doi:10.1093/comjnl/bxn034

Capsule Reviews

FAIROUZ KAMAREDDINE

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue in order to bring the content to a wider readership. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the Department of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

Evaluation of Economy in a Zero-Sum Perfect Information Game AZLAN IQBAL

Zero-sum games of perfect information (where every player knows all the moves) are amenable to computation since a perfect game is possible by analysing the game tree. Chess is an example of a zero-sum game of perfect information. This paper is concerned with economy in the chess game playing where the emphasis is on winning with style. Economy is either deemed good or bad and is somewhat subjective while being closely tied to the rules of the game. In chess, economy includes economy of material (pieces) and space (full usage of the board) and needs to be defined clearly so that players could rate the positions. The paper collects a number of economic features from chess literature which it uses to develop an evaluation function to generate a numerical score for any checkmate position. The steps required to evaluate a mating's position's economy are given and a chess computer program which accommodates the economy evaluation function was written. Four experiments were performed to test the evaluation function and these showed positive results. The paper addresses further issues which include minor economical differences between two positions, paradoxical positions, perfect economy, and economy outside checkmate and in other games.

Modeling ODP Computational Specifications using UML ROMERO, TROYA AND VALLECILLO

Model engineering considers models as first-class citizens allowing the creation, analysis and manipulation of systems. The size and complexity of current IT systems challenge most software engineering methods. The reference model of open distributed processing (RM-ODP) supports the integration of distribution, interworking and portability and provides five viewpoints on a system: enterprise, information, computational, engineering and technology. The computational viewpoint focuses on the software architecture of the system and the quality of service (QoS) is determined by the environment contracts of the computational specifications. However, the ODP reference model lacks a user-friendly notation for expressing the different models in a multi-viewpoint specification and which is able to represent the semantics of the ODP viewpoints concepts. The paper proposes that UML is a promising candidate for solving this problem especially since it has been improved to incorporate better mechanisms for describing components by means of UML profiles. This paper is part of a project which defines a standard for the use of UML for ODP system specifications. It describes the approach to express ODP computational specifications in UML and covers the specification of environment contracts. The authors give an introduction to the computational viewpoint in RM-ODP and to UML version 2. Then, the paper summarizes how the main concepts of the ODP computational language are expressed in terms of the UML 2 concepts. Computational objects and interfaces, environment contracts and computational specifications are introduced and a summary of the ODP computational viewpoint profile is given. The UML profile for the ODP computational viewpoint is demonstrated in a case study and a number of issues related to this approach are discussed.

Composition of Self-Adapting Components for Customizable Systems PASTRANA, PIMENTEL AND KATRIB

In component-based software engineering, component interfaces are a syntactic definition rather than behavioral modules. However, the definition of the behavior and interaction amongst components cannot be extracted from the interface. This is essentially problematic when components are devleoped by different teams. This paper proposes the use of the so-called connectors as a way of viewing an application's architecture as a composition of independent components giving more explicit application architecture at code level. Furthermore, the paper develops a tool for generating automatically the connectors which represent the interaction relationships between components. This way, connectors are run-time entities that describe and control inter-components communication and behavior. First, the preliminaries and

state of art are given. Then, the paper presents a method of using web services as connectors and gives a graphical tool to automatically generate connectors. The paper develops both the syntax and semantics and discusses typical characteristics of real-time systems that can be incorporated to connectors. A chess game example is developed to illustrate how the proposal works. The proposal is further consolidated type theoretically where it is shown how sub typing can be used to capture important features like inheritance, reuse, delegation and composition. Further theoretical and implementation analysis and studies are carried out.

The effect of the Distributed Test Architecture on the Power of Testing HIERONS AND URAL

When testing a distributed system, a distributed test architecture is needed where a tester is placed at each port and a test sequence is applied. This brings out the possibility of coordination problems related to controllability and observability. This paper shows that in the distributed test architecture one needs a different notion of an input sequence distinguishing two states. The paper introduces the notion of locally s-distinguishable and local s-equivalent states of a Finite State Machine (FSM) and shows that in distributed test architecture, testing can distinguish between two states without creating a controllability problem if and only if the states are locally s-distinguishable. The paper starts with the necessary preliminaries introducing multi-port FSMs and controllability and observability problems. Then, the paper introduces the notions of globally distributing and s-locally distributing states and defines what it means for an input sequence to locally s-distinguish two states of an FSM giving bounds on the length of such sequences. A polynomial time algorithm is given and works as a variant of a classical algorithm for generating sequences that globally distinguish states of a single-port FSM. Another algorithm is given to produce a locally s-minimal FSM.

Efficient algorithms for Integer division by constants using multiplication. CAVAGNINO AND WERBROUCK

Normally, integer multiplication of two single words produces a double-word product, and hence division is a double-word dividend divided by a single-word divisor to produce a single-word quotient and a single-word remainder. This paper analyzes a method of integer division of an unsigned single-word dividend by an unsigned single-word divisor in which the principle operation is the multiplication of the dividend by the multiplicative inverse of the constant divisor known at compile time. The paper introduces the division by multiplication method (DBM) which computes the quotient Q in an integer division of an unsigned dividend N by an unsigned divisor D known at compile time, through a first approximation of Q by a function DBM_a(N,J) where N is known at run-time and J is computed at compile-time and then the paper attempts to assess when this approximation is indeed the quotient Q. Further optimizations of the function DBM are given. A number of qualitative analysis measurements are given through two tables which treat odd versus even divisors. Then the paper extends DBM so that instead of only treating division of an unsigned single-word by another unsigned single-word, one can treat division of an unsigned double-word by an unsigned single-word.

Analysis of Linear Time Sorting Algorithms SHUTLER, WOON AND LIM

Linear time algorithms (e.g., linear probing sort [Dob]) compare the sizes of the elements being sorted and have attracted much attention recently. These algorithms require random access to the data being sorted making them excellent examples of the impact of cache latency. This paper reviews in detail the theory and practice of linear probing sort (LPSORT) giving CPU time formulae underlining the importance of using CPU time as a measure of success of any theoretical analysis. Experimental results are given which are used in an attempt to model random access latency more accurately. Comparisons with existing algorithms show encouraging results that both complement and confirm the earlier literature.

Computing with Time: From Neural Networks to Sensor Networks SZYMANSKI AND CHEN

This paper proposes a new way of using timing information where a competition is introduced to look for an optimal firing time which encodes information. The proposed approach is called computing with time. It is highly influenced yet complements the computing with action potentials approach of Hopfield. The power of computing with time is illustrated through an example that involves n students sitting in a hall and listening to a lecturer who wants to find the youngest student in the room. The paper proposes an efficient lecture hall algorithm which solves the problem and which is independent of the number of students involved. A number of extensions and applications of the algorithm are discussed and this is followed by a detailed analysis of the algorithm. This algorithm is applied to sensor networks and in particular to the so-called self-selective routing (SSR) protocol. The properties of SSR are discussed and it is stated that SSR can automatically avoid congestion and can automatically converge to the shortest path. Extensive performance studies are given.

Selectively Convertible Authenticated Encryption in The Random Oracle Model HUNG-YU CHIEN

Encryption schemes allow privacy in the public key setting and privacy/authenticity in the symmetric setting. Authenticated encryption allows both authenticity and privacy and

may provide non-repudiation in the public key setting but does not do so in the symmetric setting. A verified signature provides the information and the non-repudiation of both the signing/transaction event and the signed/transaction content simultaneously. This paper is concerned with authenticity, privacy and non-repudiation of both the transaction content and event. The paper offers a selectively convertible authenticated encryption (SCAE) scheme which allows the sender to generate an authenticated encryption and enables the communicating parties to reveal the transaction/event content. First, the CSAE scheme is presented through eight algorithms. Then, to consider the issues that affect privacy, an FSCAE-model is presented in detail and a number of security issues are analysed. Furthermore, unforgeability and security reduction for both confidentiality and unforgeability are studied in detail and are consolidated through simulations. Extensive analysis is given and a number of applications are introduced.