text{ to } i \text{ and as long as the variables exist} \]

\[ T_i = 2C_{i+1} + Z_i \]

and the facts that the \( Z_i \) determine the parity of the \( T_i \) and that \( X_i \) is a binary variable.

4.1 Step 0

\[ C_0 = 0 \]

\[ T_0 = C_0 + X_0Y_0 = X_0Y_0 \]

\[ T_0 = 2C_1 + Z_0 = 2C_1 + 1 \]

but \( X_0Y_0 \) can only be 0 or 1 therefore \( X_0Y_0 = 1; X_0 = 1 \ Y_0 = 1 \ T_0 = 1 \ C_1 = 0 \)

4.2 Step 1

\[ T_1 = C_1 + X_0Y_1 + X_1Y_0 = Y_1 + X_1 \]

\[ T_1 = 2C_2 + Z_1 = 2C_2 + 1 \]

\( T_1 \) must be odd; therefore \( X_1 = 1 - Y_1; T_1 = 1 \) and \( C_2 = 0 \)

4.3 Step 2

\[ T_2 = C_2 + X_0Y_2 + X_1Y_1 + X_2Y_0 = Y_2 + X_2 \]

\[ T_2 = 2C_3 + Z_2 = 2C_3 \]

but \( T_2 \) is even; therefore \( X_2 = Y_2 \ T_2 = 2Y_2 \) and \( C_3 = Y_2 \)

4.4 Step 3

\[ T_3 = C_3 + X_0Y_3 + X_1Y_2 + X_2Y_1 + X_3Y_0 = Y_2 + Y_3 + Y_2 - Y_1Y_2 + Y_1Y_2 + X_3 \]

\[ T_3 = 2C_4 + Z_3 = 2C_4 + 1 \]

\( T_3 \) is odd; therefore \( X_3 = 1 - Y_3 \ T_3 = 2Y_2 + 1 \) and \( C_4 = Y_2 \)
4.5 Step 4

\[ T_4 = C_4 + X_1Y_3 + X_2Y_2 + X_3Y_1 + X_4Y_0 \]

\[ = Y_2 + Y_3 - Y_1Y_3 + Y_2 + Y_1 - Y_1Y_3 + X_4 \]

\[ = 2Y_2 - 2Y_1Y_3 + Y_1 + Y_3 + X_4 \]

while \( T_4 \) is odd, we cannot make \( X_4 = 1 - Y_1 - Y_3 \) for if both \( Y_1 \) and \( Y_3 \) were to be 1, \( X_4 \) would become -1 which is impossible. A correction term needs to be added, making \( X_4 = 1 - Y_1 - Y_3 + 2Y_1Y_3 \). This makes \( T_2 = 2Y_2 + 1 \) and \( C_5 = Y_2 \)

4.6 Step 5

\[ T_5 = C_5 + X_2Y_3 + X_3Y_2 + X_4Y_1 + X_5Y_0 \]

\[ = Y_2 + Y_2Y_3 + Y_2 - Y_2Y_3 + Y_1 - Y_1Y_3 + 2Y_1Y_2 + X_5 \]

\[ = 2Y_2 + Y_1Y_3 + X_5 \]

with \( T_5 \) even this gives \( X_5 = Y_1Y_3 \) \( T_5 = 2Y_2 + 2Y_1Y_3 \) and \( C_6 = Y_2 + Y_1Y_3 \).

4.7 Step 6

\[ T_6 = C_6 + X_3Y_3 + X_4Y_2 + X_5Y_1 \]

\[ = Y_2 + Y_1Y_3 + Y_2 - Y_2Y_3 + 2Y_1Y_2Y_3 + Y_1Y_3 \]

\[ = 2Y_2 + 2Y_1Y_3 + Y_2Y_3 + 2Y_1Y_2Y_3 \]

this gives the first of the 3 BDE's

4.8 Step 7

\[ T_7 = C_7 + X_4Y_3 + X_5Y_2 \]

\[ = Y_3 - Y_1Y_3 - Y_3 + 2Y_1Y_3 + Y_1Y_2Y_3 \]

\[ = Y_1Y_3 + Y_1Y_2Y_3 \]

this is the 2\textsuperscript{nd} BDE.

4.9 Step 8

\[ T_8 = C_8 + X_5Y_3 \]

\[ = Y_1Y_3 \]

this is the 3\textsuperscript{rd} BDE.
4.10 Step 9

Solving the BDE's. Substituting the 3rd BDE into the second followed by substituting the result into the first BDE gives:

\[ 1 = 2Y_2 - Y_1 Y_2 - Y_2 Y_3 \]

which has two solutions corresponding to the factors of 91.

5. The correction factor

The correction factor complicates an otherwise very simple algorithm. Can the correction factor be ignored? Since the X_i are binary variables, knowing the parity is enough. Unfortunately the C_i are decimal variables and they are affected by the X_i values. Using the proposed method on 221 for example and ignoring the correction factors quickly leads to erroneous answers.

How should the correction factor be formulated? The correction factor insures that X_i stays in the range \((0, 1)\) if more than one Y_i is 1. If only two factors are involved, inspection shows that \(Y_i + Y_j - 2Y_i Y_j\) does the trick. If three factors are involved \(Y_i + Y_j + Y_k - 2Y_i Y_j - 2Y_i Y_k - 2Y_j Y_k\) overcompensates by 4 if all three \(Y_i, Y_j\) and \(Y_k\) are one. A term \(+4Y_i Y_j Y_k\) needs to be added. Fortunately there is an easy formula to generate the correct polynomial. Our first attempt did this recursively and while it worked the overhead became too much. A simple iterative process was discovered to overcome the problem. It turns out that \(...(((Y_i - Y_j)^2 - Y_k)^2 - Y_l)^2 \ldots\) does the trick.

6. Acceleration for Fermat numbers

Since the proposed method reconstructs the factors digit by digit any additional knowledge about the factors can often be used to speed up the process. If it known for example (say by trial division) that the smallest factor is larger than \(N\), then the number of X-digits (and thereby the number of equations to be constructed) can be reduced to \(\text{NoX} = \text{NoZ} - \text{floor}(\log_2 N)\).

For Fermat numbers it is known that all factors of \(F_n\) are of the form \(a \cdot 2^{n+2} + 1\). This means that the first \(n+2\) \(X\) and \(Y\) are known and that the maximum number of \(X\)
digits can be reduced by n+2.

7. Programming considerations

We implemented the algorithm in C++. Since the variables of the equations are all binary variables we use a bit vector to indicate the absence or presence of variable i.e. 000101001 means Y₃Y₅Y₆. The coefficients are kept as long integers. Multiplication multiplies the coefficients and OR's the variable term. Addition checks for identical variable terms and then adds the coefficients. We developed classes for BitVec, Term and Poly. By making them persistent we can restart a factorization after each X equation.

8. Conclusion

The example shows that by using mixed binary mode multiplication and BDE's factorization can be accomplished algebraically without resorting to trials. The above process becomes too cumbersome to do by hand for any worthwhile size integer. The algorithm is not particularly difficult, but does contain a few traps for the unwary.

References

Riesel, H. (1985)
Prime Numbers and Computer Methods for Factorization
Birkhäuser, Boston.