Overview

The XMODZ IP collection provides fast hardware implementations for the $x \mod z$ computation on integers. The collection comprises of two distinct IP modules, modk for modulo by a fixed integer constant and modv for modulo by an integer variable.

The algorithm used for implementing $x \mod z$ is based on modulo reduction where at each stage, the magnitude of $x$ is reduced, but the residue remains the same.

Modulo reduction is widely used in cryptographically-secure systems, for fast pseudo-random number generation and is suitable for RNS (Residue Number System) applications.

Functional description

XMODZ is implemented as fully-parameterized RTL VHDL using a clean process-based style with combinational-only and sequential-only processes. Both registered and combinational designs provide a fully-synchronous interface by registering their outputs.

The interface block diagrams for both designs are shown below.

Each core uses a single external clock source, connected to signal CLK. It can be asynchronously reset with the active high signal RESET. Signal START activates the core. Data inputs X and Z (the latter only for the modv case) are the numerator and denominator involved in the modulus operation. Data output Y is the outcome of this computation. DONE signifies the end of the current computation. READY indicates that the core can accept new input.

FEATURES

- Highly-parameterized synchronous architecture
- Combinational or register-pipelined operation
- Support for arbitrary-precision integer arithmetic
- Compatible with IEEE-1076 standard
- Uses the standard IEEE packages (numeric_std)
- Tested for large data bitwidths (including 256-bit, 512-bit operation)
- Simple block-level interface for bus-level integration to third-party designs

DELIVERABLES

- Documentation in ASCII text, PDF, HTML forms
- Vendor-independent VHDL code for both cores
- Self-checking testbenches
- Configurable multi-precision integer reference C models for test data generation

Performance/QoR

<table>
<thead>
<tr>
<th>IP</th>
<th>Mode</th>
<th>Clock freq</th>
<th>Area (LUTs/regs)</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>modk (K=10)</td>
<td>REG</td>
<td>239</td>
<td>2914 (6%)/2135 (2%)</td>
<td>4.44 us</td>
</tr>
<tr>
<td>modv</td>
<td>REG</td>
<td>198</td>
<td>4706 (10%)/6241 (6%)</td>
<td>5.38 us</td>
</tr>
</tbody>
</table>

Synthesis results on Xilinx XC6VLX75T for reference use. Timing estimates for 1000 random tests. 64-bit data width is assumed.