

ABSTRACT

The Greatest Common Divisor (GCD) is a fundamental arithmetic operation crucial for numerous applications, including cryptography and digital signal processing. However, conventional software implementations on embedded systems, particularly on resource-constrained platforms like FPGA-based MicroBlaze V Systems-on-Chip, face significant performance challenges due to their iterative nature and sequential execution, leading to escalating execution times. To address these limitations, this thesis presents a custom FPGA-based GCD hardware accelerator, implementing the Euclidean algorithm, integrated with a MicroBlaze V soft processor via the AXI4-Lite interface. This dedicated hardware accelerator offloads the computational burden from the processor and leverages pipelined processing to maintain nearly constant execution times.

Experimental evaluations conducted on a Digilent Basys3 board reveal a stark performance contrast between the two approaches. While the software baseline exhibits an exponential increase in execution time, reaching 82,192 clock cycles for a 12-digit GCD, the proposed hardware accelerator maintains an approximate execution time of 206-4301 clock cycles across varying numbers of input digits (from 2 to 12). This demonstrates that the hardware accelerator achieves a remarkable performance improvement of up to 19 times for 12-digit GCD computations compared to the software implementation. Although the hardware-accelerated design utilizes approximately 1.98 times more Look-Up Tables (LUTs) and 1.58 times more Flip-Flops (FFs) compared to the software-only baseline, this resource overhead is justified by the substantial performance gains. These results validate the effectiveness of the FPGA-based hardware solution in significantly enhancing computational throughput in resource-constrained embedded systems, establishing a promising foundation for future performance optimizations and scalable accelerator designs for arithmetic primitives.

Keywords: Greatest Common Divisor, FPGA, MicroBlaze V, Hardware Accelerator, Embedded Systems, Performance Optimization, AXI4-Lite interface.

Greatest Common Divisor (GCD) atau Faktor Persekutuan Terbesar merupakan operasi aritmatika dasar yang sangat penting untuk berbagai aplikasi, seperti kriptografi dan pemrosesan sinyal digital. Namun, implementasi perangkat lunak konvensional pada sistem terbenam (embedded systems), khususnya pada Sistem-on-Chip (SoC) MicroBlaze V berbasis FPGA, sering kali menghadapi kendala performa akibat waktu eksekusi yang meningkat secara signifikan seiring bertambahnya jumlah angka dan lebar bit. Untuk mengatasi tantangan tersebut, penelitian ini menghadirkan akselerator perangkat keras GCD berbasis algoritma Euclidean yang terintegrasi dengan prosesor lunak (soft processor) MicroBlaze V melalui antarmuka AXI4-Lite. Akselerator khusus ini dirancang untuk mengambil alih beban komputasi dari prosesor utama dan memanfaatkan pemrosesan pipelined, sehingga waktu eksekusi dapat dipertahankan hampir konstan.

Hasil evaluasi eksperimental pada Board Digilent Basys3 menunjukkan perbedaan kinerja yang signifikan antara kedua pendekatan. Implementasi perangkat lunak menunjukkan peningkatan waktu eksekusi secara eksponensial, hingga mencapai 82.192 siklus clock untuk GCD 12-digit. Sebaliknya, akselerator perangkat keras yang diusulkan mampu mempertahankan waktu eksekusi sekitar 206-4301 siklus clock untuk berbagai jumlah digit input (2 hingga 12 digit). Hal ini membuktikan bahwa akselerator perangkat keras memberikan peningkatan kinerja hingga 19 kali lipat pada komputasi GCD 12-digit dibandingkan implementasi perangkat lunak. Walaupun desain berbasis perangkat keras ini menggunakan sekitar 1,98 kali lebih banyak Look-Up Tables (LUTs) dan 1,58 kali lebih banyak Flip-Flops (FFs) dibandingkan baseline perangkat lunak, peningkatan kinerja yang diperoleh jauh melebihi overhead sumber daya yang dibutuhkan. Temuan ini menegaskan efektivitas solusi perangkat keras berbasis FPGA dalam meningkatkan throughput komputasi pada sistem terbenam yang terbatas sumber daya, serta membuka peluang untuk optimasi dan pengembangan akselerator aritmatika yang lebih skalabel di masa mendatang.

Kata Kunci : Faktor Persekutuan Terbesar, FPGA, MicroBlaze V, Hardware Accelerator, Embedded Systems, Performance Optimization, AXI4-Lite.