1 Motivation

Hardware accelerators (currently Graphical Processing Units or GPUs) are an important component in many existing high-performance computing solutions [5]. Their growth in variety and usage is expected to skyrocket [1] due to many reasons. First, GPUs offer impressive energy efficiencies [3]. Second, when properly programmed, they yield impressive speedups by allowing programmers to model their computation around many fine-grained threads whose focus can be rapidly switched during memory stalls. Unfortunately, arranging for high memory access efficiency requires developed computational thinking to properly decompose a problem domain to gain this efficiency. Our work currently addresses the needs of the CUDA [5] approach to programming GPUs. Two important classes of such rules are bank conflict avoidance rules that pertain to CUDA shared memory and coalesced access rules that pertain to global memory. The former requires programmers to generate memory addresses from consecutive threads that fall within separate shared memory banks. The latter requires programmers to generate memory addresses that permit coalesced fetches from the global memory. In previous work [6], we had, to some extent addressed the former through SMT-based methods. Several other efforts also address bank conflicts [7, 8, 4]. In this work, we address the latter requirement—detecting when coalesced access rules are being violated.

Table 1. Performance Comparison between Bank Conflicts and Memory Coalescing Violations: 100000 iterations of: Read an int from shared memory; Write back to global memory

<table>
<thead>
<tr>
<th>#Threads</th>
<th>1024</th>
<th>512</th>
<th>256</th>
<th>128</th>
<th>64</th>
<th>32</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.K.</td>
<td>0.035587</td>
<td>0.035589</td>
<td>0.017809</td>
<td>0.010054</td>
<td>0.008529</td>
<td>0.008304</td>
<td></td>
</tr>
<tr>
<td>M.C.V.</td>
<td>0.417909</td>
<td>0.417933</td>
<td>0.208980</td>
<td>0.104513</td>
<td>0.052281</td>
<td>0.026188</td>
<td>0.013126</td>
</tr>
</tbody>
</table>

Table 2. Execution times in seconds with and without Memory Coalescing: 10000 iterations of: Read an int from global memory; Increment; Write back to global memory

<table>
<thead>
<tr>
<th>#Threads</th>
<th>2^24</th>
<th>2^20</th>
<th>2^16</th>
<th>1024</th>
<th>256</th>
<th>32</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coalescing(s)</td>
<td>14.210834</td>
<td>0.890957</td>
<td>0.055718</td>
<td>0.001061</td>
<td>0.000605</td>
<td>0.000580</td>
<td>0.000583</td>
</tr>
<tr>
<td>No-Coalescing(s)</td>
<td>128.674240</td>
<td>8.349093</td>
<td>0.520744</td>
<td>0.007005</td>
<td>0.001779</td>
<td>0.000994</td>
<td>0.000602</td>
</tr>
</tbody>
</table>
The motivation for detecting memory coalescing violations is provided by Table 1 and Table 2. These results demonstrate through experimental runs on actual CUDA hardware, that the efficiency of CUDA programs can be significantly influenced by performance flaws. Table 1 shows memory coalescing violations can take up to 10 times the runtime of bank conflicts, which leads to the conclusion that memory coalescing violations have more effects than bank conflicts on performance. Besides, Table 2 shows hand-written kernels that follow/violate the coalescing rules can differ by an order of magnitude in performance. Although these are small examples, they capture how performance degradations such as non-coalesced and bank-conflicting accesses may get strewn across one’s code, with each occurrence giving rise to the same degree of performance degradation. Since GPU are streaming architectures, they are memory bandwidth-bound for all but the most trivial of problems. This immediately tells us that the additive effect of each performance degradation will severely degrade the whole kernel. Besides, another reason we utilize these small examples is to eliminate the effects of other performance flaws as much as possible and therefore we are able to measure the influences accurately. Our contribution is to ferret out each such performance degrading occurrence not easily discerned by conventional tools or by code inspection.

This paper analyzes different cases of memory coalescing violations and derives an approach to detect such performance flaws. Our approach has been implemented in our tool PUG [6]—a symbolic verifier for CUDA kernels based on Satisfiability Modulo Theories (SMT [9]).

2 Details of Bank Conflict and Coalescing

To provide context for our problem, we briefly introduce some basic concepts of GPUs and CUDA C. More details can be obtained through [2].

GPUs consist of a number of streaming multiprocessors (SM), with each running up to thousands of parallel threads concurrently. These threads are
organized in block granularity and each block is further divided into warps which each consist of 32 consecutive threads. Correspondingly, a half-warp consists of 16 consecutive threads. Each warp of threads are co-scheduled on a SM and then execute the same instruction in a given clock cycle (SIMD fashion). \texttt{syncthreads()} guarantees that every thread in the block has completed instructions prior to \texttt{syncthreads()} before the hardware will execute the next instruction on any thread. \textbf{Global memory} is the memory allotted to the entire GPU. All threads can read and write to global memory. \textbf{Shared memory} is a fast work-space for threads within a block. It is worth mentioning that the shared memory is at least 100 times faster than global memory. The CUDA memory access model is shown in Fig. 1.

Under memory coalescing, \textbf{global memory} accesses by a half-warp of threads are combined into a single, wide memory access. This results in a bandwidth improvement of up to 16 times per half-warp—a figure that easily adds up. Given that each global memory access takes about 400 − 600 clock cycles, the difference is between 6400 − 9600 clock cycles without coalescing down to 400 − 600 clock cycles with coalescing.

To ensure memory coalescing, the memory request for a half-warp must satisfy the following conditions:\footnote{These conditions are required by GPUs with Compute Capability 1.0 and 1.1}

\begin{itemize}
  \item Type Consistency Rule: the size of the words accessed by the threads must be 4, 8, or 16 bytes.
  \item Sequential Access Rule: threads must access the words in sequence: The $k^{th}$ thread in the half-warp must access the $k^{th}$ word.
\end{itemize}

Note that not all threads are required to participate. If the half-warp does not meet these requirements, 16 separate memory transactions are issued.

### 3 Detection of Memory Coalescing Violations

Memory coalescing violations are either \textit{type consistency} or \textit{sequential access} violations. A type consistency violation occurs when the size of the words accessed is not 4, 8, or 16 bytes (not one of \textit{int}, \textit{int2}, \textit{int4} or their equivalents). For example, a kernel prototype declared as

\begin{verbatim}
__global__ void violation(int3 * data, int n, int iter)
\end{verbatim}

results in a coalescing violation. Type checking, when feasible, achieves this check. Sequential access violations occur when the $k^{th}$ thread in the \textbf{half-warp} does not access the $k^{th}$ word in global memory, as in

\begin{verbatim}
1 __global__ void violation(int * data, int n, int iter)  
2 { int idx = threadIdx.x;  
3     if(idx%2==0)  
4         for (int i = 0; i < iter; ++i)  
5             data[idx+1] = data[idx] + 1;
\end{verbatim}
At Line 5, thread \textit{idx} reads \textit{data} at \textit{idx} and then writes \textit{data} at \textit{idx+1}. The \textit{read} access strictly follows the sequential access rule. However, the \textit{write} access breaks the sequential access rule in that thread \textit{idx} writes \textit{data} at \textit{idx+1}. A similar violation occurs at Line 8. It is interesting to consider whether memory accesses at Line 9 violates the sequential access rule. Since memory \textit{data[idx + 16, \cdots , idx + 31]} accessed by \textit{data} by a half-warp of threads is still in an aligned 64-byte memory segment, such an access is still a sequential access. As a result, there is no sequential access violation for both \textit{read} and \textit{write} accesses at Line 9.

Based on the above observations coupled with the fact that memory coalescing is organized for every 16 threads, sequential access violation can be detected by checking this assertion across the entire kernel:

\begin{equation}
\text{Index of array \%16 == thread ID \%16}
\end{equation}

Our approach to detect memory coalescing violations is as follows:

\begin{itemize}
\item Detect Type Consistency Violations
\item Detect Sequential Access Violation:
\begin{itemize}
\item Each access to global memory is encoded as an \textit{unsat} problem, also considering the path conditions leading to the access. Essentially we check for $\text{Index}_{\text{array}} \%16 \neq \text{threadID} \%16$.
\item We then obtain a disjunction of all access encodings: $\lor (\text{array}_i \mod 16 \neq \text{threadId} \mod 16)$
\item If \textit{unsat}, all memory accesses are coalesced; else we obtain a violation witness.
\end{itemize}
\end{itemize}

Our procedures for encoding CUDA C to SMT are described in detail in [6] and the workflow of PUG is illustrated in Fig. 2.

4 Experiment

Our proposed approach has been implemented in PUG [6]. To evaluate the effectiveness and efficiency of our approach, experiments involving different cases of violations (or non-violations) have been conducted, as shown in the following kernel functions.

```c
void _global_ kernel1 (int *data)
{
    int idx = threadIdx.x+1;
    data[idx] = data[idx] + 16;
}
// return sat, violation: offset of index is 1
```

```c
void _global_ kernel2 (int *data)
{
    int idx = threadIdx.x;
    data[idx] = data[idx+16] + 16;
}
// return unsat, no violation:
// idx+16 \% 16=idx
```
void __global__ kernel3 (int *data) {
    int idx = threadIdx.x;
    data[n-idx] += 16;
} // return sat, violation:
// ∃ idx, n-idx % 16 ≠ threadIdx.x

void __global__ kernel4 (int *data) {
    int idx = threadIdx.x+1;
    data[idx-1] += 16;
} // return unsat, no violation
// idx-1=threadIdx.x+1-1=threadIdx.x

In addition to the above case-by-case violations (non-violations), complicated kernel functions (e.g. containing multiple violation cases, as the one shown in kernel 2) are also run by PUG. PUG catches all these violations (or non-violations) efficiently with a negligible runtime: < 0.1. The efficiency is derived from the fact that we only need to consider indices of array involved. All other information in the kernel function is discarded, which significantly reduces computations performed by the SMT solvers.

5 Conclusion and Future Work

The paper proposed an approach to detect memory coalescing violations and experimental results illustrate the efficiency and effectiveness of our proposed method. With the corporation of our proposed method, PUG now can detect race conditions, bank conflicts and memory coalescing violations efficiently.

Since there are not much work focusing on functional equivalence checking for CUDA kernels (concurrent programs), an attractive direction to evolve PUG is to incorporate functional equivalence checking whose major work is to check the equivalence between CUDA kernels and optimized CUDA kernels.
References

2. Cuda programming guide version 3.0.
3. Dally, W.: (2010), keynote at SC 2010