University of California

Los Angeles

Trustworthy Tools for Trustworthy Programs: A Mechanically Verified Verification Condition Generator for the Total Correctness of Procedures

A dissertation submitted in partial satisfaction

of the requirements for the degree

Doctor of Philosophy in Computer Science

by

Peter Vincent Homeier

1995

The dissertation of Peter Vincent Homeier is approved.

Rajive Bagrodia

Donald A. Martin

D. Stott Parker

David F. Martin, Committee Chair

University of California, Los Angeles

1995

I dedicate this dissertation

to the most wonderful friend I have ever had,

my Messiah, Lord, and Savior, the Son of God,

Y'shua Ha Mashiach, Jesus the Christ.

He has cared for every need faithfully,

in the midst of earthquake and opposition.

He has wholeheartedly poured out His Holy Spirit on me.

At each point of difficulty, at each resistant problem,

like a cool drop of rain, He quietly dropped the answer into me.

When the ultimate impossible cliff arose before me,

He opened doors of understanding,

drawing me beyond what I thought was the end,

through the darkness of the grave

to the dawn of a new morning.

He has been the lifter of my head, and the restorer of my hopes.

Of all the people I know,

He is the most precious to me.

He loved me enough to humbly go to the Cross and die in my place.

I can never repay such a pure and shattering gift.

This dissertation is only the smallest of ways

I can express my heart's wonder and love

for such a greater love He has lavished on me.

Table of Contents

List of Figures

List of Tables

Acknowledgments

My earnest thanks go to Professors Rajive Bagrodia, Donald A. Martin, D. Stott Parker, and my advisor, David F. Martin, for serving on my committee.

I am grateful to The Aerospace Corporation for supporting my education with a fellowship for several years through most of my graduate studies.

Ching-Tsun Chou read early drafts of this manuscript and provided many helpful comments and suggestions. We have faced the heat of the battle together, and I have enormous respect for his intellect. I am grateful to Raymond Toal for his cheerful inspiration and solid example.

I thank my wonderful father and stepmother, Skip and Della Homeier, for too much to say, but especially for their encouragement to return to school and pursue the Ph.D. Their words sparked the desire of my heart to become a manifest reality, and have profoundly sharpened my life as a sword on the anvil.

Pastor Jim Nelson at The Church on the Way has given me consistent and faithful support over the years. From the beginning of this quest, with insight and devotion he has tenaciously watched over me, and I shall always be grateful for his protective care. I also want to thank Pastor Chip Graves, for praying and encouraging me when I needed to choose between my job and my degree.

Pastor Jack Hayford has been a staff and a covering for me. His wisdom and simple sincerity of heart have been a living model, blending biblical brilliance with tender faith and honest humility. He has an uncanny ability to speak to the heart of a situation, inevitably displaying the perspective of heaven. He has

focused me on the essentials, on integrity of heart, passion for fullness, and fierceness of commitment, as an elite trained soldier. (Isaiah 28:5-6, Zechariah 6:11, 1 Peter 5:4) The little boy who was healed from falling down is now teaching us all to go "leaping upon the mountains, skipping upon the hills." My respect and love for him know no bounds.

Verra Morgan is a shining angel, clucking like a mother hen. Her fierce, eager, combative spirit is always ready like a growling mother bear to defend her cubs, and then to cuff them when they misbehave. She has saved my neck administratively more times than I can count. I honestly do not know if I would have completed my degree if in the accident she had been taken from us. My heart overflows with thanks she was not. Verra has always lived for the success of the graduate students in her care. May she someday find a joy even greater.

Susan has been a gift beyond expectations, knitting raveled edges. She has shown me a mother's love, faith, and encouragement in the secret depths, with wisdom that few have ever seen. "For the Spirit searches all things, yes, the deep things of God. For what man knows the things of a man except the spirit of the man which is in him?" (1 Corinthians 2:10–11) She has eyes for the light in the heart of the dark, and a rod of healing held over troubled waters. My deep thanks go to her for our many rich words and woven times.

My special heartfelt appreciation goes to my advisor, Professor David F. Martin, for his supervision of this research. He has been a guiding light, an inspiration, a constant source of encouragement and approval, and the warmest of friends. He has truly been "the advisor from Heaven," in every way going beyond all that I ever conceived or could have asked for. I want to always give the same consci-

entious and diligent care he has given me. Through this long walk together, he has become a father to me, cherished beyond words. May his brilliance and his heart be recognized and rewarded.

My highest gratitude goes to someone not seen on Earth, who spun the galaxies with His fingertips, and blew the stars aflame. It was He who gave me the strength to leap each wall. Indeed every good and perfect gift comes down from above, from the Father of Lights. When opposition arose demanding I stop, He provided the way to continue and grow. When I was at the end of myself, with all my hopes at risk, He reached down and kept me from sliding into the pit, and placed my feet on a rock. He who said, "Let there be light," has shone in my heart. (2 Corinthians 4:6) All of this dissertation is only here by His hand extended in grace and peace.

Soli Deo Gloria.

Vita

1956	Born, Santa Monica, California, USA
1979	B.S. in Mathematics/Computer Science Summa Cum Laude Mathematics/Computer Science Senior Prize University of California, Los Angeles (UCLA) Los Angeles, California, USA
1979	Regents Fellowship University of California, Los Angeles (UCLA) Los Angeles, California, USA
1981	M.S. in Computer Science University of California, Los Angeles (UCLA) Los Angeles, California, USA
1981–1983	Member of the Technical Staff Hughes Aircraft Corporation El Segundo, California, USA
1983–1995	Member of the Technical Staff The Aerospace Corporation El Segundo, California, USA

1988–1994 Aerospace Graduate Fellowship
The Aerospace Corporation
El Segundo, California, USA

Publications

Peter V. Homeier and David F. Martin, "A Mechanically Verified Verification Condition Generator," *The Computer Journal*, Vol. 38, No. 2, 1995, pages 131–141.

Peter V. Homeier and David F. Martin, "Trustworthy Tools for Trustworthy Programs: A Verified Verification Condition Generator," in *Proceedings of the 7th International Workshop on Higher Order Logic Theorem Proving and its Applications*, eds. Thomas F. Melham and Juanito Camilleri, Valletta, Malta, September 19–22, 1994, Lecture Notes in Computer Science Vol. 859, Springer–Verlag, pages 269–284.

Peter V. Homeier, Thach C. Le, Y. Peter Li, and Peter C. Eggan, "DEF–CLIPS: Extensions to the CLIPS Production System Environment," in *Proceedings of Artificial Intelligence/Expert Systems Symposium*, El Segundo, CA, September 1–2, 1993.

Peter V. Homeier and Thach C. Le, "ECLIPS: An Extended CLIPS for Backward

Chaining and Goal-Directed Reasoning," in *Proceedings of the Second CLIPS Users Group Conference*, September 23–25, 1991, Houston, Texas, NASA Conference Publication 10085, Volume 2, pages 213–225.

Thach C. Le and Peter V. Homeier, "PORTABLE INFERENCE ENGINE: An Extended CLIPS for Real-Time Production Systems," in *Proceedings of the Second Annual Workshop on Space Operations Automation and Robotics*, (SOAR '88), July 20–23, 1988, NASA Conference Publication 3019, pages 187–192.

Abstract of the Dissertation

Trustworthy Tools for Trustworthy Programs: A Mechanically Verified Verification Condition Generator for the Total Correctness of Procedures

by

Peter Vincent Homeier

Doctor of Philosophy in Computer Science

University of California, Los Angeles, 1995

Professor David F. Martin, Chair

As an alternative to testing, formal proofs of a program's correctness may be constructed. The application of these techniques has been limited by the difficulty of constructing the required proofs by hand. The task of proving a program correct can be simplified and eased by a tool called a *Verification Condition Generator* (VCG), which automatically constructs a significant portion of the proof. The VCG processes programs written in the specified language, and produces as its result a set of lemmas called *verification conditions*, as the remainder left for the programmer to prove. The truth of these is intended to imply the correctness of the program. However, most VCGs that have been written have not themselves been verified, making that support unreliable.

We have written a VCG and verified its soundness, proving that if the verification conditions produced are true, then the original program is totally correct. This proof is conducted within and checked by the Higher Order Logic (HOL) mechanical proof checker, ensuring its complete soundness. The resulting verified VCG provides an effective means for proving programs totally correct with complete security.

The programming language studied contains two areas of special interest, expressions with side effects, and mutually recursive procedures, with global variables and variable and value parameters. As part of this work, we provide five program logics which together provide an axiomatic semantics for total correctness. Of the five program logics, three are fundamental inventions in this dissertation. These new logics are used to verify the correctness of expressions, the progress achieved between recursive calls of the same procedure, and the termination of procedures. All of these logics are mechanically proven within the HOL system to be sound with respect to the formal semantics of the language.

The most novel contribution of this dissertation is the discovery of a new method for proving the termination of programs with mutually recursive procedures, which is both more general and easier to use than prior proposals. In addition, VCG automation is naturally supported. This method analyzes the structure of the procedure call graph, generating verification conditions based on the cycles found.