Pipelined FPGA Adders
Florent de Dinechin, Hong Diep Nguyen, Bogdan Pasca

To cite this version:

HAL Id: ensl-00475780
https://hal-ens-lyon.archives-ouvertes.fr/enl-00475780v2
Submitted on 1 Nov 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Pipelined FPGA Adders
LIP Research Report RR2010-16

Florent de Dinechin, Hong Diep Nguyen, Bogdan Pasca
LIP, projet Arénaire
ENS de Lyon
46 allée d’Italie, 69364 Lyon Cedex 07, France

Abstract—Integer addition is a universal building block, and applications such as quad-precision floating-point or elliptic curve cryptography now demand precisions well beyond 64 bits. This study explores the trade-offs between size, latency and frequency for pipelined large-precision adders on FPGA. It compares three pipelined adder architectures: the classical pipelined ripple-carry adder, a variation that reduces register count, and an FPGA-specific implementation of the carry-select adder capable of providing lower latency additions at a comparable price. For each of these architectures, resource estimation models are defined, and used in an adder generator that selects the best architecture considering the target FPGA, the target operating frequency, and the addition bit width.

Keywords—addition; pipeline; low-latency; FPGA

I. INTRODUCTION

Integer addition is used as a building block in many coarser operators. Examples which require large adders include integer multipliers, most floating-point operators, and modular adders used in some cryptographic applications. In floating-point, the demand in precision is now moving from double (64-bit) to the recently standardized quadruple precision (128-bit format, including 112 bits for the significand) [1]. In elliptic-curve cryptography, the size of modular additions is currently above 150 bits for acceptable security.

This study presents an operator generator for binary integer addition that is based on resource estimation models of possible implementations. Given a specification including a target frequency, the generator queries the implementation models in order to select the one matching this frequency at minimal cost. Once found, the VHDL code of the selected implementation is generated.

Adders differ in the way they propagate carries. Modern FPGAs include special hardware dedicated to carry propagation [2], [3], [4], [5], [6]. Sending a carry to a neighbouring cell through the dedicated carry line is much faster than sending a bit to the same cell through the general recongifurable routing fabric. Therefore, proven solutions for VLSI designs [7] bring little speed improvement on FPGAs over the ripple carry adder (RCA) except for addition size exceeding 64 bits [8]. These speed improvements are small, and they come at a cost penalty exceeding a factor 2 over the RCA. Therefore, a binary addition is expressed in VHDL as a + and is implemented by default as an RCA.

This article re-evaluates this situation when a pipelined adder is needed. Pipelining is used for cutting the critical path in order to increase operator frequency. To the best of our knowledge, there is no IP core generator nor VHDL/Verilog library which provide high-performance pipelined binary adders for FPGAs. This work introduces the adder generator used in the FloPoCo project as a building block of most other operators.

The main contributions of this work are:
- an alternative pipelining of ripple-carry adder;
- a novel short-latency pipelined adder;
- resource estimation models including slice, register and LUT count for three adder architectures;
- integration of these models into an addition operator generator that takes as input a list of user specifications, and returns the VHDL code of the best operator.

A. Related Work

The simplest pipelining of binary addition [9], [10], [7] consists in buffering the carry-out of each full-adder (FA) along the carry propagation path, and inserting synchronization registers for I/O. The previous technique is wasteful when the objective period is larger than the delay of a 1-bit carry propagation. For these cases, a better version [11], [7], [12] consists in registering carries only every \( \alpha \) FA cell. This technique will be detailed in section II-A, and is referred to as the classical RCA pipelining technique.

Faster techniques than the previous classical architecture have been developed for VLSI. A first idea is to speed up the logic on the carry propagation path [13], [10]. Other, more algorithmic approaches include carry-select, carry-skip, and the family of prefix adders [7]. These designs map poorly on FPGAs, however they have served as an initial source of inspiration for the proposed pipelining techniques from section II-C.

A complete study on unpipelined binary FPGA addition is presented in [8]. The authors present FPGA-specific optimization opportunities for carry-skip and carry-select adders and show that optimized versions of these adders can be faster than the RCA for large addition sizes. However, these faster versions come at a significant size penalty, which recommends them only for delay-critical applications. Moreover, pipelining is not covered. The present article extends this previous study to pipelined addition.

1 http://www.ens-lyon.fr/LIP/Arenaire/Ware/FloPoCo/
B. FPGA addition in the FloPoCo context

FloPoCo is a generator of arithmetic cores (Floating-Point Cores, but not only) for FPGAs. FloPoCo also provides a framework for arithmetic operator development that is, to our knowledge, the easiest way to design complex operators with flexible pipelines [14]. The operators presented in this paper have been developed using the FloPoCo framework and are essential building blocks of most complex FloPoCo operators.

FloPoCo generates arithmetic operators in human-readable synthesizable VHDL starting from a list of user specifications (see Figure 1). These specifications include: operator parameters (operand width for binary addition), deployment FPGA target, target frequency and others. One of the original features of FloPoCo is that operator generation is frequency-driven. Instead of generating the fastest possible operator, the FloPoCo philosophy is to provide the smallest operator meeting a frequency constraint. This approach has the advantage of being compositional: a larger operator working at frequency \( f \) may be assembled out of sub-components working at frequency \( f \).

This study formalizes frequency-driven addition pipelining.

C. Design-space exploration by resource estimation

Modern FPGA resources are heterogeneous, including LUT-based logic, embedded memories, embedded DSP blocks, and others. For addition, we only need to estimate logic and registers. This study gives resource estimation formulae for these resources for several Xilinx FPGAs. Altera targets are currently only partially supported. This doesn’t mean that FloPoCo operators do not work on Altera, just that they are not optimized accurately.

The formulae allow for a fast and exhaustive design-space exploration, where only the selected architecture will be generated and synthesized. For this method to be valid, we will check in III-A that these formulae effectively predict the performance and resource consumption of the operator after synthesis and technology mapping. Addition and register mapping is simple enough for these formulae to be accurate to about one percent in all cases.

D. FPGA targets

In the FloPoCo framework, each FPGA is abstracted to a list of essential attributes: LUT features, routing delays, DSP configurations, on-chip memory, etc.

The Xilinx VirtexII-Pro [2], Spartan3 [3] and Virtex-4 [4] FPGAs have very similar slice structure (Figure 2): two 4-input LUTs with corresponding flip-flops and arithmetic logic for carry-bit computation and propagation. Carry-bit propagation is accomplished by means of dedicated carry-chains running vertically through the FPGA layout.

This is the default slice type and is denoted by \( \text{sliceL} \). In addition, a secondary slice type featuring a superset of functionalities is available. The \( \text{sliceM} \) cell allows the LUT to be configured as a variable-length shift-register (SRL16). When this configuration is used, shift registers of up-to 16 bits can be absorbed in one half-slice. This feature, when available, allows minimizing input/output synchronization cost.

The Virtex-5 and Virtex-6 slices [5] are similar with respect to addition. However, they allow independent use of the LUTs and registers, which means that estimation formulae have to count them separately.

II. Pipelined addition on FPGA

Let \( X, Y \) be two integers on \( w \) bits (in the range \( \{0, ..., 2^w - 1\} \)) and \( c_{in} \) a carry-in bit. The sum of \( X, Y \) and \( c_{in} \) is noted \( R = X + Y + c_{in} \). It is in \( [0, 2^{w+1} - 1] \) and is representable on \( w + 1 \) bits. Note that all the following also applies to signed integers in 2’s complement notation.

The RCA delay is proportional to the addition size. It has three components. First, the LUT delay, \( \delta_{LUT} \), used to precompute the carry multiplexer select signal. Then there is a worst-case delay of \( (w - 1)\delta_{carry} \) for carry propagation. Finally, \( \delta_{\text{xor}} \), the delay of the xor gate used to compute the MSB sum bit.

\[
\delta_w = \delta_{LUT} + (w - 1)\delta_{carry} + \delta_{\text{xor}} \tag{1}
\]

As \( w \) increases the addition frequency decreases as illustrated in Figure 3 for three FPGAs.

In the context of frequency-driven pipelining, a pair \((w, f)\) which is under the corresponding curve in Figure 3 meets the frequency constraint. There are two solutions for additions not meeting this constraint. We can choose a different addition architecture that is able to reach the frequency without too much of a cost penalty [8]. This solution is unable to cover the entire \((w, f)\) space. Another solution is to pipeline the adder design such that the critical path of the circuit is less than the target period \( T = 1/f \). This study focuses on the second solution, because it is more scalable and often consumes less resources.
A. Classical RCA Pipelining

A tight frequency-driven pipelining is obtained by first determining the maximal addition size $\alpha$ in equation 1 for which the critical path delay is less than the target period $T$:

$$
\alpha = 1 + \left[ \frac{T - \delta_{LUT} - \delta_{xor}}{\delta_{carry}} \right].
$$

Next, the addition is split into $k$ chunks of $\alpha$ bits (except the last chunk denoted by $\beta$, $\beta \leq \alpha$) such that $w = (k-1)\alpha + \beta$. An instantiation of this architecture highlighting the previously discussed parameters is presented in Figure 4 for $k = 4$. As $k$ decreases, the number of registers used for synchronization decreases. When the critical path of the $w$-bit addition is $\leq T$, no pipelining is required ($k = 1$) and the addition may be expressed as a simple $+$ in VHDL.

The column labelled Classical in Table II presents the resource estimation formulae function of $\alpha$, $\beta$, $w$, $k$, respectively with and without allowing shift-register packing in LUTs (SRL). Let us now explain how such formulae were built.

B. Resource estimation techniques

Let us take as a running example the previous classical architecture, annotated on Figure 5.

The LUTs of the Xilinx FPGAs can be be used either as a function generator or as a variable length shift-register, as previously presented in Section I-D. Let us take as a running example the previous classical architecture, as per section II-A. The algorithm first determines the chunk size $\alpha$ as per section II-A. Next, two sums are computed for each pair of chunks: $X_i + Y_i$ and $X_i + Y_i + 1$. The final result $R$ is a combination of the corresponding sub-sums and is found in a space of $2^k$ combinations. Selecting the appropriate sub-sum is done by using a carry-in bit. The novel idea in this algorithm is the use of the dedicated fast-carry chains to compute the carry-bits for the result selection.

Actually, for each chunk, a pair (sum, carry-out) is computed for both possible values of the carry-in. We use the

![Fig. 3. Ripple-Carry Addition Frequency for VirtexIV, Virtex5 and Spartan3E](image-url)
ever, choosing the correct splitting for the inputs is not trivial.

The short-latency architecture depicted in Figure 8 has a constant latency of two cycles. In addition, for lower frequency operators, the second register levels can be discarded. However, choosing the correct splitting for the inputs is not trivial as we have to ensure that the critical path length is smaller than the target period \( T \). Considering that the first sums are registered, we have to find the correct sizes for splitting the inputs, such that the critical path length that includes the carry generation circuit and the final additions is less than \( T \).

Intuitively, as the index of the chunks added is higher, the length of the corresponding carry bit propagation is longer and thus the length of the final addition has to be smaller. We use a greedy algorithm that, at index \( i \), finds the maximum addition size such that the carry propagation for index \( i \) and the final addition for this index is smaller than \( T \). However, it is

\[
c_i - c_i s_i' = c_{i-1} + c_i^0 + c_i^1 + 2
\]

One can verify the correctness of the carry generation by checking the truth table presented in Table I. Note that the greyed-out rows of the table will never be needed, as \( c_i^0 = 1 \) implies \( c_i^1 = 1 \) (it is not possible that \( X_i + Y_i \) overflows and \( X_i + Y_i + 1 \) doesn’t). The value of \( s_i' \) is not used further but is necessary for correct inference and mapping of the addition on the fast-carry chains of the FPGA.

It should be noted that a strong point of this approach is that this carry propagation is expressed as an addition, and therefore portable (no need for vendor-specific low-level LUT-filling primitives). For instance, porting it to Altera chips should simply involve choosing the appropriate values for the delay-related parameters influencing the chunk size.

The formulae presented in Table II are deduced for \( k \geq 3 \).

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
\( c_{i-1} \) & \( c_i^0 \) & \( c_i^1 \) & \( c_i \) & \( s_i' \) \\
\hline
0 & 0 & 0 & 0 & 1 & 0 \ \\
0 & 0 & 1 & 0 & 1 & 1 \ \\
0 & 1 & 0 & 0 & 1 & 1 \ \\
0 & 1 & 1 & 1 & 0 & 0 \ \\
1 & 0 & 0 & 0 & 1 & 1 \ \\
1 & 0 & 1 & 1 & 0 & 0 \ \\
1 & 1 & 0 & 1 & 0 & 0 \ \\
1 & 1 & 1 & 1 & 0 & 1 \ \\
\hline
\end{tabular}
\caption{CAC Truth Table. Greyed-out rows are not needed}
\end{table}
possible that for a given input size \( w \) and a target frequency \( f \), such a solution does not exist. In this case the second register level is inserted, and the chunk size becomes \( \alpha \).

In addition to latency reduction, this optimization brings the following gains: the number of registers is reduced by the carry propagation size (which now needs no registering), the LUT count is reduced by approximatively \( w \), and the number of slices by approximatively \( w/2 \).

Finally, the scalability of this architecture may be ensured by pipelining the carry propagation circuit. Once \( k > \alpha/2 \) the length of the carry propagation becomes greater than the target period and violates the constraints. In this case we pipeline this addition with the best pipelining algorithm function on its size.

The increase in resources of the obtained architecture only equals the increase in size of the carry-propagation operator, as the possible delay introduced by this operator will be transparently absorbed by the shift registers.

E. No packing of shift registers in LUTs (SRL)

The addition architectures presented so far make extensive use of the shift-registers available in the sliceM. However, this resource is getting rarer over the years. All the slices in a VirtexII-Pro device were similar to sliceM, but they were reduced to half the total number of slices for Virtex4 and Spartan3, and about a quarter in Virtex5 and Virtex6 devices (with higher density at the input of the DSP48E blocks). There is an ISE option that prevents using this resource. It may therefore be relevant to be able to generate adders with this in view.

Out of the presented architectures, the low-latency one will behave better when no shift registers are allowed. This is due to the fact that it requires fewer registers for synchronization. When \( k = 2 \), the alternative implementation behaves better than the classical one, as it propagates approximatively half as many signals on the upper part of the addition diagonal. Resource estimations for the three architectures when not allowing SRLs are presented in Table II.

F. Managing partial cycle delays

By assembling two pipelined components \( A \) and \( B \) working at frequency \( f \) with registers between them, one obtains an operator \( A|B \) that also works at frequency \( f \), whose latency is the sum of those of \( A \) and \( B \), plus one. However, one may sometimes save the registers between \( A \) and \( B \) if this doesn’t introduce a critical path longer than the target period. The FloPoCo framework includes experimental support for this possibility. In general, a component may input a vector of input delays, and will report the delays on each of its outputs (see Figure 1). It could also work from output to input, this is an arbitrary choice.

Back to adders, for the classical architecture, in the presence of an input delay, the upper-rightmost addition now needs to use a \( \gamma \) chunk size, \( \gamma < \alpha/\text{beta} \) so that the period of the \( \gamma \) addition is less than \( T \) minus the input delay. The rest of the chunks are split as before, as they are registered anyway. We now have \( w = \beta + (k-2)\alpha + \gamma \). The cost impact on the architecture is dictated by \( \beta_{\text{old}} > \gamma \) and the use of SRLs. The \( \beta_{\text{old}} > \gamma \) leads to an increment in pipeline depth. This is absorbed by the shift-registers if available at no extra cost, or costs as much as \( w/2 \) slices.

For both alternative and low-latency architectures, there are two options: either perform all additions in using chunk size \( \gamma \), or buffer the inputs and perform computations using chunk size \( \alpha \). For the alternative architecture, lower values for \( \gamma \) will increase the latency of the operator. When SRLs are available, the cost is maintained under control, otherwise the synchronization cost greatly increases. For the low-latency operator, a smaller \( \gamma \) may require pipelining the carry generation circuit. However, the size of this circuit remains small with respect to the total size.

All this shows that the best adder really depends on the context. Work is under way to exploit these new possibilities in FloPoCo.

III. REALITY CHECK

A. Estimation formulae

We have checked our estimation formulae against synthesis results using Xilinx ISE 11.1. Results presenting the resource usage estimations, obtained results and relative errors for both with and without SRLs are presented in Table III for a 128-bit addition synthesised on a Virtex4 (speedgrade -12) with a required frequency of 400MHz.

First, it should be mentioned that all the synthesized adders met the frequency target. In addition, one may observe that the resource estimations are accurate for all criteria. The best estimations are obtained as expected for LUTs and registers. The slice estimations represent the lowest bound obtainable leading to underestimation of the result. Nevertheless, the relative error of the estimation remains small, of the order \(10^{-2}\), or one percent.

B. Synthesis results

Synthesis results for some combinations of the input specifications are presented in Table IV. We choose different target FPGA and different operating frequencies. For each architecture and set of specifications we present the costs reported by Xilinx ISE 11.1 and its pipeline depth. The last column shows the gain of using the generated addition operator against using the classical implementation.

The grey cells in Table IV highlight the lowest costs for the given specifications. We can observe that for different addition sizes the lowest cost is obtained by different architectures. The accurate estimation formulae help choosing the best architecture given the specifications and obtain the reported gain.

IV. CONCLUSIONS

This article addresses the construction of pipelined adders for large operands working at high frequencies, from specifications including operand size, deployment target, running frequency, and optimization directives.
When the FloPoCo project was initiated, it was not expected that we would need to dedicate so much work to something as seemingly simple as integer addition on FPGAs. The reason why it became important is that addition is so pervasive. The presented adder generator provides subcomponents for integer multipliers and constant multipliers, and for most floating-point cores, including addition, multiplication, division and square root, and elementary functions. If we want these cores to work at a high frequency for double precision and beyond, we need high-performance adders, but we also need them to consume as little resources as possible. Therefore, the adder generation described here is frequency-driven (possibly inheriting the frequency from the wider context) and minimizes resource consumption, based on accurate resource estimation formulae for three alternative pipelined adder architectures.

When the FloPoCo project was initiated, it was not expected that we would need to dedicate so much work to something as seemingly simple as integer addition on FPGAs. The reason why it became important is that addition is so pervasive. The presented adder generator provides subcomponents for integer multipliers and constant multipliers, and for most floating-point cores, including addition, multiplication, division and square root, and elementary functions. If we want these cores to work at a high frequency for double precision and beyond, we need high-performance adders, but we also need them to consume as little resources as possible. Therefore, the adder generation described here is frequency-driven (possibly inheriting the frequency from the wider context) and minimizes resource consumption, based on accurate resource estimation formulae for three alternative pipelined adder architectures.

Work is under way to integrate the proposed adders in all the coarser cores of the FloPoCo project, and to support more FPGA targets. Future work also includes extending the optimization options to include operator latency, and possibly combinations such as “LUTs and latency”.

This work was partly supported by the ANR EVA-Flo project and Stone Ridge Technology.

---

**TABLE II**

<table>
<thead>
<tr>
<th>SRL</th>
<th>Classical</th>
<th>Alternative</th>
<th>Short-Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG</td>
<td>(3k - 5)α + 2β + k - 1</td>
<td>(2k - 3)α + β + 2k - 3</td>
<td>(k - 1)α + β + 4k - 7</td>
</tr>
<tr>
<td>LUT</td>
<td>α + β : k = 2</td>
<td>α + 2β : k = 2</td>
<td>(4k - 6)α + 3β + 2k - 4</td>
</tr>
<tr>
<td>SLICE</td>
<td>[((4k - 7)α + 3β + k - 1)/2]</td>
<td>[((α + 2β + 1)/2)] : k = 2</td>
<td>[((4k - 6)α + 3β + 2k - 4)/2]</td>
</tr>
</tbody>
</table>

---

**TABLE III**

<table>
<thead>
<tr>
<th>Architecture</th>
<th>SRL</th>
<th>128bit</th>
<th>400MHz</th>
<th>32bit</th>
<th>400MHz</th>
<th>64bit</th>
<th>64bit</th>
<th>64bit</th>
<th>64bit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>128</td>
<td>573</td>
<td>309</td>
<td>128</td>
<td>573</td>
<td>300</td>
<td>0</td>
<td>0</td>
<td>2.10^-2</td>
</tr>
<tr>
<td>Y</td>
<td>318</td>
<td>292</td>
<td>198</td>
<td>318</td>
<td>292</td>
<td>194</td>
<td>0</td>
<td>0</td>
<td>2.10^-2</td>
</tr>
<tr>
<td>N</td>
<td>222</td>
<td>392</td>
<td>216</td>
<td>223</td>
<td>393</td>
<td>207</td>
<td>4.10^-4</td>
<td>2.10^-2</td>
<td>4.10^-4</td>
</tr>
<tr>
<td>Y</td>
<td>352</td>
<td>199</td>
<td>183</td>
<td>352</td>
<td>199</td>
<td>177</td>
<td>0</td>
<td>0</td>
<td>3.10^-4</td>
</tr>
<tr>
<td>N</td>
<td>288</td>
<td>264</td>
<td>216</td>
<td>293</td>
<td>263</td>
<td>214</td>
<td>10^-3</td>
<td>3.10^-3</td>
<td>9.10^-4</td>
</tr>
<tr>
<td>Y</td>
<td>416</td>
<td>136</td>
<td>216</td>
<td>421</td>
<td>137</td>
<td>211</td>
<td>10^-2</td>
<td>7.10^-2</td>
<td>2.10^-2</td>
</tr>
</tbody>
</table>

---

**TABLE IV**

<table>
<thead>
<tr>
<th>Size</th>
<th>Freq</th>
<th>Target</th>
<th>Optimisation</th>
<th>Classical</th>
<th>Alternative</th>
<th>Short-Latency</th>
<th>Gain w/r classical</th>
</tr>
</thead>
<tbody>
<tr>
<td>32bit</td>
<td>200</td>
<td>Spartan3 3s200pq208-5</td>
<td>SLICE/SLICE/SLICE/</td>
<td>62</td>
<td>62</td>
<td>76</td>
<td>2</td>
</tr>
<tr>
<td>64bit</td>
<td>450</td>
<td>Virtex4 4vlx15s363-12</td>
<td>SLICE/SLICE/SLICE/</td>
<td>96</td>
<td>81</td>
<td>109</td>
<td>2</td>
</tr>
<tr>
<td>128bit</td>
<td>450</td>
<td>Virtex5 4vx30f334-3</td>
<td>REG/REG/REG/</td>
<td>247</td>
<td>230</td>
<td>255</td>
<td>5</td>
</tr>
<tr>
<td>128bit</td>
<td>450</td>
<td>Virtex5 5vx30f334-3</td>
<td>REG/REG/REG/</td>
<td>718</td>
<td>525</td>
<td>267</td>
<td>2</td>
</tr>
</tbody>
</table>

**REFERENCES**