



Solving the Multiple Constant Multiplication Problem with Constraint Programming

The 32nd International Conference on Principles and Practice of Constraint Programming

Théo Cantaloube¹ Xiao Peng² Christine Solnon¹ Anastasia Volkova¹

¹CITI, INSA Lyon / Inria, France

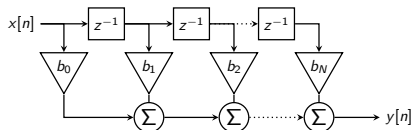
²LAAS-CNRS, Toulouse, France

July 23, 2026

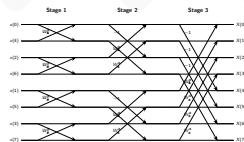
Introduction

Embedded computations everywhere

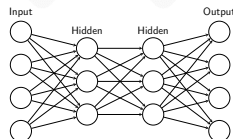
⇒ Need for cheap and fast arithmetic operator implementations



Digital Signal Processing for linear digital filter evaluation [Meh2011; How2014; Kum2023; Gar2022; Aks2007]



Discrete Transforms (Discrete Cosine, Fast Fourier) [Ghi2010; Wen2015]



Inference of Deep Neural Networks [Gar2025; Hab2022]

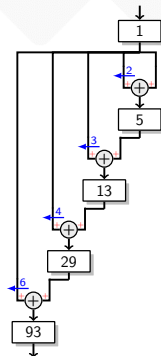
Multiple Constant Multiplication problem (MCM)

- Multiply an unknown integer by several fixed known integer target constants
- Exploit *a priori* knowledge of constants to design optimized implementations instead of costly generic multipliers

Motivation - Single Constant Multiplication

Illustration of SCM for $T = \{93\}$ when using the binary approach of $93_{dec} = 1011101_{bin}$

$$\begin{array}{r}
 X = \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \\
 \times 93 = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline \end{array} \text{bin} \\
 \hline
 1 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \\
 + 0 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \quad \text{1} \\
 + 1 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \quad \text{2} \\
 + 1 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \quad \text{3} \\
 + 1 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \quad \text{4} \\
 + 0 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \quad \text{5} \\
 + 1 \times \begin{array}{|c|c|c|c|c|c|c|} \hline X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\ \hline \end{array} \quad \text{6}
 \end{array}$$



Corresponding adder graph
 $\Rightarrow$ 4 adders

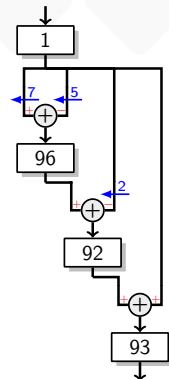
Motivation - Single Constant Multiplication

Illustration of SCM for $T = \{93\}$ when using the Canonical Sign Digit approach of $93_{dec} = 10\bar{1}00\bar{1}01_{CSD}$

$$\begin{aligned}
 & X = \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} \\
 & \times 93 = \begin{bmatrix} 1 & 0 & \bar{1} & 0 & 0 & \bar{1} & 0 & 1 \end{bmatrix}_{CSD} \\
 = & \frac{1 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} + 0 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} - 1 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} + 0 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} + 0 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} - 1 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} + 0 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix} + 1 \times \begin{bmatrix} x_6 & x_5 & x_4 & x_3 & x_2 & x_1 & x_0 \end{bmatrix}}{7}
 \end{aligned}$$

Diagram illustrating the Canonical Sign Digit (CSD) representation of 93 and its decomposition into a sum of products. The CSD representation is $10\bar{1}00\bar{1}01_{CSD}$. The decomposition shows the multiplication of the input X by 93, resulting in a sum of products. The products are:

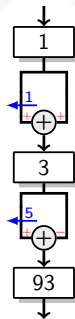
- $1 \times X$ (blue arrow 7)
- $+ 0 \times X$ (red line, blue arrow 5)
- $- 1 \times X$ (blue arrow 2)
- $+ 0 \times X$ (red line, blue arrow 3)
- $+ 0 \times X$ (red line, blue arrow 4)
- $- 1 \times X$ (blue arrow 6)
- $+ 1 \times X$ (blue arrow 7)



Corresponding adder graph
 $\Rightarrow$ 3 adders

Motivation - Single Constant Multiplication

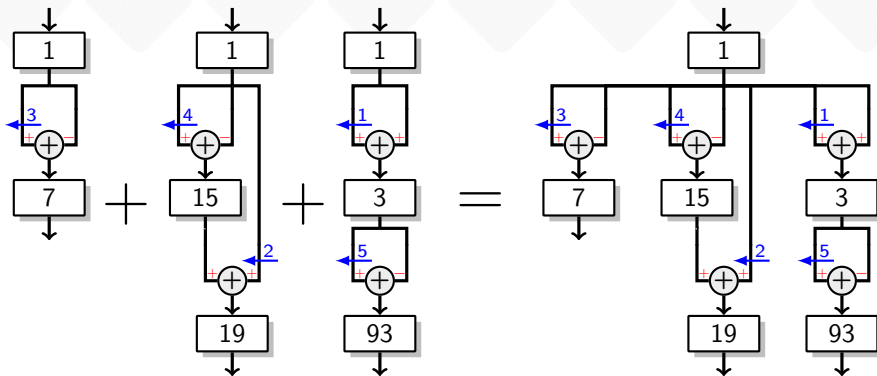
Optimal graph for $T = \{93\}$



$\Rightarrow$ 2 adders

Motivation - Multiple Constant Multiplication

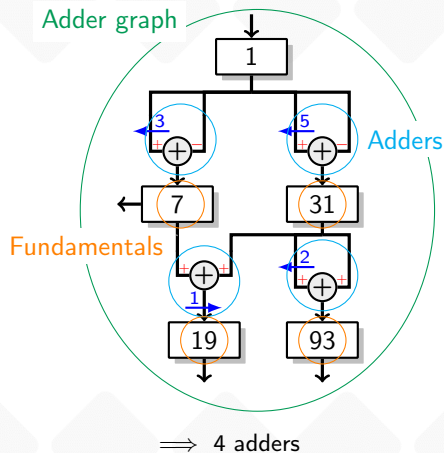
Illustration of MCM for $T = \{7, 19, 93\}$ when optimizing separately each single constant



Corresponding adder graph $\Rightarrow$ 5 adders

Motivation - Multiple Constant Multiplication

Optimal graph for $T = \{7, 19, 93\}$



Formal definition - MCM problem

- Optimization metric: number of adders
- ⚠ Doesn't perfectly reflect hardware cost but good proxy variable

Definition (MCM)

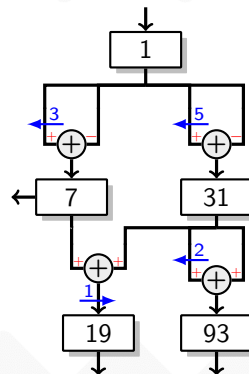
Problem: $\text{MCM}(T)$

Input: Target constant set T

Output: Adder graph producing T minimizing the number of adders

Input: $T = \{7, 19, 93\}$

Output:





CP Model

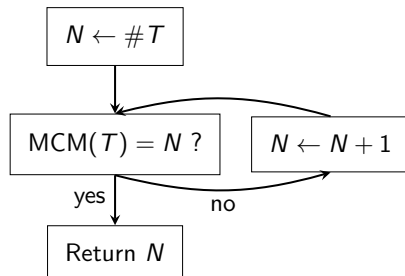


CP model - MCM problem

$T \subset \mathbb{N}$: target constant set;

$w \in \mathbb{N}$: maximal wordlength in T ;

$N \in \mathbb{N}$: number of adders.



Transform minimization problem into a sequence of decision problems

C1: $\forall v \in \llbracket 1, N \rrbracket, \alpha_v * c_v = \beta_v$

C2: $\forall v \in \llbracket 1, N \rrbracket, \delta_v * c_{p_v} = \gamma_v$

C3: $\forall v \in \llbracket 1, N \rrbracket, \sigma_{v,q} * c_{v,r} = \epsilon_v$

C4: $\forall v \in \llbracket 1, N \rrbracket, \beta_v = \gamma_v + \epsilon_v$

C5: $\forall v \in \llbracket 1, N \rrbracket, \delta_v > 0 \text{ or } \sigma_{v,q} > 0$

C6: $\forall v \in \llbracket 1, N \rrbracket, |\alpha_v| = 1 \text{ xor } |\delta_v| = 1$

C7: $T \subseteq \{c_v \mid v \in \llbracket 1, N \rrbracket\}$

C8: $c_0 = 1$

C9: $\forall v \in \llbracket 1, N - 1 \rrbracket, \text{ if } \#\{v' \in \llbracket v + 1, N \rrbracket \mid p_{v'} = v \text{ or } q_{v'} = v\} = 0 \text{ then } c_v \in T$

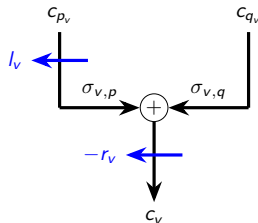
C10: $\text{allDifferent}((c_v)_{v \in \llbracket 0, N \rrbracket})$

C11: $\forall v \in \llbracket 1, N \rrbracket, c_v \bmod 2 = 1$

CP model for the decision problem, when N is fixed

Constraints - Adder modeling

- p_v, q_v : parents of vertex v
- c_v : constant produced by v



Can we break symmetries ?

- We do not know in advance the non-target fundamentals so difficult to break symmetries on them...
- But possible to break symmetries on target constants!

$$c_v = 2^{-r_v} * (\sigma_{v,p} * 2^{l_v} * c_{p_v} + \sigma_{v,q} * c_{q_v})$$

Left shift only on the left input xor right shift on both inputs [Dem1994]



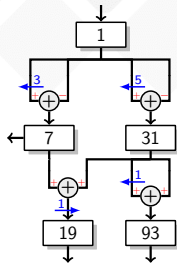
Symmetry breaking



Symmetry breaking rule 1 - Choosing p_v and q_v

- Breaking symmetries between the 2 parents of v when $c_v \in T$:
 - $p_v \leq q_v$
- If $c_v \in T$ can be produced from different couples of parents:
 - q_v must be minimized;
 - further ties are broken by minimizing p_v .

Symmetry breaking rule 2 - Partial order on fundamental sequences



$c_0 \quad c_1 \quad c_2 \quad c_3 \quad c_4$
 $S_1 = (1, 7, 31, 19, 93)$
 $S_2 = (1, 7, 31, 93, 19)$
 $S_3 = (1, 31, 7, 19, 93)$
 $S_4 = (1, 31, 7, 93, 19)$
 $S_5 = (1, 31, 93, 7, 19)$

Definition (Comparability)

$S_{\downarrow T} := S$ without T ; S and S' are comparable according to $T \Leftrightarrow S_{\downarrow T} = S'_{\downarrow T}$.

With $T = \{19, 93\}$, S_1, S_2 are comparable, but S_1, S_3 are not.

Definition (Partial order $\prec_T$)

$c_v \in T$	$c_u \in T$	Relation
✓	×	$c_v \prec_T c_u$
×	×	$c_v =_T c_u$
✓	✓	$c_v \prec_T c_u \Leftrightarrow c_v <_{\mathbb{N}} c_u$

With $T = \{7, 19, 93\}$, $S_1 \prec_T^{lex} S_2 \prec_T^{lex} S_3 \prec_T^{lex} S_4 \prec_T^{lex} S_5$.

Minimal Fundamental Sequences (MFS) global constraint and propagator

Definition (MFS)

MFS_T is satisfied if Rule 1 and Rule 2 are satisfied.

MCM for $T = \{7, 19, 93\}$



```

1   $i \leftarrow v, k \leftarrow v + 1$ 
2  while  $i < k$  do
3      forall  $T_j \in T \setminus (c_{v'})_{v' \in \llbracket 0, k-1 \rrbracket}$  by increasing value do
4          forall  $l \in \llbracket 0, i \rrbracket$  do
5              if  $c_l$  and  $c_i$  can produce  $T_j$  then
6                   $c_k \leftarrow T_j, p_k \leftarrow l, q_k \leftarrow i \dots$ 
7                   $k \leftarrow k + 1$ 
8                  break
9           $i \leftarrow i + 1$ 
10 if  $k \leq N$  then  $\mathcal{D}(c_k) \leftarrow \mathcal{D}(c_k) \setminus T$ 
  
```

Minimal Fundamental Sequences (MFS) global constraint and propagator

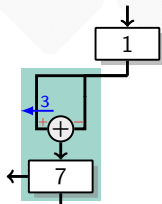
Definition (MFS)

MFS_T is satisfied if Rule 1 and Rule 2 are satisfied.

```

1   $i \leftarrow v, k \leftarrow v + 1$ 
2  while  $i < k$  do
3      forall  $T_j \in T \setminus (c_{v'})_{v' \in \llbracket 0, k-1 \rrbracket}$  by increasing value do
4          forall  $l \in \llbracket 0, i \rrbracket$  do
5              if  $c_l$  and  $c_i$  can produce  $T_j$  then
6                   $c_k \leftarrow T_j, p_k \leftarrow l, q_k \leftarrow i \dots$ 
7                   $k \leftarrow k + 1$ 
8                  break
9           $i \leftarrow i + 1$ 
10 if  $k \leq N$  then  $\mathcal{D}(c_k) \leftarrow \mathcal{D}(c_k) \setminus T$ 
  
```

MCM for $T = \{7, 19, 93\}$



Propagation

Minimal Fundamental Sequences (MFS) global constraint and propagator

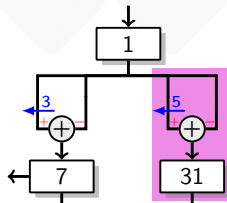
Definition (MFS)

MFS_T is satisfied if Rule 1 and Rule 2 are satisfied.

```

1   $i \leftarrow v, k \leftarrow v + 1$ 
2  while  $i < k$  do
3      forall  $T_j \in T \setminus (c_{v'})_{v' \in \llbracket 0, k-1 \rrbracket}$  by increasing value do
4          forall  $l \in \llbracket 0, i \rrbracket$  do
5              if  $c_l$  and  $c_i$  can produce  $T_j$  then
6                   $c_k \leftarrow T_j, p_k \leftarrow l, q_k \leftarrow i \dots$ 
7                   $k \leftarrow k + 1$ 
8                  break
9           $i \leftarrow i + 1$ 
10 if  $k \leq N$  then  $\mathcal{D}(c_k) \leftarrow \mathcal{D}(c_k) \setminus T$ 
  
```

MCM for $T = \{7, 19, 93\}$



Branching

Minimal Fundamental Sequences (MFS) global constraint and propagator

Definition (MFS)

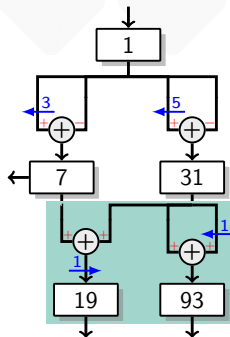
MFS_T is satisfied if Rule 1 and Rule 2 are satisfied.

```

1   $i \leftarrow v, k \leftarrow v + 1$ 
2  while  $i < k$  do
3      forall  $T_j \in T \setminus (c_{v'})_{v' \in \llbracket 0, k-1 \rrbracket}$  by increasing value do
4          forall  $l \in \llbracket 0, i \rrbracket$  do
5              if  $c_l$  and  $c_i$  can produce  $T_j$  then
6                   $c_k \leftarrow T_j, p_k \leftarrow l, q_k \leftarrow i \dots$ 
7                   $k \leftarrow k + 1$ 
8                  break
9           $i \leftarrow i + 1$ 
10 if  $k \leq N$  then  $\mathcal{D}(c_k) \leftarrow \mathcal{D}(c_k) \setminus T$ 

```

MCM for $T = \{7, 19, 93\}$



Propagation

Minimal Fundamental Sequences (MFS) global constraint and propagator

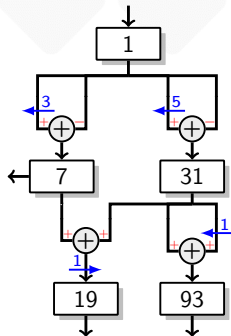
Definition (MFS)

MFS_T is satisfied if Rule 1 and Rule 2 are satisfied.

```

1   $i \leftarrow v, k \leftarrow v + 1$ 
2  while  $i < k$  do
3      forall  $T_j \in T \setminus (c_{v'})_{v' \in \llbracket 0, k-1 \rrbracket}$  by increasing value do
4          forall  $l \in \llbracket 0, i \rrbracket$  do
5              if  $c_l$  and  $c_i$  can produce  $T_j$  then
6                   $c_k \leftarrow T_j, p_k \leftarrow l, q_k \leftarrow i \dots$ 
7                   $k \leftarrow k + 1$ 
8                  break
9           $i \leftarrow i + 1$ 
10 if  $k \leq N$  then  $\mathcal{D}(c_k) \leftarrow \mathcal{D}(c_k) \setminus T$ 
  
```

MCM for $T = \{7, 19, 93\}$



Time complexity of one MFS propagation is polynomial

Time complexity of Solving MCM with CP and MFS

Property

With MFS and suitable var ordering heuristic, our CP model never branches on target constants.

$T \subset \mathbb{N}$: target constant set; $w \in \mathbb{N}$: maximal wordlength in T ; $N \in \mathbb{N}$: number of adders.

$K := N - \#T \in \mathbb{N}$: number of non-target fundamentals;

Theorem (Polynomiality)

When $N = \#T$, MCM is solved in $\mathcal{O}(w \cdot \#T^3)$

Theorem (Fixed Parameter Tractability)

When $N > \#T$, MCM is solved in $\mathcal{O}(2^{K \cdot w} \cdot w \cdot N^2 \cdot \#T) \implies$ FPT time parametrized by (K, w)



Results



Implementations and experiments

Our CP models

- CP: CP model written in Java / Choco [Pru2022]
- CP^{MFS}: CP + MFS global constraint in Java / Choco;

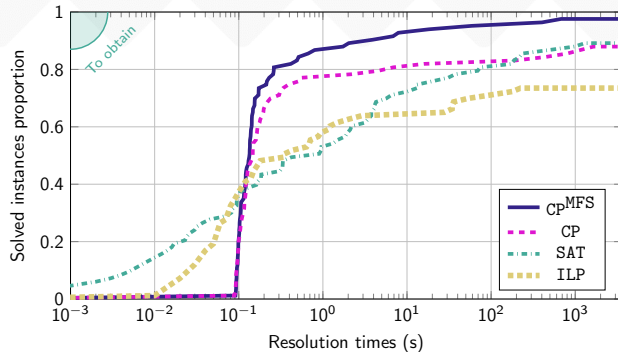
State of the Art

- ILP: ILP model of [Gar2023] written in Julia / Gurobi
- SAT: SAT model of [Fie2024] written in C++ / Cadical

Benchmark

- Widely-used collection of FIR filters that can be evaluated with MCM [Fir2021]:
 - 83 instances
 - $1 \leq |T| \leq 51$
 - $4 \leq w \leq 19$

Performance results - MCM problem



■ Time-out set to 1h

Approach	Solved
ILP	68%
SAT	89%
CP	88%
Cp^{MFS}	98%

Distribution of the solved instances proportion through time



Conclusion



Conclusion and further work

Takeaway

- Straight-forward CP model is competitive but not enough; new global constraints were needed to outperform SotA
 $\rightsquigarrow$ Choco solver enabled rapid prototyping of new propagators: importance of open-source solvers compatible with academic research
- Arithmetic optimization is a promising playground for CP

Further work

- Generalizing the MFS constraint to Straight-Line Programs
- Solving the Very Large Constant Multiplication (MCM with wordlength on up to 500 bits)

Thank you for your attention!

Appendix - References

-  Aksoy, Levent et al. "Optimization of Area in Digital FIR Filters using Gate-Level Metrics". In: *44th ACM/IEEE Design Automation Conference*. 2007, pp. 420–423.
-  Dempster, Andrew G. and Malcolm D. Macleod. "Constant Integer Multiplication Using Minimum Adders". In: *IEE Proceedings - Circuits, Devices and Systems* 141.5 (1994), pp. 407–413.
-  Fiege, Nicolai, Martin Kumm, and Peter Zipf. "Bit-Level Optimized Constant Multiplication Using Boolean Satisfiability". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 71.1 (2024), pp. 249–261.
-  Garcia, Rémi et al. "Hardware-Aware Design of Multiplierless Second-Order IIR Filters With Minimum Adders". In: *IEEE Transactions on Signal Processing* 70 (2022), pp. 1673–1686.
-  Garcia, Rémi et al. "Hardware-Aware Training for Multiplierless Convolutional Neural Networks". In: *32nd International Symposium on Computer Arithmetic*. IEEE, 2025, pp. 1–8.
-  Garcia, Rémi and Anastasia Volkova. "Toward the Multiple Constant Multiplication at Minimal Hardware Cost". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* (2023), pp. 1–13.

Appendix - References

-  Ghissoni, Sidinei et al. “Radix-2 Decimation in Time FFT implementation based on a Matrix-Multiple Constant multiplication approach”. In: *17th IEEE International Conference on Electronics, Circuits and Systems*. 2010, pp. 859–862.
-  Habermann, Tobias et al. “Hardware-Aware Quantization for Multiplierless Neural Network Controllers”. In: *IEEE Asia Pacific Conference on Circuits and Systems*. 2022, pp. 541–545.
-  Howard, Charles D., Linda S. DeBrunner, and Victor DeBrunner. “Hybrid MCM Implementation for FIR Filters in FPGA Devices”. In: *International Conference on Electro/Information Technology*. IEEE, 2014, pp. 1–6.
-  Kumm, Martin, Anastasia Volkova, and Silviu-loan Filip. “Design of Optimal Multiplierless FIR Filters With Minimal Number of Adders”. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 42.2 (2023), pp. 658–671.
-  Meher, Pramod Kumar and Yu Pan. “MCM-Based Implementation of Block FIR Filters for High-Speed and Low-Power Applications”. In: *IFIP 19th International Conference on Very Large Scale Integration and System-on-Chip*. IEEE, 2011, pp. 118–121.
-  Nanyang Technological University, Singapore. *FIRsuite: Suite of Constant Coefficient FIR Filters*. 2021.

Appendix - References



Prud'homme, Charles and Jean-Guillaume Fages. "Choco-solver: A Java library for constraint programming". In: *Journal of Open Source Software* 7.78 (2022), p. 4708.



Wendt, James B., Nathaniel A. Conos, and Miodrag Potkonjak. "Multiple Constant Multiplication Implementations in Near-Threshold Computing Systems". In: *International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2015, pp. 1071–1075.