Computer Science Colloquium

Seventeenth Series - Spring 2003

Thursdays noon to 12:50 in Darwin 108 on the SSU Campus
Open to the Public

February 13	SOFTWARE TECHNOLOGIES FOR WIRELESS APPLICATIONS David Ni Crescentec and Memes Technology, Danville The continuous growth of wireless applications such as cellular phones and wireless LAN has been pushing the vendors searching more new technologies for service deployment, feature enhancement and cost reduction. This talk will focus on some of software technologies, which are important to different stages of wireless application development: from RF IC design, telecom/wireless standard/architecture, and service infrastructure. We will discuss some challenges in each area and the related computing disciplines.
February 20	A BRUSH WITH FAME, DIGITAL ARTWORK AND DOZENS OF DEADLY WEAPONS Bill Nelson Petaluma A chronicle of the journey of a non-digital artist into the world of bits, bytes and bus. Digital imagery has changed our perception of the world in many ways, in particular how we SEE it. How do we translate from an analog world into the digital realm? Even our actors may become digital representations. How do we come to relate in a meaningful way with a world consisting of ephemeral differences in voltage and generated images? Learning to live with and love an interactive world within a Graphical User Interface.
February 27	EARLY SUPERCOMPUTERS AND DISASSEMBLERS Steve Jasik Jasik Designs, Menlo Park

	Steve Jasik talks about the 1st supercomputers of the 1960's, the Control Data 6600 and 7600, and about the global disassembler MacNosy. Mr Jasik was associated with Control Data from 1967 to 1984 where he worked on the FORTRAN compiler, mostly the code optimizer. At the time the 6600 was the first computer with multiple functional units and a micro parallel architecture, it presented some unique problems for those who tried to generate code for it. In 1984 wrote the first global disassembler, MacNosy for then new Apple Macintosh computer.
March 6	WHEN CAN I BUY A 50" 1920x1080 HDTV WITH HIGH BRIGHTNESS FOR 999$? Mary Lou Jepsen MicroDisplay Corp., San Pablo MicroDisplay Corporation creates HD-resolution LCOS (liquid crystal on silicon) display chipsets for use in optical projection systems. MicroDisplay panels are capable of 500 frame per second operation allowing their use in single-panel projection systems. Single panel systems offer substantial cost and quality advantages over the three-chip (one for red, green and blue) alternatives. MicroDisplay's single panel operation is enabled by 1) high speed electronics 2) fast, high contrast, TN liquid crystals (80 microsecond switch time) 3) ability to manufacture thin (fast) layers of liquid crystal material at our manufacturing facility in San Pablo. This technology is about to be become widely available, and will likely find uses in other newer, currently high-end, display technologies.
March 13	SOLVING THE KNIGHT'S TOUR WITH A GENETIC ALGORITHM Vahl Scott Gordon California State University, Sacramento The Knight's Tour puzzle has captured the imagination of mathematicians and chess players for centuries. The goal is to find paths through a chessboard with standard chess knight moves, touching every square exactly once. A simple hill-climbing solution is presented, and applied to a random population of 1 million individuals. The same framework is then used as the basis for a Simple Genetic Algorithm (SGA), which evolves 1 million individuals with simulated natural selection, crossover, and mutation. Running time is identical for both cases. The results of the two experiments are compared, and the efficacy of the SGA on this problem is evaluated. The experiments were done at Sonoma State University and at CSU Sacramento by the author, with SSU Alumnus Terry Slocum.

March 20	JAVA: IT'S BETTER THAN YOU THINK, FOR REASONS YOU HAVEN'T REALIZED YOU ALREADY KNOW William Grosso Mountain View In this talk, the speaker will draw upon his past experience as chair of SDForum's Java SIG (www.sdforum.org/sigs/java) and his current role as the chair of SDForum's Emerging Technology SIG (www.sdforum.org/sigs/emerging) to explain why beginning and intermediate programmers should learn Java, why most (practical) software innovations over the next few years will involve programs written in Java, and why programmers using Java-based systems are going to reinvent the internet over the next 5 years.
March 27	LUBY-RACKOFF CIPHERS OVER FINITE ALGEBRAIC STRUCTURES OR WHY XOR IS NOT SO EXCLUSIVE Zully Ramzan IP Dynamics, Campbell Luby and Rackoff showed how to construct pseudo-random permutations from pseudo-random functions; their paper formalized the concept of a secure block cipher. Their goal was to understand what makes the U.S. Data Encryption Standard (DES) secure. The technique is based on composing several Feistel permutations. The Feistel permutation, a fundamental building block of DES, involves applying a so-called round function to the right half of the input and taking the XOR with the left half of the input. We consider the question of what happens when operations other than the XOR are applied. In particular, we engage in a study of Luby-Rackoff ciphers when the operation in the underlying Feistel network is addition over an arbitrary finite algebraic structure. We obtain the following results: We construct a Luby-Rackoff cipher which can be easily broken when XOR is used, but is secure against adaptive chosen plaintext and ciphertext attacks when addition in finite groups of characteristic greater than 2 are considered. This cipher has better time/space complexity and uses fewer random bits than all previously considered Luby-Rackoff ciphers. We show that our construction is tight when operations are performed over a finite field, and a minor relaxation in one of the requirements results in it being insecure, though the attack here is non-obvious. We examine various other Luby-Rackoff ciphers known to be insecure under XOR. In some cases, we can break these ciphers over arbitrary Abelian groups - -- though we have to employ new more complex techniques. In other cases, however, the security remains an open problem. This talk is based on joint work with Sarvar Patel and Ganesh Sundaram of Lucent Technologies/Bell Labs, and appeared in SAC 2002.
April 3	INFORMATICS AND VISUALIZATION TOOLS FOR PHARMACOGENETICS RESEARCH Tom Ferrin

	University of California, San Francisco Genetic variation among individuals can play a critical role in their response to drug therapy. Dosage levels that provide good efficacy in one individual may produce toxic effects in another, or may have little therapeutic effect at all. Understanding and predicting individual drug response will become increasing important in the future and requires the analysis of large amounts of genomic information. This talk will describe one of the current studies underway in this area and discuss the types of data analysis and visualization required to elucidate the pharmacogenetics of a class of proteins known as membrane transporters.
April 10	SPRING RECESS - NO COLLOQUIUM
April 17	TRENCH-BASED PRACTICAL TIPS FOR CREATIVE SOLUTIONS TO VEXATIOUS PROGRAMMING PERPLEXITIES Don L. Jewett Abratech Corp., Sausalito Creative solutions to difficult problems are often retrospectively honored in our society (when the solution works). But there is also a mystery that seems to surround the process, and many think one must passively wait for inspiration to "strike". Many examples abound that show the Steps to creativity can be enhanced and even manipulated, and the examples come from programming, and from science. This talk is about those examples, and the generalizations that can be derived from them. One generalization: Very high intelligence is not a requisite, but there is one behavioral trait that is absolutely necessary.
April 24	INSIDE COMPUTER GAME DEVELOPMENT Jason Shankel Maxis Corp., Walnut Creek The computer game industry is a hybrid of two very different fields: technology and entertainment. In this talk, I will describe how a typical computer game evolves from the concept stage, through development, and finally to the marketplace, with special emphasis on how game developers deal with the many conflicts that arise between the technological and the entertainment requirements of a game.
May 1	THE FRIENDLY ORANGE GLOW: THE LIFE AND TIMES OF THE PLATO SYSTEM AND THE BIRTH OF CYBERCULTURE Brian Dear

	La Jolla Long ago, out on a prairie far, far away . . . back before PCs, the Internet, AOL, the Web, and USENET existed, back before Steve Jobs, Bill Gates, Steve Case, and Scott McNeally had even graduated from high school, a rich, vibrant online culture was already booming at the University of Illinois, an online world complete with open-source hacking, email, message forums, Slashdot-like news blogs, chat, instant messaging, MUDs, and other intense multiplayer games. How could this be? Come to this presentation and learn all about the research Brian Dear has been undertaking for a book on the history of PLATO: the legendary and profoundly-influential system whose saga has long been overshadowed by the stories of ARPANET, Xerox PARC, and Silicon Valley. In this session, we'll explore a wide range of topics including: the quirky system architecture of PLATO; gas-plasma flat-panel displays (originally invented for PLATO); the origins of Lotus Notes (descended from PLATO Notes); the story of CERL (the PLATO laboratory that predates PARC by three years); and how numerous PC games (including Flight Simulator, Wizardry, FreeCell, Castle Wolfenstein) all descend from PLATO.
May 8	SOFTWARE: THE WORLD'S BUSINESS STRATEGY COINED IN CODE Alfred Chuang BEA Systems, San Jose Mr. Chuang's speech will be the intertwined story of BEA's founding by Mr. Chuang and two partners 8 years ago in a one-room office, its achievement in becoming the fastest company in history to reach $1 billion in revenue and its current emergence in the top tier of information technology companies; doing battle with IBM, Microsoft and Oracle, among others; set against the technical evolution of BEA from providing the transaction-based;operating system for Internet business; to its current focus on delivering an entire application infrastructure that allows global businesses to develop, deploy, integrate and extend the applications that represent their business strategy expressed in 1s and 0s.
May 15	1 + 1 = 3 Marc LeBrun Fixpoint Inc. "Incredible systems abound, but of pleasant construction or of a sensational kind." -- Jorge Luis Borges, "Tl'n, Uqbar, Orbis Tertius" We entertain the thesis that there are no bugs, only under-appreciated outputs. Probing familiar primitive operations at subatomic scales, we sketch an introductory natural history of some arithmetics from alternate universes. This in turn recommends more systematic spelunking in the wide dark space of programs, attending carefully to the whispering vox machina. (Note: While abstaining from inventing any allegedly New Kinds of Science, we cannot rule out possible wild discursions into the nature of knowledge and the future of culture.)

	As a concrete warm-up exercise, you are invited to contemplate what the simple expression x & -x computes for integral x.