Model Checking with Edge Valued Decision Diagrams

Pierre Roux, École Normale Supérieure de Lyon, France. pierre.roux@ens-lyon.fr
Radu I. Siminiceanu, National Institute of Aerospace, Hampton, Virginia, USA. radu@nianet.org

Abstract

We describe an algebra of Edge-Valued Decision Diagrams (EVMDDs) to encode arithmetic functions and its implementation in a model checking library. We provide efficient algorithms for manipulating EVMDDs and review the theoretical time complexity of these algorithms for all basic arithmetic and relational operators. We also demonstrate that the time complexity of the generic recursive algorithm for applying a binary operator on EVMDDs is no worse than that of Multi-Terminal Decision Diagrams.

We have implemented a new symbolic model checker with the intention to represent in one formalism the best techniques available at the moment across a spectrum of existing tools. Compared to the CUDD package, our tool is several orders of magnitude faster.

1 Introduction

Binary decision diagrams (BDD) [**?**] have revolutionized the reachability analysis and model checking technology. Arithmetic decision diagrams [**?**], also called Multi-Terminal Binary Decision Diagrams (MTBDD) [**?**] are the natural extension of regular BDDs to arithmetic functions. They take advantage of the symbolic encoding scheme of BDDs, but functions with large co-domains do not usually have a very compact representation because there are less chances for suffixes to be shared.

Edge-valued decision diagrams have been previously introduced, but only scarcely used. An early version, the edge valued binary decision diagrams (EVBDD) [**?**], is particularly useful when representing both arithmetic and logic functions, which is the case for discrete state model checking. However, EVBDD have only been applied to rather obscure applications: computing the probability spectrum and the Reed-Muller spectrum of (pseudo)-Boolean functions.

Binary Moment Diagrams [**?**] were designed to overcome the limitations of BDDs/EVBDDs when encoding multiplier functions. However, their efficiency seems to be limited only to this particular type of functions. A new canonization rule for edge-valued decision diagrams enabling them to encode functions in $\mathbb{Z}\cup\{+\infty\}$ was introduced in [**?**] along with EVMDDs, an extension to multi-way diagrams (MDD) [**?**], but, again, this was applied to a very specific task, of finding minimum length counterexamples for safety properties. Later, EVMDDs have been also used for partial reachability analysis.

In this paper we first present a theoretical comparison between EVMDDs and MTMDDs for building the transition relation of discrete state systems before dealing with an implementation in a model checker along with state-of-the-art algorithms for state space construction.

2 Background

2.1 Discrete-state Systems

A discrete–state model is a triple (S, S_0, T), where the discrete set S is the *potential state space* of the model; the set $S_0 \subseteq S$ contains the *initial states*; and $T : S \to 2^S$ is the *transition function* specifying which states can be reached from a given state in one step, which we extend to sets: $T(X) = \bigcup_{i\in X} T(i)$.

We consider structured systems modeled as a collection of K *submodels*. A (global) system state i is then a K-tuple $(i_K, \ldots, i_1)$, where i_k is the *local state* for submodel k, for $K \geq k \geq 1$, and S is given by $S_K \times \cdots \times S_1$, the cross–product of K local state spaces S_k, which we identify with $\{0, \ldots, n_k - 1\}$ since