Capsule Reviews

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. This issue's Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the School of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

New models of computation. P. WEGNER AND E. EBERBACH
This paper argues for other models of computation than Turing machines. The paper uses the fact that present-day computing deals with notions such as non-sequentiality, interactions and dynamic processes. The paper reviews three alternative models of computation: Milner's π-calculus of mobile processes, the interaction machines of the first author (which describes interactions in object-oriented and distributed systems) and the \$-calculus model of processes of the second author. The paper argues that these three models are better than Turing machines for the solution of computational problems.

Generalized template splay: a basic theory and calculus. G. GEORGAKOPOULOS AND D. MCCLURKING
This paper deals with the problem of maintaining a directory which supports at least the operations of inserting, deleting and searching for an element. Although this problem is well-studied in the literature, there remain many open questions related to the various existing approaches. This paper deals with one such approach, the so-called 'splay trees'. Splay trees are self-adjusting search structures which enjoy nice properties, such as amortized cost for searching and being competitive with respect to any static binary search tree on the same elements. The authors explain why splay trees are successful and extend the splay tree theory in an attempt to find a way such that 'splay' can be performed under more general conditions in any multi-way tree, while still enjoying good properties related to cost, optimality and performance. This generalization is achieved via a new calculus where a potential on a weighted tree is first defined and then used by a new technique for calculating the changes in potential. In this way, the calculus estimates the cost of a candidate set of rules for splay.

The towers of Hanoi with forbidden moves. A. SAPIR
As the title expresses, this paper deals with the towers of Hanoi problem but where limitations are imposed on the possible moves amongst the three pegs of towers. The 3-peg tower of Hanoi problem involves moving n disks of different sizes from the first peg onto the third one. At every stage, including the initial one, no disk resides on top of a smaller one, only one disk is moved at a time and only the top disk is moved. The middle peg serves as an intermediary peg to enable the moves respecting the conditions imposed. This problem, despite appearances, involves a huge amount of moves, even for a small number of disks. This complexity has attracted a great number of studies, and it has given rise to many varieties of the problem (coloured disks, more than three pegs, etc.). This paper analyses all possible variants of the tower of Hanoi problem with three pegs and with movement restrictions. A variant is defined as a directed graph with three vertices where a vertex represents a peg and a directed edge between two pegs means a move (in the edge direction) is possible between the pegs. This definition leads to five possible variants. The paper gives an algorithm for the variant problems, which is shown to need a minimal number of moves and establishes the number of moves carried out by the algorithm for each variant.

Analyzing information flow properties in assembly code by abstract interpretation. R. BARBUTI, C. BERNARDESCHI AND N. DE FRANCESCO
With mobile technology more and more prominent, the problem of security leakages becomes more and more important. Due to this importance, the problem of security leakages is extensively studied in the literature. However, since the downloaded code may be an assembly code, this paper studies the problem of secure information flow in stack-based assembly languages. The method used in the paper is an abstract interpretation of the operational semantics, where programs are analysed in order to collect approximate information about their run-time behaviour. The authors define a notion of security, the so-called sigma security, and give sufficient conditions that the abstract transition system needs to satisfy in order to ensure sigma-security. Since the approach of this paper is semantical, there is a good potential for its automation. The authors exploit this potential and outline the approach of using model checking for checking sigma-security where, in particular, security properties are formalized as temporal logic formulas.

Inversion coding. Z. ARNAVUT
The Burrows–Weeler compression (BWC) algorithm is a block sorting lossless data compression technique which applies to text or image data and achieves good compression rates. The algorithm first performs lexical sorting transformations and then initiates the Move To Front (MTF) coder. The final stage of the BWC algorithm is a statistical compressor such as an arithmetic coder. However, researchers have questioned whether the MTF coder can be replaced with another scheme to improve the compression. This paper departs from these questions and investigates the compression of data by converting multiset permutations to canonical sorting permutations, followed by an inversion technique on the permutations performed. This leads to a more memory efficient and faster algorithm for inversion coding. The author shows that the inversion

coding technique introduced yields significant compression gains over the MTF coder, and that compression of data can be improved when the inversion coder is used instead of the MTF coder in the second stage of the BWC algorithm.

Combining encryption and proof of knowledge in the random oracle model. M. ABE

This paper deals with validity checking, which confirms the security of a ciphertext against adaptive ciphertext attacks. Two classes of validity checking are known. The first requires a decryption key to perform the checking and allows validity checking to be very efficient. The second allows anyone to perform validity checking and requires a proof of knowledge/membership about the underlying message made non-interactive in some model. This second class requires a large overhead for validity checking of such a proof. Despite its drawbacks, the second class of validity checking is useful in some scenarios and this led some researchers to make some assumptions related to it to make it work. However, these proposed schemes lead to difficulties related to proving their security. For this reason, this paper combines weak encryption schemes with proofs of knowledge made non-interactive through the use of a hash function. This is done through a generic construction of encryption schemes with public ciphertext checking which are provably secure against attacks. As a result, security of these schemes can be proven solely in the random oracle model.

Model checking of abstract description of state machines. Y. XU, X. SONG, E. CERNY AND A.-M. OTMANE

Model checking is a practical tool for the automatic verification of data. However, this method works well when the data is represented at the Boolean logic level and otherwise leads to a state explosion when the datapath is large. For this reason, this paper uses the so-called abstract description state machine (ASM) where a data value can be represented as a single variable of abstract type (rather than as a vector of Boolean variables) and a data operation can be represented by an uninterpreted function symbol. In the verification process using ASMs, the state explosion problem of large datapath disappears since the complexity no longer depends on the width of the datapath. ASMs already existed, but this paper studies the model checking aspect of ASMs. For this, the authors develop a first-order linear-time temporal logic which allows to verify properties on designs represented by ASMs. Property checking algorithms for this logic are given and are shown to be correct in another publication. However, these algorithms may not always terminate. Moreover, the decidability of model checking for the first-order linear-time temporal logic is left open.

Diagnosis of symmetric graphs under the BGM model. R L. C. P. ALBINI, S. CHESSA AND P. MAESTRINI

System-level diagnosis is a methodology to discover faulty units in large systems and depends on units being able to test other units. The best known model for such testing is the so-called PMC model which assumes that tests of faulty units performed by fault-free ones always return 1 and that the tests performed by faulty units return arbitrary results. Another proposed model is the BMG model, which is similar to the PMC model except that it assumes that a faulty unit is always tested as faulty regardless of the state of the tester. Research on system-level diagnosis places a strong emphasis on systems represented by symmetric regular graphs with a limited number of nodes. But this limitation imposed on the number of nodes led to new approaches which either use random graphs or impose upper bounds on the number of faulty nodes. In particular, new methods provided diagnosis algorithms for regular systems, which give almost complete diagnosis under the PMC model. This paper extends these methods from the PMC model to the BMG model and provides a diagnosis algorithm for symmetric systems under the BMG model (called DABS). The authors show that DABS provide correct diagnosis, but which may be incomplete. This leads the authors to define a measure of diagnosis incompleteness and to introduce an evaluation approach under this diagnosis incompleteness which leads to various results relating to the performance of the method.

A suggestion for fast residue multiplier for a family of moduli of the form $(2^n - (2^p + -1))$**.** A. A. HIASAT

A residue number system (RNS) is an arithmetic system which increases the speed of computations. For this reason, RNSs have been used in many applications. This paper deals with modular multiplication on RNSs. The subject of modular multiplication on RNSs is largely studied but this paper is concerned with a family of moduli that have the form $(2^n-(2^p+-1))$. A new modulo $(2^n-(2^p+-1))$ multiplication algorithm is presented and its hardware implementation is given. The algorithm compresses the magnitude of the partial products to be less than 2^n. The performance of the new proposed modular multiplier algorithm is studied. It is shown that this multiplier requires a larger area than required by other existing residue multipliers. However, despite the larger area requirement, the new modular multiplier is faster than any other similar multiplier. In particular, it is shown that the new multiplier is faster than a binary-based iterative multiplier for any $n > 16$ and that the new multiplier is most suitable when p is less than or equal to $n/2$.

Building footprint simplification techniques and their effects on radio propagation predictions. Z. CHEN, A. DELIS AND H. BERTONI

The widespread use of mobile communications calls for the need for fast and accurate radio wave propagation prediction systems. Ray-tracing-based radiopropagation prediction models have shown promise but they depend on features like building shapes, locations, weather, vegetation, etc. Hence, for a ray-tracing system to work well, the building database needs to be precise and the prediction time needs to be reasonable. But the prediction time is closely related to both building and vertices involved, and if the number of footprints in the vertices is reduced, then the predictions can be generated more quickly. As a result, this paper proposes four families of efficient single-pass algorithms to simplify building footprints. Moreover,

maintaining prediction accuracy leads the authors to propose a number of constraints and subsequently to propose multi-pass and hybrid algorithms. Multi-pass simplification algorithms use multiple constraints simultaneously and avoid backtracking. Hybrid simplification algorithms take advantage of complementary properties of different footprint simplification studies and hence offer better performance. The paper investigates the performance of the proposed building footprint simplification algorithms using different experiments and establishes various results concerning the performance of the different methods with respect to one another and with respect to other methods.