AN IMPLEMENTATION OF SECURE FLOW TYPE INFERENCE FOR A SUBSET OF JAVA

Ismail Okan Akdemir-Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 1992
Master of Science in Computer Science-September 1998
Advisor: Dennis Volpano, Department of Computer Science
Second Reader: Craig Rasmussen, Department of Mathematics

Smart cards play an important role in a digital society. A smart card contains memory or an embedded microprocessor with the capability of enabling a wide variety of services, such as electronic cash in the case of memory cards and digital signature computation in the case of processor cards. A processor card can require a cardholder to authenticate herself in order to prevent others from using the card's services, from forging the cardholder's signature, for example. Authentication can be done by storing a personal identification number (PIN) or digitized fingerprint of the cardholder on the card itself. The PIN or fingerprint must always remain confidential no matter how the card is (ab)used.

This thesis addresses the problem of preserving the privacy of information stored on smart cards. Volpano and Smith have developed a static analysis for analyzing source code for information flow violations. This technique is developed further here for a language called Java Card, in which smart card applications are written. A prototype analyzer is presented for a subset of Java Card and applied to a sample card application to demonstrate its utility in protecting private information stored on smart cards.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Other (Smart Cards, Software Security, Type System)

KEYWORDS: Java Card, Smart Cards, Secure Flow Analysis, Type System

ON THE QUASIMONOTONICITY OF A SQUARE LINEAR OPERATOR WITH RESPECT TO A NONNEGATIVE CONE

Philip Beaver-Major, United States Army
B.S., United States Military Academy, 1983
M.S., Naval Postgraduate School, 1991
Doctor of Philosophy in Applied Mathematics-June 1998
Advisor: David Canright, Department of Mathematics
Committee: Christopher L. Frenzen, Department of Mathematics
Robert F. Dell, Department of Operations Research
Clyde L. Scandrett, Department of Mathematics
Maurice D. Weir, Department of Mathematics

The question of when a square, linear operator is quasimonotone nondecreasing with respect to a nonnegative cone was posed for the application of vector Lyapunov functions in 1974. Necessary conditions were given in 1980, which were based on the spectrum and the first eigenvector. This dissertation gives necessary and sufficient conditions for the case of the real spectrum when the first eigenvector is in the nonnegative orthant, and when the first eigenvector is in the boundary of the nonnegative orthant, it gives conditions based on the reducibility of the matrix. For the complex spectrum, in the presence of a positive first eigenvector the problem is shown to be equivalent to the irreducible nonnegative inverse eigenvalue problem.

DoD KEY TECHNOLOGY AREA: Other (Applied Mathematics)

KEYWORDS: Quasimonotonicity, Nonnegative Cone

THE UTILITY OF THE ADVANCED SEAL DELIVERY SYSTEM (ASDS) (U)

David E. Chelsea-Lieutenant Commander, United States Navy
B.S., University of California at San Diego, 1987
Master of Science in Defense Analysis-June 1998
Master of Science in Management-June 1998
Advisors: Gordon H. McCormick, Special Operations /Low Intensity Conflict Curriculum Committee
Bard Mansager, Department of Mathematics

The United States Special Operations Command (USSOCOM) is in the process of procuring the Advanced SEAL Delivery System (ASDS), a mini-submersible, to be used by Naval Special Warfare (NSW) forces to conduct maritime special operations. During the development of the ASDS, costs have more than doubled. Consequently, USSOCOM is reevaluating the future of ASDS. This thesis assesses the utility of the ASDS by viewing the ASDS as a part of an "infiltration system" and analyzing the linkages and fit of ASDS within the strategic framework in which it is intended to operate. Modeling the primary factors that define ASDS as a viable special operations platform in high, medium, and low threat environments does this. The output of the model is the capability of ASDS expressed in terms of "mission success." The estimated annual cost of ASDS is also calculated using the current acquisition strategy. In order to compare against current capabilities and their respective costs, this process is repeated for four alternative NSW infiltration systems. Although the ASDS has the highest cost, it is the only system that presents an acceptable probability of mission success in high and medium threat environments. Given NSW's strategic framework, the ASDS has a high utility.

DoD KEY TECHNOLOGY AREAS: Surface/Undersurface Vehicles-Ships and Watercraft, Modeling and Simulation

KEYWORDS: Advanced SEAL Delivery System, Mini-Submersible, ASDS, NSW, USSOCOM, Mission Success

MATRIX ALGEBRA

Anthony R. Delatorre-Lieutenant, United States Navy
B.S., University of Arizona, 1991
Master of Science in Applied Mathematics-June 1998
and
William K. Cooke-Lieutenant, United States Navy
B.E.E., Georgia Institute of Technology, 1989
Master of Science in Applied Mathematics-June 1998
Advisors: Carlos F. Borges, Department of Mathematics
Craig W. Rasmussen, Department of Mathematics

This thesis is designed to act as an instructor's supplement for the Naval Postgraduate School's (NPS) refresher matrix algebra courses. The need for a beginning matrix algebra supplement is driven by the unique circumstances that a majority of NPS students find themselves. Most military students attend NPS several years after receiving their undergraduate degrees. This supplement, unlike most college textbooks, bridges the gap between the student's educational lay-off and the rigors of mathematically oriented degrees such as applied math, operations research and engineering. By reviewing the fundamental concepts of vectors and matrices, and computationally performing operations on them, the student quickly develops the requisite knowledge to succeed in NPS' demanding curriculums. This supplement focuses on matrix and vector operations, linear transformations, systems of linear equations, and the techniques required to computationally solve systems of linear equations. The goal of this thesis is to enhance current textbooks and help the beginning student in matrix algebra in order to build a foundation for higher level engineering and mathematics based courses.

DoD KEY TECHNOLOGY AREA: Other (Matrix Algebra Supplement)

KEYWORDS: Matrix Algebra

CHANNEL ALLOCATION IN WIRELESS INTEGRATED SERVICES
FUEL-OPTIMAL LOW-EARTH-ORBIT MAINTENANCE
Karl E. Jensen, Lieutenant United States Navy
B.S. in Aerospace Engineering, United States Naval Academy, 1990
Master of Science in Astronautical Engineering-June 1998
Aeronautical and Astronautical Engineer, Naval Postgraduate School-June 1998
Advisors: I. Michael Ross, Department of Aeronautics and Astronautics
Fariba Fahroo, Department of Mathematics

First-order solutions indicate that a forced Keplerian trajectoiy (FKT) obtained by thrust-drag cancellation is as fuel-efficient as a Hohmann transfer. Further analysis has shown that the FKT is not Mayer-optimal. Therefore, there must exist another trajectory that matches or exceeds the efficiency of the Hohmann transfer. The application of this result to the fuel-optimal orbit maintenance problem implies that periodic reboosts must be more efficient than an FKT profile. This research begins with the formulation of an optimal periodic control (OPC) problem to determine the minimum fuel-reboost strategy. The problem is numerically solved by a spectral collocation method. The optimization code is further modified to increase accuracy and reduce sensitivity to initial guesses. The results of this effort identified a trajectory for a sample satellite that was 3.5% more efficient than an ideal impulsive Hohmann transfer over the same period of time. From the optimal code, a maximum thruster size is also identifiable for a set of initial conditions. The optimal trajectory can save as much as 10% of the propellant budget when compared to finite-bum Hohmann transfers.

DoD KEY TECHNOLOGY AREAS: Aerospace Propulsion and Power, Space Vehicles, Modeling and Simulation

KEYWORDS: Orbital Maintenance, Orbital Mechanics, Hohmann Transfer, Orbit Reboost, Orbit Transfer, Forced Keplerian Trajectory, Optimization, Periodic Control

IDENTIFICATION OF RANDOM LOADS IMPINGING ON THE RAH-66
COMANCHE HELICOPTER EMPENNAGE USING SPECTRAL ANALYSIS
Patrick H. Mason-Major, United States Army
B.S., Georgia Institute of Technology, 1986
Master of Science in Aeronautical Engineering-June 1998
Advisors: E. Roberts Wood, Department of Aeronautics and Astronautics
Donald A. Danielson, Department of Mathematics
Joshua H. Gordis, Department of Mechanical Engineering

The Army RAH-66 Comanche Helicopter is currently undergoing developmental flight testing. The empennage of the aircraft is experiencing buffeting where the horizontal and vertical tail vibrate at resonant frequencies. These high buffet loads are manifested in higher than anticipated fitting loads, particularly on the tail, and vibrations in the crew stations and at the nose cone where the targeting sensors are located. Significant effort has been devoted to identifying the sources of excitation and the nature of the structural response. This thesis determines the location and magnitude of empennage vibratory airloads. Because the nature of the excitation is a random function, spectral analysis is used. To obtain the loads, a three-step process was utilized. First, from aircraft differential pressure transducers and accelerometers, the spectral content of the response and excitation was determined Then, using a NASTRAN model modified to replicate the flight test aircraft, frequency response functions were determined between selected points on the aircraft's tail and the accelerometers. Finally, using this information, a solution was obtained for the vibratory airloads. Having provided information on the nature of the driving forces, structural modifications can be made that move the natural frequencies away from the frequencies of the applied airloads.

DoD KEY TECHNOLOGY AREA: Air Vehicles

KEYWORDS: RAH-66 Comanche Helicopter, Random Vibrations, Comanche Tail Section, Structural Analysis, Spectral Analysis, NASTRAN Analysis

AN EXAMINATION OF BI-ORTHOGONALITY RELATIONSHIPS IN ELASTIC-FLUID MEDIA

Coley R. Myers, III-Lieutenant, United States Navy
B.S., North Carolina State University, 1992
Master of Science in Applied Mathematics-June 1998
Advisors: Clyde L. Scandrett, Department of Mathematics
Christopher L. Frenzen, Department of Mathematics

The bi-orthogonality relationships for vertically heterogeneous porous media in contact with various surfaces have been previously established. For the special case in which the porous substance has zero porosity, the relationships reduce to those for elastic media. The biorthogonality relationship for a fluid loaded elastic slab will be considered numerically by discritizing the boundary value problems using finite differences. The resulting matrix will be analyzed for the purpose of determining eigenvalues of the complex dispersion relationship of the layered media, as well as discerning the corresponding eigenvectors which are discrete analogies of the propagation/evanescent eigenfunctions of the media.

DoD KEY TECHNOLOGY AREA: Other (Acoustics, Mathematics)

KEYWORDS: Acoustics, Bi-orthogonality, Elasticity

AN EXPERIMENTAL INVESTIGATION OF VORTEX BREAKDOWN IN TUBES AT HIGH REYNOLDS NUMBERS

Francis G. Novak-Lieutenant Commander, United States Navy
B.S., United States Naval Academy, 1985
M.S., Naval Postgraduate School, 1992
M.E., Naval Postgraduate School, 1992
Doctor of Philosophy in Mechanical Engineering-September 1998
Advisor: T. Sarpkaya, Department of Mechanical Engineering
Committee: Matthew Kelleher, Department of Mechanical Engineering
F. Kevin Owen, Department of Mechanical Engineering
David Netzer, Department of Aeronautics and Astronautics
Richard Franke, Department of Mathematics

This thesis deals with non-cavitating swirling flows with vortex breakdown in various tubes. Phenomenological and quantitative investigations were carried out at Reynolds numbers ($Re_D = U_0D_0/n$) as high as 300,000. It was shown that a high Re_D vortex transitions to its new state (breaks down) via a rapidly spinning spiral form, as demonstrated with 4,000 frame per second video, short exposure time (6 ns) imaging, and Digital Particle Image Velocimetry. Of the known types, the spiral emerges as the fundamental breakdown form, and the axisymmetric bubble may now be regarded as a relatively low Re_D occurrence that is bypassed at sufficiently high Re_D. Some new phenomena were observed at high Re_D: Extremely rapid spiral rotation (over 1,000 revolutions per second), core bifurcation, and reversals in the sense of the spiral windings. Familiar features of breakdowns, such as the transition from jet-like to wake-like axial velocity profiles and the rapidly expanding vortex core, were observed in extensive time averaged velocity and turbulence profiles ascertained with Laser Doppler Velocimetry. However, a mean stagnation point and recirculation were absent in the highest Re_D flow. The core meandering and stagnation point darting in the turbulent flow field were quantified and discussed in detail.

DoD KEY TECHNOLOGY AREA: Air Vehicles

KEYWORDS: Vortex Breakdown, Turbulence, Laser Doppler Velocimetry, Particle Image Velocimetry, Swirling Flow, Spectra

BIZIER CURVE FITTING
Tim A. Pastva-Major, United States Marine Corps
B.S., University of Michigan, 1986
Master of Science in Applied Mathematics-September 1998
Advisor: Carlos F. Borges, Department of Mathematics
Second Reader: Richard Franke, Department of Mathematics

We typically think of fitting data with an approximating curve in the linear least squares sense, where the sum of the residuals in the vertical, or *y*, direction is minimized. The problem addressed here is to fit a BJzier curve to an ordered set of data in the total least squares sense, where the sum of the residuals in both the horizontal and vertical directions is minimized. More exact: given an ordered set of *m* data points d_i, *i*'1,2,ˇ,*m* find a set of control points b_i, *i*'0,1,ˇ,*n* where *n* is the order of the BJzier curve, and a vector t of nodes, $0 \# t_1 \# t_2 \# \text{˛} \# t_m \# 1$ that minimize $\| B(t)P - D \|_F$. The matrix *D* contains the data points, the matrix *P* contains the control points, and the matrix *B*(t) is a Bernstein matrix. The algorithm to accomplish this is explained in detail and makes extensive use of the linear algebra representation of BJzier curves.

DoD KEY TECHNOLOGY AREA: Other (Applied Mathematics)

KEYWORDS: BJzier Curves, Gauss-Newton Method, Affine Invariant Node Spacing

NAVY SEALS: THEORY VS. REALITY
Brian W. Reeves-Lieutenant, United States Navy
B.S., University of South Carolina, 1986
Master of Science in Defense Analysis-December 1997
Advisor: Gordon H. McCormick, Command, Control, and Communications Academic Group
Second Reader: Bard K. Mansager, Department of Mathematics

The purpose of this thesis is to examine two books that advance alternate theories to explain the success or failure of special operations. The first book is *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy*, by Lucien S. Vandenbroucke. Vandenbroucke discusses recurrent problems with U.S. special operations and identifies what he believes are the causes of failure of such operations. The second book is *Spec Ops*, written by William H. McRaven. McRaven examines eight historic cases from around the globe and develops his theory on how to conduct successful special operations. From the analysis of three recent Navy SEAL's special operations missions, both theories seem to provide a useful tool for thinking about the failure or success of special operations. Combining these theories provides a complete framework for senior planners and tacticians in formulating a plan for successfully conducting future special operations missions.

KEYWORDS: SEALs, Urgent Fury, Just Cause, Desert Storm

DoD KEY TECHNOLOGY AREA: Other (Special Operations)

DEVELOPMENT OF A TEST MECHANISM FOR ANALYZING FORCE ATTRITION METHODOLOGIES WITHIN AGGREGATED COMBAT SIMULATIONS
Michael L. Shenk-Captain, United States Army
B.S., Clarion University of Pennsylvania, 1988
Master of Science in Applied Mathematics-June 1998
Advisors: Bard K. Mansager, Department of Mathematics
James G. Taylor, Department of Operations Research

For aggregated combat simulation models, the methods for calculating force attrition must be based upon sound mathematical formulations and parameter estimations. With an inherent lack of representative combat data for modern warfare scenarios, one effective method for determining the required parameter estimates is to thoroughly analyze the output from a

stochastically based high-resolution combat model. It is this development of attrition parameters process, which so profoundly influences the validity of aggregated simulations, that lacks any comprehensive documentation or mathematical justification within the modeling community. By examining the development and validity of these processes for parameter estimation, valid attrition calibration formulae can be determined and used within force attrition algorithms in order to more precisely and justifiably model aggregated combat operations. The establishment of a user-friendly test bed for examining this attrition rate development process will play a major role in solidifying the understanding, implementation, and validation of current and future process techniques.

DoD KEY TECHNOLOGY AREA: Modeling and Simulation

KEYWORDS: Combat Modeling, JANUS, Simulation, Attrition, ATCAL

NETWORKS FOR LOW-BIT-RATE APPLICATIONS

Amir Uziel-Major, Israeli Army
B.Sc., Tel-Aviv University, 1988
Doctor of Philosophy in Electrical Engineering-June 1998
Advisor: Murali Tummala, Department of Electrical and Computer Engineering
PhD Committee: Gus K. Lott, Jr., Department of Electrical and Computer Engineering
Craig W. Rasmussen, Department of Mathematics
Gilbert M. Lundy, Department of Computer Science

This work addresses issues related to the design and performance of a wireless integrated services network with emphasis on a tactical framework. We propose an asynchronous transfer mode (ATM)-like protocol architecture for the mobile network, which is an extension of schemes proposed in the literature. A medium-access-control (MAC) scheme, based on slot reservation by the remotes, is proposed for the network. Traffic models for low-bit-rate applications, suitable for low-capacity channels, such as a multiple-access (macrocell) wireless network, are presented. New bi-directional speech-conversation and bursty data models are proposed.

The issue of scheduling in wireline integrated services networks is thoroughly addressed and new algorithms are proposed. An analytical scheme to obtain the required (static) capacity for homogeneous sources based on their Markov-chain characterization is provided. A necessary condition for optimality of a scheduling algorithm is the balance of cell-loss-probability (CLP) ratios to values approaching 1 from below, on the boundary of the admissible region. The balanced-CLP-ratio (BCLPR) algorithm satisfies this condition but ignores the deadlines of the cells. The shortest time to extinction (STE) with BCLPR (STEBR) algorithm, proposed here for the first time, utilizes the earliest-deadline-first concept while satisfying the necessary condition. A proof is provided to show that the STEBR decisions are optimal at each service slot given that no information about future traffic arrivals is available. Simulation results indicate that STEBR admits more sources and yields larger normalized channel throughput (by up to 4%) than STE.

The wireless network presents a case of distributed queues at the command post (CP) and in the remotes, making channel allocation more involved compared to scheduling in wireline systems. Based on the schedulers discussed for the wireline queue, corresponding algorithms for operation in the wireless network are developed. The cases of partial and complete status reports of the remotes are investigated as a function of the network load in five representative scenarios. The following (descending) order of performance under both partial and complete status reports is maintained in all scenarios:STEBR, STE, BCLPR, and static allocation. Performance of the schedulers using partial or complete status reports depends on the value of the normalized throughput. The complete-status mechanism is preferred whenever the normalized throughput is smallerthan 0.70-0.75; partial status reports are sufficient for normalized throughput larger than 0.70-0.75. A hybrid approach that makes use of this outcome is proposed to best utilize the available channel capacity under all possible levels of network load.

DoD KEY TECHNOLOGY AREA: Command, Control, and Communications, Modeling and Simulation, Other (Networking)

KEYWORDS: B-ISDN, ATM, MAC, Scheduling, Channel Allocation, Mobile Networks, Low-Bit-Rate Source Models

APPLICATIONS OF JOINT TACTICAL SIMULATION MODELING

Steve VanLandingham-Lieutenant, United States Navy
B.S., United States Air Force Academy, 1992
Master of Science in Defense Analysis-December 1997
Advisor: Bard K. Mansager, Department of Mathematics
Second Reader: Gordon H. McCormick, Command, Control, and Communications Academic Group

Advances in technology allow Computer Simulation Models (CSM) to be used as a powerful tool to aid military decision-makers. This thesis explores the usefulness of one of these models, the Joint Tactical Simulation (JTS). First, this thesis outlines the information and tasks required to run JTS, which will give the reader a basic understanding of the program and how much effort it requires. Next, it describes the scenario presented in this thesis by detailing the methodology of terrain development, listing the assets required and the mission concept employed. It concludes by discussing some of the advantages and disadvantages of JTS followed by a reevaluation of the simulation and its possible uses.

The concluding appendix is a tutorial that guides the reader through an amphibious assault modeled on the UNIX-based computer systems at the Naval Postgraduate School's (NPS) Secure Systems Technology Laboratory. It was designed to be accomplished in less than four hours and give the user an opportunity to run a simulation while conducting minimal interaction.

KEYWORDS: Joint Tactical Simulation, Naval Special Warfare, High Resolution Models

DoD TECHNOLOGY AREA: Modeling and Simulation

SOLUTION OF LARGE-SCALE ALLOCATION PROBLEMS WITH PARTIALLY OBSERVABLE OUTCOMES

Kirk A. Yost-Lieutenant Colonel, United States Air Force
B.S., United States Air Force Academy, 1980
M.S., Rensselaer Polytechnic Institute, 1986
Doctor of Philosophy in Operations Research-September 1998
Advisor: Alan R. Washburn, Department of Operations Research
Committee: Gerald G. Brown, Department of Operations Research
Robert F. Dell, Department of Operations Research
Guillermo Owen, Department of Mathematics
Craig M. Rasmussen, Department of Mathematics

Methods were developed for optimally solving problems that require allocating scarce resources among activities that either gather information on a set of objects or take actions to change their status. Also, the information gathered on the outcomes of the actions taken may be erroneous. The latter situation is called *partial observability*, and methodology available prior to this dissertation is combinatorially intractable for problems with more than one object. Two previously-uncombined methods were used–linear programming (LP) and partially observable Markov decision processes (POMDPs) – to construct a decomposition procedure to solve the resulting large-scale allocation problem with partially observable outcomes. Theoretically it was shown that this procedure is both optimal and finite; in addition, improvements were developedto the procedure that reduce runtimes on test problems by 95%. It was demonstrated that the procedure on a small targeting problem with a known analytical solution, as well as a large-scale military example concerned with allocating aircraft sorties, weapons, and bomb-damage assessment sensors to targets. Finally, analytical bounds were developed on the expected objective function values of a related allocation problem with more stringent resource constraints, and present a simulation-based approach to estimate the distributions of the outcomes for that model.

DoD KEY TECHNOLOGY AREAS: Air Vehicles, Command, Control, and Communications, Conventional Weapons, Sensors, Modeling and Simulation, Materials, Processes, and Structures

KEYWORDS: POMDP, MDP, Linear Programming, USAF, BDA, Sensor Modeling