Optimization of Very Large Constant Multiplication

Théo Cantaloube, Christine Solnon and Anastasia Volkova

INSA Lyon, Inria, CITI, Villeurbanne, France

Keywords : *operations research, optimization, computer arithmetic, digital circuit design.*

1 Context and problem statement

Design of efficient and sustainable arithmetic circuits for resource-constrained hardware proposes a broad range of combinatorial optimization problems. One of them is the Multiple Constants Multiplication (MCM) problem, which finds its application in digital signal processing, machine learning and cryptography. Classical MCM consists in finding a computational graph corresponding to an implementation of multiplications of an integer input x by some integer target constants such that only additions/subtractions and bit-shifts are used, for example $7x = 2^3x - x$. The interest stems from the fact that generic multiplier circuits are very costly compared to adders/subtractors and bit-shifts (considered as free), and when multiple constants are used, intermediate terms can, and should, be shared to save resources. Thus, typical MCM formulations aim to minimize the number of adders and maximize sharing.

The MCM problem has been extensively modeled and solved using ILP [5], SAT [4] and very recently CP [3]. All of these approaches, however, suffer from limitations to the maximum size of the target constants, mostly due to limited data precision within the solvers and numerical instabilities. While for a large part of embedded signal processing systems, MCM is typically solved within these limits of 10 to 20 bits, others do require at least 50-bit integer target constants. This is in particular the case of octave-band filters used for sound-pressure analysis and metrology. Naturally, cryptographic applications require constants of hundreds and thousands bits. Hence, there is a practical need to solve the MCM for larger constants.

With this work, we study the case of Very Large Constant Multiplication (VLCM) for one target constant. A straightforward approach is to cut it into smaller equally-sized chunks, solve the MCM for them and reconstruct the target at the cost of some additions and bit-shifts. Existing methods quickly give up the optimality criterion and integrate graph-based and common sub-expression elimination heuristics [1, 2]. The proposed methodology aims to enhance state-of-the-art techniques by optimizing the decomposition of target constants. To do so, we search for bit patterns that minimize the number of required MCM sub-constants, and consequently the overall cost. The subsequent section provides an overview of the approach, which is formulated within a constraint-programming (CP) framework.

2 Constraint Programming Approach

Since the target constant cannot fit on variables of our solver, we model it using binary variables arrays. To compensate for the absence of arithmetic constraints, our perspective is to instantiate sub-constants in such a way that no carries occur during the reconstruction of the target constant. This implies that each of its 1-bits will be attributed to exactly one sub-constant. The sub-constants values are linked to their binary decomposition through channeling constraints. In contrast to previous approaches, we allow bit-patterns of the sub-constants to overlap. We can address VLCM in two different ways:

1. Separating the subdivision of very large constant on one hand and the MCM solving process of the sub-constants in another hand, as displayed in Fig. 1.

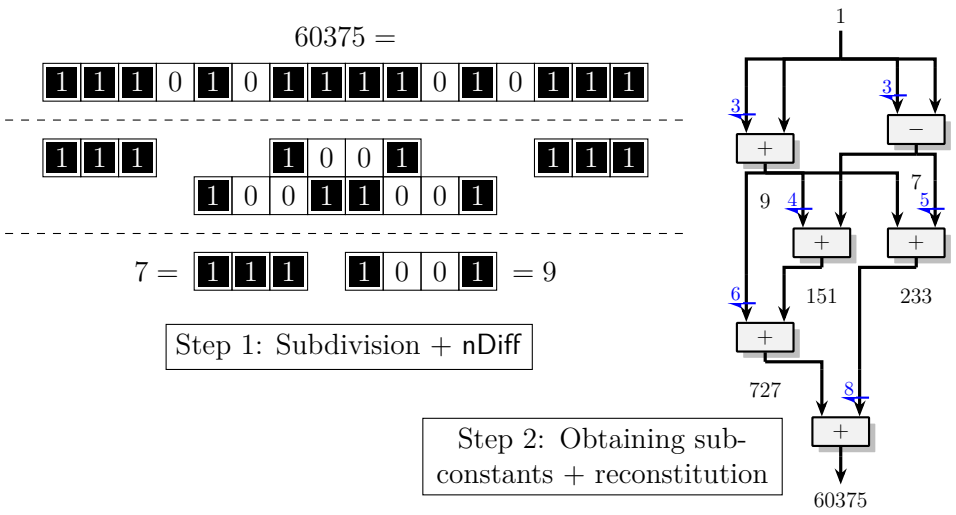

FIG. 1: Subdividing 60375 into sub-constants of size 4 bits (blue arrows represent shifts)

2. Integrating the subdivision of very large constant into the MCM solving process of sub-constants using activation variables.

While option 2 certainly yields better optimization results, it represents a significant computational load. However, in order to generate sub-constants more likely to be inexpensive to produce, option 1 needs an appropriate optimization metric. We chose to minimize the number of different sub-constants using nDiff global constraint, counting the different elements in a set.

3 Conclusion and on-going work

In this work, we examine how bit-pattern search during subdivision improves the overall cost of VLCM, even if global optimality is not reached. In the future work we will address the optimal subdivision for multiple large constants, where the pool of intermediate constants is shared. Then, a finer-grained cost for the reconstruction step will be considered, potentially permitting subtractions in the reconstruction and counting the number of one-bit adders.

References

[1] Levent Aksoy, Debapriya Basu Roy, Malik Imran, Patrick Karl, and Samuel Pagliarini. Multiplierless design of very large constant multiplications in cryptography. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 69(11):4503–4507, 2022.

[2] Levent Aksoy, Debapriya Basu Roy, Malik Imran, and Samuel Pagliarini. Multiplierless design of high-speed very large constant multiplications. In *2024 29th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 957–962, 2024.

[3] Théo Cantaloube, Xiao Peng, Christine Solnon, and Anastasia Volkova. A new constraint programming model for the multiple constant multiplication. In *Proceedings of the 24th Workshop on Constraint Modelling and Reformulation*, Glasgow, United Kingdom, 2025.

[4] Nicolai Fiege, Martin Kumm, and Peter Zipf. Bit-level optimized constant multiplication using boolean satisfiability. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 71(1):249–261, 2024.

[5] Rémi Garcia and Anastasia Volkova. Toward the multiple constant multiplication at minimal hardware cost. *IEEE Transactions on Circuits and Systems I: Regular Papers*, pages 1–13, 2023.