# On Parallel Software Verification using Boolean Equation Systems

Alexander Ditter[1], Milan Češka[2], and Gerald Lüttgen[1]

[1] University of Bamberg, 96045 Bamberg, Germany,
{alexander.ditter,gerald.luettgen}@swt-bamberg.de,
[2] Masaryk University, 602 00 Brno, Czech Republic
xceska@fi.muni.cz

**Abstract.** Multi- and many-core hardware platforms are today widely accessible and used to significantly accelerate many computationally demanding tasks. In this paper we describe a parallel approach to solve *Boolean Equation Systems* (BESs) in the context of *model checking*. We focus on the applicability of state-of-the-art, shared-memory parallel hardware – multi-core CPUs and many-core GPUs – to speed up the resolution procedure for BESs. In this setting, we experimentally show the scalability and competitiveness of our approach, compared to an optimized sequential implementation, based on a large benchmark suite containing models of software systems and protocols from industry and academia.

**Keywords:** formal verification, parallel model checking, boolean equation systems.

## 1 Introduction

In this paper we propose and evaluate a parallel approach to the resolution of *Boolean Equation Systems* (BESs) on parallel, shared memory systems, i.e., utilizing state-of-the-art multi-core and many-core processors – though not in a hybrid setting. Our goals are to (i) evaluate the scalability of our parallel approach with respect to an increasing number of parallel *processing units* (PUs), and (ii) prove its competitiveness in comparison with an optimized sequential algorithm, which we implemented as described in [1].

**Motivation.** Today, hardware manufacturers no longer increase clock rates but the number of available PUs of processors. Along with the evolving massively parallel, throughput oriented hardware architectures [13], this has led to an increasing interest in the parallelization of software. Indeed, this trend has already found its way into the field of software verification and model checking years ago [5, 16, 17] and must be considered further in order to push the limits of verification techniques further towards industrial strength, allowing one to deal with larger state spaces and providing rapid feedback to developers.

Modern processors can be divided into two main branches: (i) CPU-based multi-core processors with up to tens of cores and (ii) GPU-based many-core

processors with up to several hundreds of cores. The key differences are (i) the ability to efficiently deal with control flow at the expense of lower data throughput and, respectively, (ii) the ability to provide high data throughput rates at the expense of a lack of efficient, control-flow guided execution. We assume the trend to continue – see e.g., Intel's "Terra Scale Computing"[3] project – suggesting future hardware to consist of more, yet simpler PUs. With respect to parallel algorithms, current hardware development favors approaches that are geared towards the *single instruction multiple data* (SIMD) paradigm, since they can most easily take advantage of this type of parallel hardware. Therefore, it is inevitable to consider the applicability of massively parallel, SIMD-based (i.e., many-core) systems in our experiments.

**Background.** The standard model checking problem [9], $M \models \varphi$, can be encoded by a BES [23], where the solution of the BES is equivalent to the solution of the underlying model checking problem. The BES is obtained by the synchronous composition of a *Labeled Transition System* (LTS), corresponding to $M$, and a property $\varphi$ (e.g., deadlock freedom) that is to be checked for this LTS. Consequently, the data dependencies within the resulting BES are closely related to the structure of the LTS from which it was generated. For our evaluation we rely on the well established VLTS benchmark,[4] which provides 40 LTSs – originating from academia and industry – that can be checked for deadlocks and livelocks, i.e., our resulting benchmark suite consists of a total of 80 BESs.

The average branching factor, i.e., the average number of outgoing edges per vertex, over all 40 LTSs in the benchmark is 5.73. With respect to parallelization, this number can be interpreted as an upper bound for the potential parallelism that is inherent to an LTS, as in our setting information needs to be propagated along edges. For workset based (i.e., bag of tasks) producer-consumer parallelizations [2] this means that (i) for each work item processed only few new work items are expected to be added to the workset, and (ii) synchronization is needed for concurrent operations on the dynamic data structure used to store the work items.

Due to this, our approach is not based on the producer-consumer paradigm that propagates only essential information, but on a more naive fixed point iteration. This promises a much higher potential for the utilization of parallel hardware as it does not require dynamic data structures. In our particular setting, data operations can even be implemented lock-free. Furthermore we do not have to populate a workset since we propagate all possible changes during a fixed point iteration, at the price of computational overhead, which is negligible considering the ever growing number of parallel PUs.

**Cilk Plus and CUDA.** Our approach is based on data-parallelization, which is commonly referred to as fine-grained parallelization (in contrast to task-parallelization, i.e., "coarse grained" parallelization). To efficiently parallelize this type of problem the choice of framework is very important, because it most

[3] http://techresearch.intel.com/ResearchAreaDetails.aspx?Id=27
[4] http://www.inrialpes.fr/vasy/cadp/resources/benchmark_bcg.html

significantly influences the overhead connected to context switches. In case of our multi-core parallelization the overhead of manual thread maintenance is not negligible since the amount of productive work per thread invocation is very limited. Therefore, the naive use of multi-threading environments, such as PThreads [26], is very likely to nullify the gain we expect from the parallelization itself. For this reason we chose Intel's Cilk Plus framework[5] which offers a work stealing based thread-pool and internally employs efficient scheduling and load balancing mechanisms. The scheduling of workers is not explicit and more lightweight than the manual management of threads.

For general purpose programming on GPUs, NVIDIA's *Compute Unified Device Architecture* (CUDA)[6] is the de facto standard framework for parallel computation. It provides an *Application Programming Interface* (API), allowing the utilization of NVIDIA's GPUs for massively parallel, throughput oriented applications beyond the scope of rendering graphics. Since the CUDA framework is tailored to applications with many data-parallel threads, light-weight computations per thread and frequent context switches [13], it is well suited for our application.

**Contributions and Related Work.** In the area of software model checking [9], the sizes of input problems become exceptionally large. For this reason, much research has been put into the development of techniques that can reduce the problem sizes by, e.g., applying abstractions, using efficient data structures such as Binary Decision Diagrams (BDDs) [8], or limiting the exploration of the problem domain to relevant parts only.

The approach advocated by us in this paper does not aim at reducing the problem size, but instead at exploiting modern parallel hardware for speeding-up the model checking of large problems. We parallelize a simple fixed point algorithm for BES solving on multi-core (CPU) and many-core (GPU) architectures. While our parallel approach is largely straightforward and its correctness is easy to understand, it gives rise to algorithms that – in the GPU case but not the CPU case – outperform an optimized sequential algorithm [1]. This standard algorithm for solving BESs is based on a workset data structure that propagates information during fixed point computation; however, in a parallel setting, synchronizations on this workset would lead to unacceptable overheads. In contrast, our approach does not require this workset; its higher computational costs are met by the higher number of PUs and their efficient utilization by us.

We extensively evaluate the performance of our workset-less multi-core and many-core algorithms when model checking deadlock and livelock properties on the large examples of the VLTS benchmark. More precisely, we used the tool "evaluator" distributed with the CADP toolset [24] to generate the BESs for our benchmark suite from the VLTS examples and the desired deadlock and liveness properties expressed as temporal logic formulae in the alternation-free $\mu$-calculus [19]. For convenience, we restrict ourselves to the evaluation of the

[5] http://software.intel.com/en-us/articles/intel-cilk-plus/

[6] http://developer.download.nvidia.com/compute/cuda/4_0/toolkit/docs/CUDA_C_Programming_Guide.pdf

solution step in the model checking process, since there exist several efficient and even parallel approaches for the construction of compact data representations in our setting [4, 5, 20], which can be used for preprocessing of input data.

Regarding closely related work, only two approaches on the parallel resolution of BESs are known to us. The first one [28] is based on a multi-core parallelization of the "Gaussian Elimination" as proposed in [23], which turns out not to be viable in practice due to its exponential space complexity. The second one [18] is tailored to distributed systems and aims at the resolution of extremely large BES instances. There exist further distributed implementations [7, 14, 16, 22] but their general goal is, in contrast to our approach, to increase the total amount of memory in order to deal with larger problem instances, rather than to improve on their run-time performance, as network latency typically degrades the overall performance significantly.

The experimental evaluation of the parity-game based approach presented in [27], which performs a parallel resolution of $\mu$-formulae on shared-memory multi-core systems, provides scalability results for up to eight workers. Yet, the range of examples is restricted to three *Sliding Window Protocol* (SWP) and two randomly generated instances, and their run-times are not related to existing sequential algorithms. In contrast, we present a parallel, shared-memory model checking approach that is based on a fixed point iteration used for the parallel resolution of BESs (cf. Sec. 3). Even though this approach is targeted at large BES instances, we are not only concerned about the capability to check large models, but also the improvement of run-time performance. The evaluation of our multi-core implementation confirms the scalability results presented in [27], extends them to a much larger set of different benchmark examples and, most importantly, puts them in relation to an optimized sequential BES solver (cf. Sec. 2). In addition, we show that our approach also scales on many-core architectures, boosting the run-time performance by one order of magnitude and outperforming the optimized sequential baseline significantly (cf. Sec. 4).

## 2 Fixed Points and Boolean Equation Systems

**Fixed Points and the $\mu$-Calculus.** The $\mu$-calculus [19] is a powerful formalism, e.g., subsuming the temporal logics LTL, CTL and CTL* [11], for expressing temporal properties. It features fixed point operators to express temporal properties such as liveness (i.e., something good will eventually happen) and safety (i.e., something bad will never happen). The following intuition describes the meaning of the least ($\mu$) and greatest ($\nu$) fixed point operators in the context of temporal-logic based model checking: $\mu$ is used to express liveness properties with the initial assumption that every state violates this property, and $\nu$ is used to express safety properties with the initial assumption that every state satisfies this property.

The syntax of the $\mu$-calculus is defined by the following grammar:

$$\varphi ::= \top | \bot | x | \neg\varphi | \varphi \wedge \varphi | \varphi \vee \varphi | [a]\varphi | \langle a \rangle \varphi | \nu x.\varphi | \mu x.\varphi$$

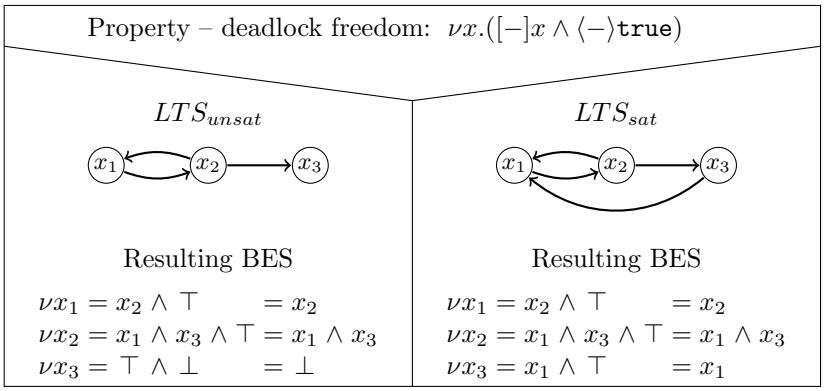



**Fig. 1.** Interpretation of $\mu$-formula over LTSs.

where $Var$ is a set of propositional variables with $x \in Var$, and $Act$ is a set of actions with $a \in Act$. In our setting, $\mu$-formulae are used to express properties over LTSs as exemplary depicted in Fig. 1.

**Boolean Equation Systems.** BESs are sets of equations, resembling monotonic functions over the Boolean lattice $\{false < true\}$, of the form $\sigma x = \varphi$. Here, the *left hand side* (LHS) $x$ is a Boolean variable from the set of propositional variables, $\sigma \in \{\mu, \nu\}$ is the least or the greatest fixed point operator, and the *right hand side* (RHS) is of the form $\varphi ::= \top | \bot | x | \varphi \wedge \varphi | \varphi \vee \varphi$.

In the context of model checking, BESs are the result of the interpretation of a $\mu$-formula over an LTS. Since the formula has to be verified for every state of the LTS, the resulting BES is of size $|LTS|$ x $|\varphi|^k$, i.e., the size of the BES is proportional to the size of the LTS and exponential in the complexity of the $\mu$-formula, where k is the alternation depth of $\phi$ which, roughly speaking, is the number of alternations of different fixed point operator types binding the same variables. Each fixed point operator of the formula is resembled by a so called *block* in the resulting BES, containing the set of equations associated with this operator. As is illustrated in Fig. 1, the resulting BESs for the deadlock freedom property with respect to the two displayed LTSs only contain one block, with three equations. This is because the corresponding formula only consists of one fixed point operator and each LTS comprises three states.

While equations may be reordered arbitrarily within a block, this is not the case for the ordering of blocks corresponding to alternating fixed point operators, as it may lead to the computation of a wrong fixed point. The order in which blocks have to be processed is defined by their nesting within the $\mu$-formula. In this paper, we consider only alternation-free $\mu$-formulae where the nesting of different fixed point operators binding the same variables is not allowed. Thus, dependencies between blocks form a tree [7] that can easily be constructed and yields the order (from leaves to root) in which the blocks have to be solved.

**Optimized Sequential Resolution of BESs.** To be able to conduct a fair evaluation of our parallel implementations for BES solving in terms of runtime competitiveness, we have implemented an optimized, sequential CPU-based algorithm in the style of the "chasing ones" as proposed in [1]. This approach is workset based and uses a queue to store work items, where a work item is equivalent to one equation of the BES. The computation in this algorithm starts at those equations where the LHS is directly assigned value *true* ($\top$) or *false* ($\bot$), and propagates this information to all equations relying on the value of these particular LHSs. For this purpose, equations must be enriched with information about such backward dependencies. As space and time complexity of this approach are linear in the size of the BES, it is well suited as a baseline for comparison with our parallel implementations.

## 3 Basic Fixed Point Algorithm and Parallelization

While a lot of effort has been put into the development and optimization of sequential model checking algorithms so as to fight computational complexity and state space explosion, our aim is to investigate whether a parallel approach can be more efficient and provide scalability not only on multi-core (CPU) architectures but also on many-core (GPU) architectures. For this purpose, we chose a fixed point iteration based algorithm, which we show to be well suited for such a parallelization. In this section we first present the algorithmic background of our approach, followed by the concepts of our parallel implementations.

**Basic Fixed Point Algorithm.** The listing of Algorithm 1 illustrates the fundamental idea of the fixed point computation that we employ for the resolution of BESs in our multi-core and many-core implementations.

**Algorithm 1**: FIXEDPOINT algorithm

**Input** : BES
**Output**: Solution of BES

```
1 Initialization of LHSs                          // true for σ = ν; false for σ = μ
2 foreach block B do                                          // block order matters
3     do
4         variablesChanged ← false
5         foreach equation E ∈ B do                // equation order does not matter
6             LHS ← evalRHS(E)
7             if LHSChanged then
8                 variablesChanged ← true
9     while variablesChanged
```

This algorithm consists of two nested loops, the outer one over the BES-blocks (line 2) and the inner one over all equations within a block (line 5). The outer loop processes blocks in a sensible order, corresponding to the dependencies within the $\mu$-formula (cf. Sec. 2). The inner loop computes the value of the LHS of an equation according to the evaluation of its respective RHS, where the RHS either consists of a terminal value (i.e., *true* or *false*) or LHS variables connected by Boolean operators. In the beginning, all LHSs are initialized depending on their associated fixed point operator $\sigma$, i.e., *false* in case $\sigma = \mu$ and *true* in case $\sigma = \nu$ (line 1). This *initial approximation* is derived from the Knaster-Tarksi fixed point theorem [29], where $\mu f = \bigsqcup\{f^i(\mathit{false}) : i \in \mathbb{N}\}$ and $\nu f = \bigsqcap\{f^i(\mathit{true}) : i \in \mathbb{N}\}$. The termination of the fixed point computation is detected by a marker variable, indicating whether one or more LHSs have changed during an iteration (line 9).

The time complexity of Algorithm 1 is quadratic with respect to the size of the BES since, in the worst case, only one LHS is changed per iteration (one execution of the inner loop), whence the maximum number of iterations is equal to the total number of equations, where each iteration performs a linear amount of work.

**Parallel Fixed Point Computation.** The core idea for the parallelization of the basic fixed point algorithm is based on the parallel resolution of individual blocks by executing the inner loop of Algorithm 1 (line 5), computing the LHS value of an equation, in parallel. It is important to note that the order in which equations are evaluated does not matter within the loop, as our parallel frameworks are not aimed at the explicit scheduling of threads. Considering the fact that this operation needs to be executed for all equations during each iteration step, this approach exposes much potential for parallel computation, even within one iteration step, as we expect the number of equations to be very large, e.g., the largest LTS in the benchmark contains 33,949,609 states. The soundness of the approach is guaranteed by the fact that BESs resemble monotonic functions, i.e., even if the evaluation of a RHS depends on several other LHS variables – which in a parallel setting are potentially modified concurrently – the updated value of each LHS is available and thus can be propagated in the subsequent iteration. For complex $\mu$-formulas the tree structure of BES-blocks can be exploited to increase the level of parallelization even further by processing all "leave blocks" in parallel.

**Multi-Core Data Structure.** Data structures for multi-core systems have to follow two main objectives. On the one hand, they have to provide good data locality, i.e., data necessary for a computation should be closely grouped so that it can, ideally, be stored in the same cache line of a CPU. On the other hand, unrelated data should be separated in such a way that it does not interfere with each other in order to avoid harmful effects, such as cache thrashing, where independent data sets depend on and thus compete for the same cache lines. Due to these two factors and the structure of our input data (variable(s) $\in$ equation(s) $\in$ block(s) $\in$ BES) we have decided to use a nested data structure, where each aforementioned component is modeled by a structured type. In this

layout, all data needed to evaluate one equation – the most frequent operation in our algorithm – is stored in a single structure resembling an equation, thus, accounting for good data locality. Clearly, this also provides good separation, and any further improvement would require machine dependent optimizations.

**Multi-Core Parallelization.** For the parallelization of Algorithm 1 on CPUs we employ the Cilk Plus framework provided by the Intel C/C++ compiler.[7] We chose Cilk Plus because it is well suited for problems with fine-grained data-parallelism and irregular structure, as shown in [12], which also is the case in our setting. Cilk Plus maintains a pool of workers, each of which is mapped to a thread during execution, and supports work stealing, i.e., taking over work that was initially assigned to another worker. This is in contrast to having to create, manage and delete threads manually, inducing a much higher overhead.

The key idea of our multi-core implementation is the parallelization of the inner for-loop, iterating over the equations, by employing Cilk Plus' parallel version of a for-loop, *cilk_for*. The reasons why we do not require any locking and further modifications are (i) the monotonicity of the Boolean function, as mentioned before, and (ii) the fact that the variable *variablesChanged* indicating a change of LHSs is only reset outside the parallel loop (Algorithm 1, line 4) and set uniformly (only to *true*) inside the parallel loop (Algorithm 1, line 8), i.e., any worker that has observed a changing variable assigns this value and, thus, the value cannot become inconsistent.

**Many-Core Data Structure.** Data structures used for CUDA accelerated computation must be specially designed for this purpose. They must support independent thread-local data processing and, at the same time, they must also be compact enough to enable good data locality. This is to avoid high latency device-memory access and generally to reduce the usage of device-memory bandwidth that may otherwise become a performance bottleneck [21].

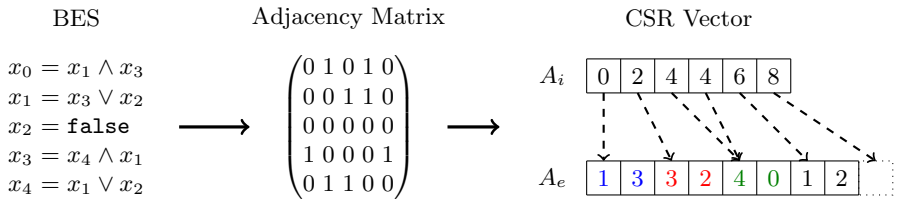



**Fig. 2.** Generation of adjacency list representation from BES.

A BES may be interpreted as a directed graph where the LHSs are vertices and the dependencies on the RHSs are edges. Such a graph can be encoded as an adjacency matrix and stored using two vectors in *compressed sparse row* (CSR)

[7] http://software.intel.com/en-us/articles/intel-compilers/

format, as depicted in Fig. 2. Since this data structure has been demonstrated to be efficient for graph based algorithms in the context of CUDA accelerated computation [3, 6, 15] we employ it to store BESs. Each vertex stores the following information: a unique index, its value along with a flag indicating whether the Boolean value is already computed, and the *type* of Boolean operator (conjunction or disjunction).

In more detail, our representation uses two one-dimensional arrays $A_i$ and $A_e$ to encode the directed graph. For all vertices $v_0$ to $v_n$, the sum of outgoing edges is stored in $A_i$, such that the number of outgoing edges from a particular vertex $v_j$ can be computed by $A_i[j+1] - A_i[j]$. The idea of this encoding is that the value of an element $A_i[j]$ serves as an index to the second array $A_e$. The array $A_e$ is a concatenation of ordered lists of target vertices of outgoing edges from individual graph vertices.

The sizes of the arrays $A_i$ and $A_e$ correspond to the sizes of the vertex set and the edge set of the graph, respectively. The array $A_i$ does not only store the indices to the array $A_e$ but also the aforementioned information (index, Boolean value, flag and type). Since the on-board memory of GPUs is very limited, we store this additional information in unused bits of $A_i$, thereby reducing the space requirement to 4 bytes per vertex.

**Many-Core Parallelization.** For our many-core parallelization we employ the CUDA framework, in which programs consist of two parts (i) *host code* that runs on the CPU and (ii) *device code* that runs on the GPU, the so called *kernels*. A kernel is executed concurrently in many independent data-parallel threads, where a group of threads, called a *warp*, executes on the same processor in a lock-step manner. When several warps are scheduled on a processor, memory latencies and pipeline stalls are hidden by switching to the execution of another warp. The CUDA framework is optimized for large numbers of simple parallel computations without explicit scheduling of threads.

For this reason the work-flow of our CUDA-accelerated fixed-point computation is divided into two parts. The host code, executing on the CPU, iterates over the outer loop, i.e., the loop over all BES-blocks, and calls the CUDA kernels executing on the GPU from within this loop. Each of the kernels is computing the solution for one LHS, i.e., evaluating one RHS. The CUDA kernel is invoked as long as LHSs change. Its pseudo code is provided in Algorithm 2.

This approach exposes fine-grained data-parallelism, requiring a dedicated thread to be executed for each vertex (LHS) of the graph (each item of Array $A_i$). Each thread first loads the data of a vertex from Array $A_i$ (stored in global memory) into a local copy (line 1) and checks if the corresponding LHS has already been solved (line 2). Then, it processes all immediate successors (loop on line 6), representing the RHS of the corresponding equation. The algorithm employs a lazy evaluation of the equations. In case that a value within a RHS immediately determines the value of the LHS (i.e., the RHS is a purely disjunctive term where at least one variable is *true*, or a purely conjunctive term where at least one variable is *false*), the loop is broken (line 10). Finally, the Boolean value of the evaluation of the RHS (stored in $mySucc.value$) is compared to the

**Algorithm 2**: FIXEDPOINT kernel – run in parallel for each LHS variable

```
   Input  : g(lobal)A_e, g(lobal)A_i, fixedPointFound
 1 myVertex ← gA_i[tid]          // tid ∈ [0,1,...,n] where n = sizeof(BES-block)
 2 if myVertex.solved then
 3     return
 4 first ← myVertex.index
 5 last ← gA_i[tid + 1].index
 6 foreach index ∈ first, ..., last do
 7     targetVertex ← gA_e[index]
 8     mySucc ← gA_i[targetVertex]
 9     if mySucc.value ≠ myVertex.type then        // type ∨ ≡ 0 and type ∧ ≡ 1
10         break
11 if myVertex.value ≠ mySucc.value then
12     myVertex.solved ← true
13     myVertex.value ← mySucc.value
14     gA_i[tid] ← myVertex
15     fixedPointFound ← false
```

Boolean value stored in the corresponding LHS (line 11). If the two values differ, the result of the evaluation is assigned to the respective LHS, written back to Array $A_i$ (line 14), and the fixed point flag is set to *false* indicating that the fixed point is not yet reached.

**Many-Core Optimizations.** For the GPU-based implementation we have experimented with two optimizations.

The first one is the so called "intra-warp fixed point iteration." It is based on the observation that all threads within a warp have to load the required data from global memory into local copies. All operations are performed on the local copies, which are written back to global memory at the end of the execution of the warp. This means that updated LHSs do not become visible to other threads until the next iteration step and, thus, changes can only be propagated one step per iteration. The intra-warp fixed point iteration is intended to increase the number of propagations by performing multiple iterations on the equations bundled in a warp and thereby propagating changes of LHSs within this warp.

The second optimization is an extension to the intra-warp fixed point iteration. It utilizes the GPU's shared memory, which provides a fast local memory for single threads or warps, allowing the intermediate storage of data. We use this shared memory to optimize the execution of the kernel by copying the LHS variables contained in a RHS from global memory to shared memory. When the data of a LHS is required by the kernel, the copy in shared memory is utilized instead of the one in global memory. When the kernel returns, the copy is written back from shared to global memory. However, the indirection on line 8 potentially requires further LHSs; this data can either be read from global memory as

before or also be copied to shared memory. This reduces access to global memory but requires additional load and store operations before and after each thread invocation.

## 4 Experimental Evaluation

In this section we experimentally evaluate the scalability of our parallel approach in its CPU and GPU variants and demonstrate the competitiveness of the GPU version when compared to the optimized sequential algorithm, using the VLTS benchmark suite.[8] We double-check the correctness of our implementations by observing that the results obtained from our sequential and parallel algorithms match those computed by CADP's sequential "bes_solve" tool [24].

To provide an outlook on the generality of our results, we also extend our evaluation using randomly generated BESs, thus analyzing the influence of the specific way in which BESs are derived from model checking problems. Furthermore, we evaluate the structure and density of the BESs generated from the benchmark suite. Besides the run-time based comparison we provide insights into the specifics of BESs in the context of model checking, i.e., we present heuristics for the order in which equations are to be solved, which may yield significant speed-ups for BES resolution in this context.

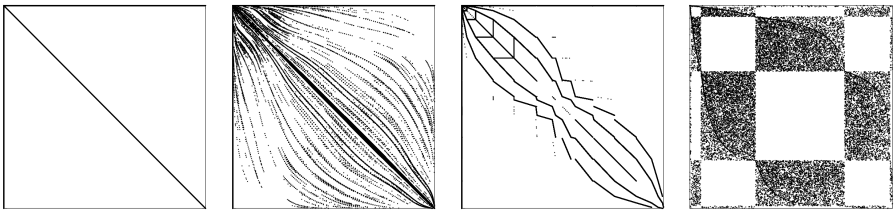
**Benchmark Suite.** Our experiments were conducted using the VLTS benchmark suite that was compiled within a joint project of CWI[9] and INRIA[10]. It consists of 40 examples from academia and industry, provided as LTSs with numbers of states ranging from 289 up to 33,949,609. The four largest examples of the benchmark were solved for the first time in 2005 [16].

**Table 1.** $\mu$-Formulae of Properties

| Property | $\mu$-formula |
|---|---|
| Deadlock freedom | $\nu X.([-]X \wedge \langle - \rangle true)$ |
| Livelock | $\mu X.(\langle - \rangle X \vee \nu Y.(\langle \tau \rangle Y))$ |

The backgrounds of the benchmark examples vary greatly; thus, different properties may be checked for individual examples. For our evaluation we use two representative properties, namely deadlock freedom and livelock, which can be checked for all examples of the benchmark suite (cf. Table 1 for their formalization). For these properties, results are also provided by the authors of the benchmark, thus allowing a direct verification of the correctness of the results obtained by our implementations.

[8] http://www.inrialpes.fr/vasy/cadp/resources/benchmark_bcg.html
[9] http://www.cwi.nl/
[10] http://vasy.inria.fr/



(a) Example 10 (b) Example 22 (c) Example 34 (d) Rnd2

**Fig. 3.** Visualization of benchmark examples as adjacency matrices.

The images of some exemplary BESs, as depicted in Fig. 3, show the significant variance in structure and density of the LTSs provided in the benchmark. The images are visualizations of the adjacency matrices of the respective BESs, with their origins, i.e., the LTSs' initial states, displayed on the top left.

In contrast to intuition, our experiments suggest that this information about structure and density does not usefully correlate with the scalability and/or run-time performance of our approach. This is the case for the following reasons: (i) the run-time generally depends on the question whether the property, for which the LTS is checked, is fulfilled or violated; (ii) our approach does not favor local propagation of changing variables, but globally propagates all possible changes during an iteration; (iii) our algorithms perform best in cases that expose large numbers of concurrent changes rather than sequential chains of changes, which in addition to a BES's structure depends on the initial distribution of terminal values. Unfortunately, none of these factors can be estimated sensibly nor be extracted from a BES in reasonable time, i.e., when compared to the time it takes to solve the BES.

**Hardware.** Our experiments were carried out on different hardware platforms for (i) the CPU and (ii) the GPU version of the implementation: (i) two interconnected Intel XEON E7-4830 processors @ 2,13 GHz, each with 8 physical cores and Hyper-Threading enabled (i.e., a total of 32 logical PUs) and 64 GB DDR3 RAM @ 1333 MHz, running Windows 7 64-bit, and (ii) one AMD Phenom II X4 940 processor @ 3,0 GHz, 8 GB DDR2 RAM @ 1066 MHz along with (a) one NVIDIA GeForce GTX 280 GPU with 1 GB of global memory, 16KB of shared memory per multiprocessor, providing 240 CUDA cores, and (b) one NVIDIA GeForce GTX 480 GPU with 1.5 GB of global memory, 48KB of shared memory per multiprocessor, providing 480 CUDA cores, running Debian 6.0 64-bit on kernel 2.6.39. Although the systems use different CPU types this fact does not affect our results since we did not evaluate a hybrid approach but only pure CPU and GPU versions of the respective algorithms.

**Overview.** Table 2 provides an overview of the run-times of the following algorithms: (i) the optimized sequential workset-based CPU implementation (the baseline for our comparison), (ii) the parallel Cilk Plus based CPU implementation, (iii) the unoptimized GPU implementation without any optimization, (iv)

**Table 2.** Overview of Run-Times for CPU and GPU Implementations [ms]

| Algorithm | | Benchmark Example | | | | | | | | | Random | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 10 | 21 | 22 | 31 | 32 | 33 | 34 | 35 | 39 | Rnd1 | Rnd2 |
| CPU | (i) sequential | 1 | 19 | 18 | 573 | 475 | 737 | 1 | 704 | 901 | 3891 | 7801 |
| | (ii) parallel | 2538 | 77 | 611 | 1564 | 1786 | 2764 | 279 | 4325 | 8170 | 7966 | 40576 |
| GPU GTX 280 | (iii) unoptimized | 1336 | 17 | 68 | 217 | 113 | 359 | 51 | 242 | 290 | 350 | 1840 |
| | (iv) intra-warp | 104 | 22 | 69 | 320 | 149 | 528 | 52 | 404 | 344 | 493 | 2594 |
| GPU GTX 480 | (iii) unoptimized | 703 | 6 | 33 | 75 | 46 | 105 | 6 | 98 | 125 | 178 | 992 |
| | (iv) intra-warp | 40 | 7 | 28 | 109 | 63 | 157 | 6 | 152 | 158 | 248 | 1391 |
| | (v) shared mem | 38 | 40 | 59 | 659 | 341 | 862 | 48 | 190 | 227 | 315 | 1800 |

the GPU implementation with intra-warp iteration, and (v) the GPU implementation utilizing shared memory. In case of the GTX 280 GPU, we omitted the results for (iv), the shared memory implementation, since this GPU does not provide a sufficient amount of shared memory for this optimization. Note that in the case of parallel CPU implementation we list the best runtimes available among the numbers of cores that have been utilized.

Because of layouting limitations, we restrict our selection of benchmark examples in Table 2 to those for which the run-time of the GPU implementation is sensibly measurable, i.e., larger than 5 [ms]; nonetheless we conducted our experiments for the entire benchmark suite. The numbering of the benchmark examples refers to their position in the table provided on the VLTS website,[11] which is sorted in ascending order relative to the number of states of the LTS; thus, Example 10 is *vasy_25_25*, Example 21 is *vasy_166_651*, Example 22 is *cwi_214_684*, Example 31 is *vasy_2581_11442*, Example 32 is *vasy_4220_13944*, Example 33 is *vasy_4338_15666*, Example 34 is *vasy_6020_19353*, Example 35 is *vasy_6120_11031* and Example 39 is *vasy_12323_27667*. In this naming scheme, the first number is the number of states divided by 1000, and the second number is the number of transitions divided by 1000.

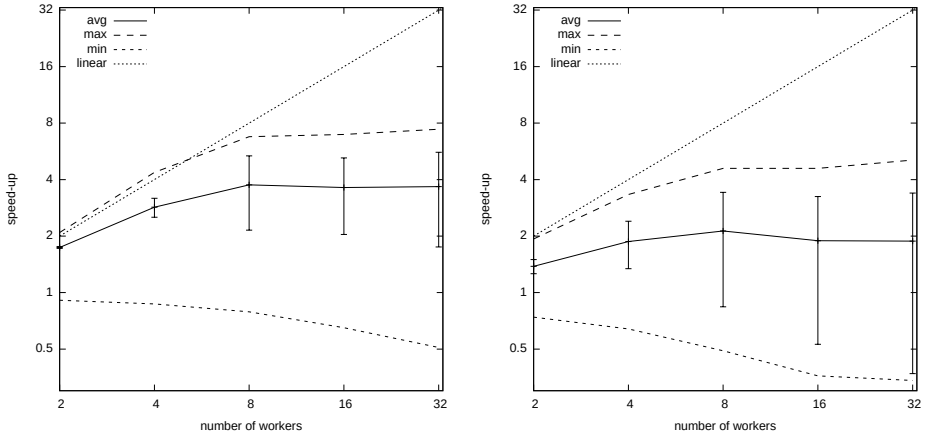
Furthermore, all examples in Table 2 are checked for the deadlock freedom property since only eight of the 40 LTSs contain livelocks. Nonetheless, our general statements about scalability and competitiveness have been evaluated and are valid for the entire benchmark suite. To check whether the specific ways in which BESs were generated for and included in the VLTS benchmark have an influence on our performance results, we extend our evaluation to randomly generated BESs. We evaluate a total of five random examples with the number of states ranging from 1 to 10 million; Rnd1 and Rnd2 are two representatives illustrating our observations for this class of BESs.

We omit memory consumptions of our implementations in the table, since (i) our parallel versions operate on a static data structure that is linear in the size of the input BES (ranging from approximately 90 KB up to 4.5 GB) and (ii) it

[11] http://cadp.inria.fr/resources/benchmark_bcg.html#section-5

is not our aim to evaluate or optimize memory efficiency within the scope of this paper, especially since all benchmark examples easily fit our systems' memory.

**Multi-Core Performance.** The results in Table 2 clearly show that our multi-core implementation is outperformed significantly by the optimized sequential baseline. The reason for this is the low total number of parallel PUs (32 logical cores) and, thus, the computational overhead of the fixed point iteration is too large when compared to the amount of productive work and cannot be compensated by parallel processing power. This observation is supported by the two graphs in Fig. 4, which show the overall scalability of our CPU-based approach for an increasing number of parallel workers. This result is in accordance with [27] and extends their results to our much larger benchmark suite.




(a) Deadlock freedom (b) Livelock

**Fig. 4.** Scalability of our multi-core implementation.

The data for the two graphs in Fig. 4 is based on the median values of 10 runs for each of the 40 benchmark examples. It is evaluated separately for the two properties: deadlock freedom (Fig. 4(a)) and livelock (Fig. 4(b)). The average scalability (avg) is compiled from all 40 benchmark examples and is below linear for both properties. However the scalability is observable for up to eight workers, which corresponds to the number of physical cores of one CPU in our system. For the sake of completeness we also include the standard deviation for the average scalability, along with maximum (max) and minimum (min) scalability.

It is important that the shape of the two graphs, which suggests better scalability for LTSs that have been checked for the no deadlock property, is affected by the fact that there are 20 examples containing deadlocks, while only 8 examples contain livelocks. In the case of the trivial examples, i.e., those that do not contain deadlocks/livelocks, our algorithm needs to perform only one iteration, which has significant impact on scalability.

The super-linear speed-up in Fig. 4(a) can be explained by the parallel execution of workers. As the Cilk Plus framework may schedule the evaluation order of equations differently from the order in the BES, this may lead to a faster propagation of updated LHSs, requiring less iterations and thus result in the seemingly above linear boost in performance.

**Many-Core Performance.** The evaluation of our many-core implementation is aimed more at the competitiveness of our approach when compared to the optimized sequential baseline than at its scalability. Indeed, the scalability analysis is more difficult than for the multi-core implementation because we had to use different GPU devices that are not comparable with respect to some important specifications. Not only did the number of CUDA cores double from the GTX 280 to the GTX 480, but also the clock rate and the available amount of memory increased significantly. For this reason we did not evaluate the scalability aspect beyond the scope provided in Table 2, which shows a significant boost in performance for the GTX 480. Further evaluations of scalability, e.g., on clusters of GPUs, are subject to future work.

The main limitation of the GPU parallelization is the length of the chain of propagations of LHS values. Example 10 in the benchmark suite contains an artificially long chain of dependencies from the initial state to the last state (cf. Fig. 3(a)). For this example, the number of iterations for the unoptimized version of our many-core implementation is equal to the number of states , yet the example is a prime candidate to benefit from the intra-warp iteration as the changes can be propagated ideally within the equations of a warp. However, the remaining benchmark examples do not have such an extreme structure and, therefore, the intra-warp iteration, on average, does not provide any advantage but rather induces overhead as the comparison of run-times in Table 2 shows.

Since the efficiency of our shared memory optimization is tightly coupled to the intra-warp iteration, it can only improve the performance of the many-core implementation in those cases in which the intra-warp iteration actually works. Due to this reason, the results for this optimization in Table 2 are, not surprisingly, even worse than for the intra-warp iteration because the transfer times from and to shared memory degrade the run-time performance even further. Moreover, in order to use the shared memory, the required data (i.e., the part of a BES corresponding to a block) has to fit the limited size of the GPUs shared memory. The size of the data that has to be stored in the shared memory is given by the block size, the number of vertices in one block and the number of their successors. In case the average out-degree (i.e., the average number of RHS variables per equations) is high, we have to decrease the group size. This can lead to underutilization or low occupancy of the individual multiprocessors and, thus, significantly reduces the performance of our algorithm.

As documented in Table 2, our GPU implementation of BES resolution provides significant speed-ups for most cases of the benchmark examples and especially for the randomly generated BESs. Surprisingly, the GPU implementation with no optimizations yields the best results, since in most cases the structure of the inspected BESs does not allow one to benefit from our optimizations.

**Table 3.** Impact of Heuristics [Total Number of Iterations]

| Heuristic | Benchmark Example | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 4 | 5 | 7 | 10 | 15 | 16 | 18 | 19 | 21 | 22 | 25 | 27 | 30 | 31 | 32 | 33 | 35 | 37 | 38 | 39 |
| Original | 64 | 19 | 7 | 25219 | 19 | 33 | 23 | 18 | 33 | 208 | 24 | 7 | 56 | 32 | 23 | 34 | 33 | 20 | 29 | 29 |
| Vectorized | 64 | 19 | 7 | 25219 | 23 | 37 | 23 | 19 | 37 | 213 | 24 | 7 | 56 | 37 | 25 | 37 | 34 | 20 | 29 | 29 |
| Reverse | 2 | 4 | 3 | 2 | 7 | 8 | 8 | 5 | 8 | 8 | 10 | 2 | 3 | 7 | 4 | 6 | 4 | 5 | 5 | 5 |
| Random | 20 | 9 | 5 | 25219 | 10 | 12 | 6 | 11 | 11 | 63 | 7 | 3 | 6 | 8 | 5 | 8 | 16 | 10 | 9 | 9 |

**Ordering Heuristics.** Table 3 provides a comprehensive overview of the total number of iterations for those examples of the benchmark, which have been checked for deadlocks and for which the initial approximation is not equal to the final solution, i.e., the total number of iterations is larger than one. Even though the available number of PUs increases with each hardware generation, it is still far from the point where a full iteration step can be computed fully in parallel. Thus, the processing order of equations within a block has a significant influence on the total number of iterations needed to compute the fixed point. Yet, our evaluation yields an interesting insight for an ideal "vectorized" parallelization, assuming that a fully parallel iteration step is possible; we model this by delaying the visibility of a changed LHSs until the next iteration step. Note that the lack of a suitable hardware architecture allowing such fully-parallel processing is the reason why we list the number of iterations instead of run-times in Table 3. Naturally the number of iterations is proportional to the run-times.

Our evaluation shows that this "Vectorized" approach does not increase the total number of iterations significantly, when compared to the "original" ordering, where equations are evaluated in their given order and changes of LHSs are directly visible in the following computations of the iteration (cf. Table 3). This result demonstrates that the penalty for a fully parallel computation is negligible regarding the total number of iterations needed to reach the fixed point.

As the application of advanced heuristics would require preprocessing of the data – causing a potentially high computational overhead – we restrict our evaluation to two simple cases that do not introduce any overhead. The first heuristics is called "Reverse" in Table 3 and takes the reverse order of equations within a BES-block, as proposed in [27]. It yields a significant improvement with respect to the total number of iteration needed to compute the fixed point (cf. Table 3). Yet, according to our observations, this heuristics only works for the examples generated from the benchmark's LTSs, but not for randomly generated BESs. This could be due to the way in which state spaces are enumerated in the CADP toolset, which in turn determines the order of equations in the VLTS examples.

The second heuristics, called "Random" in Table 3, is the randomized evaluation of equations within a BES-block. In our observations, this heuristics leads to a decrease in the number of iterations needed to solve a BESs when compared to the given ("Original") ordering. This result is of practical relevance as our parallel implementations rely on parallelizations in which the order of RHS

evaluations is not under our control, but is determined by the runtime environment of CUDA and Cilk Plus. Thus, we expect an additional performance boost rather than a degradation, due to the parallelization frameworks.

## 5 Conclusions and Future Work

We implemented an approach to the parallel resolution of BESs on multi- and many-core systems, and evaluated them with respect to scalability and run-time performance in comparison to an optimized sequential algorithm. Our measurements confirm the scalability results of [27] for our multi-core implementation, yet this implementation's overall performance is not competitive when compared to our optimized sequential implementation. In contrast, the utilization of many-core hardware, not considered in [27], yields a significant speed-up and outperforms the optimized sequential implementation for most instances of the benchmark by almost one order of magnitude. Furthermore, the scalability of our many-core approach with respect to increasing numbers of PUs was demonstrated by us by (i) comparing the multi-core and many-core implementations and (ii) evaluating the many-core implementation for two GPU cards with 240 and 480 CUDA cores, respectively.

Future work will include further evaluation of the scalability results of the many-core implementation, e.g., by its distribution over a cluster of GPUs. Since BESs are not restricted to model checking, it is also promising to evaluate input BESs from other applications, such as data-flow analyzes in optimizing compilers [10]. Furthermore, the recently proposed many-core parallelization of graph algorithms [25] should be evaluated with respect to its suitability and potential impact on our work.

*Acknowledgments.* The second author has been partially supported by the Czech Grant Agency grants No. 102/09/H042 and GAP202/11/0312. We thank the anonymous reviewers for their valuable comments.

## References

1. H. R. Andersen. Model Checking and Boolean Graphs. *Theoret. Comp. Sc.*, 126(1):3–30, 1994.
2. G. R. Andrews. *Foundations of Multithreaded, Parallel, and Distributed Programming*. Addison-Wesley, 2000.
3. J. Barnat, P. Bauch, L. Brim, and M. Češka. Computing Strongly Connected Components in Parallel on CUDA. In *IPDPS*, pages 544–555. IEEE, 2011.
4. J. Barnat, P. Bauch, L. Brim, and M. Češka. Designing Fast LTL Model Checking Algorithms for Many-Core GPUs. *To app. in J. of Par. and Distrib. Comp.*, 2012.
5. J. Barnat, L. Brim, and P. Ročkai. Scalable Multi-core LTL Model-Checking. In *SPIN*, volume 4595 of *LNCS*, pages 187–203. Springer, 2007.
6. J. Barnat, L. Brim, M. Češka, and T. Lamr. CUDA Accelerated LTL Model Checking. In *ICPADS*, pages 34–41. IEEE, 2009.

7. B. Bollig, M. Leucker, and M. Weber. Local Parallel Model Checking for the Alternation-Free $\mu$-Calculus. In *SPIN*, volume 2318 of *LNCS*, pages 128–147. Springer, 2002.
8. R. E. Bryant. Symbolic Boolean Manipulation with Ordered Binary-Decision Diagrams. *ACM Comput. Surv.*, 24(3):293–318, 1992.
9. E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. MIT Press, 1999.
10. M. d. M. Gallardo, C. Joubert, and P. Merino. On-the-Fly Data Flow Analysis Based on Verification Technology. In *COCV*, volume 190 of *ENTCS*, pages 33–48, 2007.
11. E. A. Emerson. Temporal and Modal Logic. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 16, pages 995–1072. Elsevier, 1990.
12. J. Ezekiel, G. Lüttgen, and R. Siminiceanu. To Parallelize or to Optimize? *J.of Log. and Comput.*, 21:85–120, 2011.
13. M. Garland and D. B. Kirk. Understanding Throughput-Oriented Architectures. *Commun. ACM*, 53:58–66, 2010.
14. O. Grumberg, T. Heyman, and A. Schuster. Distributed Symbolic Model Checking for $\mu$-Calculus. *Form. Methods Syst. Des.*, 26:197–219, 2005.
15. P. Harish and P. J. Narayanan. Accelerating Large Graph Algorithms on the GPU Using CUDA. In *HiPC*, volume 4873 of *LNCS*, pages 197–208. Springer, 2007.
16. F. Holmén, M. Leucker, and M. Lindström. UppDMC: A Distributed Model Checker for Fragments of the mu-Calculus. In *PDMC*, volume 128 of *ENTCS*, pages 91–105. Elsevier, 2005.
17. G. J. Holzmann and D. Bosnacki. Multi-Core Model Checking with SPIN. In *IPDPS*, pages 1–8. IEEE, 2007.
18. C. Joubert and R. Mateescu. Distributed Local Resolution of Boolean Equation Systems. In *PDP*, pages 264–271. IEEE, 2005.
19. D. Kozen. Results on the Propositional mu-Calculus. *Theoret. Comp. Sc.*, 27:333–354, 1983.
20. A. Laarman, J. van de Pol, and M. Weber. Boosting Multi-Core Reachability Performance with Shared Hash Tables. In *FMCAD*, pages 247–255. IEEE, 2010.
21. A. Lefohn, J. M. Kniss, and J. D. Owens. Implementing Efficient Parallel Data Structures on GPUs. In *GPU Gems 2*, pages 521–545. Addison-Wesley, 2005.
22. M. Leucker, R. Somla, and M. Weber. Parallel Model Checking for LTL, CTL*, and $L^2_\mu$. In *PDMC*, volume 89 of *ENTCS*, pages 4–16, 2003.
23. A. H. Mader. *Verification of Modal Properties Using Boolean Equation Systems*. PhD thesis, Technische Universität München, Germany, 1997.
24. R. Mateescu. CAESAR_SOLVE: A Generic Library for On-the-Fly Resolution of Alternation-free Boolean Equation Systems. *STTT*, 8(1):37–56, 2006.
25. D. Merrill, M. Garland, and A. Grimshaw. Scalable GPU Graph Traversal. In *PPoPP*, pages 117–128. ACM, 2012.
26. B. Nichols and D. Buttlar J. P. Farrell. *PThreads Programming*. O'Reilly, 1996.
27. J. van de Pol and M. Weber. A Multi-Core Solver for Parity Games. In *PDMC*, volume 220 of *ENTCS*, pages 19–34. Elsevier, 2008.
28. A. Sailer. Utilizing And-Inverter Graphs in the Gaussian Elimination for Boolean Equation Systems. Master's thesis, Hochschule Regensburg, Germany, 2011.
29. A. Tarski. A Lattice-Theoretical Fixpoint Theorem and its Applications. *Pacific J. of Math*, 5(2):285–309, 1955.