Definability and Verification by Model Checking

Richard Lassaigne & Michel de Rougemont

We study the verification of properties of programs when the input is a finite structure such as a word or a graph and not only a sequence of bits. We recall classical lower bounds on the size of OBDD's for natural graph properties such as *Graph Accessibility* and *Perfect Matching* and introduce the notion of a *Compression*. It is a mapping from a (large) structure $\mathcal{M}$ representing a program to a smaller one $\mathcal{M}'$ of a different signature. To verify a property of a program defined by a formula ψ (i.e. whether $\mathcal{M} \models \psi$), we study the existence of another formula φ of a logic $\mathcal{L}$ such that $\mathcal{M} \models \psi$ iff $\mathcal{M}' \models \varphi$.

For probabilistic programs we look for compression schemas such that

$$\mathcal{M} \models \text{Prob}[\psi] > b \Leftarrow \mathcal{M}' \models \varphi$$

i.e. a deterministic statement on $\mathcal{M}'$ implies a probabilistic one on a (large) $\mathcal{M}$. We give two examples, one for *Graph Accessibility* and the other for *Perfect Matching*.

Addresses
Richard Lassaigne: Equipe de Logique Mathématique, University Paris VII, Paris, France

Michel de Rougemont: Université Paris-II & LRI, Bâtiment 490, F-91405 Orsay Cedex, France