

Formal Verification of Integer Multiplier Circuits

Jonathan Wang

Price College of Engineering
University of Utah
Salt Lake City, Utah
u1306458@utah.edu

Henry Silverman

Price College of Engineering
University of Utah
Salt Lake City, Utah
henry.silverman@utah.edu

Garrett Slack

Price College of Engineering
University of Utah
Salt Lake City, Utah
u1315263@utah.edu

Dmitry Panin

Price College of Engineering
University of Utah
Salt Lake City, Utah
dmitry.panin@utah.edu

Abstract—This paper employs advanced mathematical techniques, specifically polynomials, and ideals, to rigorously verify the correctness of an integer multiplier circuit. By leveraging algebraic methods, this approach will provide a deeper understanding of the circuit's behavior and enable a more robust verification process.

Index Terms—polynomials, vanishing polynomials (J_0), ideals (J), multiplier circuit

I. INTRODUCTION

In the field of digital circuit design, integer multiplier circuits stand as fundamental components with critical applications in various computing systems, ranging from embedded devices to high-performance computing architectures. The accurate and efficient operation of these multiplier circuits is crucial for ensuring the reliability and correctness of arithmetic computations. As technology advances and design complexities escalate, the need for rigorous verification methodologies has become increasingly pronounced to guarantee the integrity of digital circuits. Our project tests and verifies an these integer multiplier circuits by employing the various methods studied in class on smaller circuits and circuits over fields.

II. APPROACH

Ideal membership testing is a great method to test and verify of a 2-bit, 3-bit, 4-bit integer multiplier circuit. We manually designed the 2-bit and 3-bit multiplier from scratch and generated the larger circuits utilizing the (.blif writing capabilities of the?) ABC synthesis tool. Next we converted the blif files to sing files using our parsing python script. The reverse topological term order (RTTO) was then derived from the circuit, and used to represent the minimal Gröbner Basis. In digital circuit verification, there are several approaches to ensure a multiplier circuit implementation performs the same function as its specification. The first option could be creating a miter between the specification polynomials and the implementation, then checking if the Gröbner Basis (GB) is 1. Other approaches will be necessary at larger circuit sizes, such as weak Nullensatz, where the GB of the ideals and vanishing polynomials is 1 ($\text{GB}(J + J_0) = 1$). Another form of verification is checking if the Gröbner Basis of $J + J_0$ equals 0 ($\text{GB}(J + J_0) = 0$).

III. PROCESS

A. Singular

The Singular file consists of a ring, polynomials, ideals, and other code to define the behavior of a circuit and interpret its output. A ring is defined by properties, including the type of coefficients, number and names of variables, and arithmetic operations. The ordering of the inputs and outputs in the ring R should follow RTTO, consisting of the following order: outputs, internal gate outputs, primary inputs. A polynomial (poly) is the algebraic representation of the logic in the circuit. This can mean a poly is defined for each logic gate in the circuit, or a more complex poly may be used to represent the functions of groups of gates. For example, f_{spec} represents the desired mathematical functionality of the implemented circuit. Ideals are a subset of the polynomial ring that consist of all polynomials satisfying certain conditions. Vanishing polynomials are polynomials over a ring which output 0 for all elements in the ring. Below is pseudo code for an integer arithmetic circuit.

B. Singular results for 2-bit, 3-bit, and 4-bit multipliers

IV. ALGORITHMS AND TECHNIQUES

Techniques for ideal membership testing:

- 1) Setup the verification formulation over the polynomial ring R .
- 2) Declare a specification polynomial from the circuit f_{spec} .
- 3) Derive the polynomials from the gates of the circuit $\{f_1, \dots, f_s\}$.
- 4) Set ideal $J = f_1, \dots, f_s$.
- 5) Create the ideal of vanishing polynomials for each variable $J_0 =$
- 6) Take the Gröbner Basis: $G = \text{GB}(J + J_0)$.
- 7) The circuit implements $f_{\text{spec}} \iff f_{\text{spec}} \in (J + J_0)$ if and only if f_{spec} is divisible by G

The steps to run Singular, ABC, and the Python script are in the README.

V. SOFTWARE IMPLEMENTATIONS

We implemented a Python function with assistance from ChatGPT to convert blif files to sing files. The code defines a gate mapping dictionary that maps gate types from the blif file to their corresponding names in Singular. It iterates

Algorithm 1 Example Singular code for arithmetic circuit

```
// Declare ring
ring R = 0, (outputs, internal outputs, inputs), lp;

// Declare  $f_{spec}$  and polys of internal gates
poly  $f_{spec}$  = specification equation of the circuit;
//  $f_4$  is an example of a polynomial describing gate behavior
//  $z$  is an output,  $s$  and  $e$  are internal signals
//  $z = s_0 - e_0 + 2*s_0*e_0$ 
poly  $f_4 = z_0 - s_0 - e_0 + 2*s_0*e_0$ ;
//Continue to model logic gates over Q

// Declare ideals
ideal J = f4, f5, f6, f7, f8, f9, f10, f11, f12, f13, f14, f15, f16;
ideal J0 = vanishing polynomials;

//Finding Gröbner Basis of the ideals plus the vanishing
polynomials
groebner(J + J0);

//Membership test using a condition checking statement to
explicitly state membership
NF( $f_{spec}$ , J + J0, 1);
//Can put a response here to print confirmation of member-
ship
```

through and searches for lines starting with '.gate' and extracts the gate type and its inputs, parsing and separating them accordingly into the Singular file. Additionally, we added code for error handling because the Singular file was empty when experimenting.

VI. CONCEPTS LEARNED

A. Mathematical Ideals

Ideals ensure the accuracy of electronic systems In circuit testing and verification. Ideal membership testing involves using mathematical models to assess whether a circuit aligns with specified ideal characteristics. Engineers compare these models with real-world circuit implementations to identify discrepancies to help detect potential faults in the design. This approach enhances precision and provides a systematic framework for validating complex circuits, contributing to the development of high-quality electronic systems.

B. Gröbner Basis

Gröbner Basis in-circuit testing and verification is a powerful method that involves algebraic techniques to analyze and validate complex electronic systems. Gröbner Bases provide a systematic way to address polynomial equations representing circuit behaviors. Gröbner Bases are a fundamental concept in algebraic geometry and computer algebra systems, and they play a crucial role in solving systems of polynomial equations. The primary idea behind Gröbner Bases is to provide a

Algorithm 2 Convert BLIF to Singular

```
if content exists then
  map gates
  for each line in blif file do
    if line starts with ".gate" then
      gate_type, gate_inputs  $\leftarrow$  parse line
      if gate_type EXISTS IN gate_map then
        Generate Singular code based on gate_type and
        gate_inputs
      end if
    end if
  end for
  if singular_code is NOT EMPTY then
    write singular_code TO output_file_path
    print "Singular code written to output_file_path"
  else
    print "No valid Singular code generated. Check the
    BLIF file content."
  end if
else
  print "File 'file_path' not found."
end if
end function
```

systematic method for transforming a set of polynomials into a more manageable and structured form.

C. blif to sing conversion

By using a python script to parse our mapped blif files (lib2.genlib), we can convert the list of gates contained in the blif file to a list of corresponding polynomials for our sing file. By splitting the blif file line by line and parsing for key words such as ".gate," "XOR," "NAND," and "INV" to create the different polynomial equations to model logic gates over Q. For example, "XOR" uses the equation $z = a - b + 2ab$, and "AND" uses the equation $z = a * b$ for the corresponding polynomials. Python makes this very easy with its parsing functionalities.

D. Ideal Membership Testing

Ideal membership testing is a mathematical approach used in circuit verification to determine whether a given circuit satisfies ideal properties or conditions. It involves algebraic structures known as ideals, particularly in the context of polynomial rings. An ideal is a subset of the polynomial ring that consists of all polynomials that satisfy certain conditions. In the context of circuit verification, the ideal encapsulates the set of polynomials representing the desired ideal behavior of the circuit. The core of the process involves determining whether a given polynomial, representing the behavior of the actual circuit, belongs to the ideal. If the polynomial is an element of the ideal, it indicates that the circuit satisfies the ideal properties. Otherwise, it suggests a deviation from the expected behavior.

E. Mitters

Mitters play a crucial role in circuit testing and verification. A model of the circuit is integrated into the testing process, allowing for comprehensive analysis. The miter compares the expected behavior with the actual circuit response using an xor gate to highlighting any discrepancies based on the model. By using mitters, we can identify and address potential issues before moving to further stages of development or production, ensuring that the circuit functions as intended.

VII. LABOUR DIVISION

- Jonathan: Generated the blif files and converted it to Singular files and wrote the report
- Henry: Debugged Python Code and helped write report
- Garrett: Help write the report
- Dmitri: Provided Singular code for 2-bit,3-bit and 4-bit multipliers and visuals

REFERENCES

- [1] D. Ritirc, A. Biere and M. Kauers, "Column-wise verification of multipliers using computer algebra," 2017 Formal Methods in Computer Aided Design (FMCAD), Vienna, Austria, 2017, pp. 23-30, doi: 10.23919/FMCAD.2017.8102237.
- [2] T. Pruss, P. Kalla and F. Enescu, "Efficient Symbolic Computation for Word-Level Abstraction From Combinational Circuits for Verification Over Finite Fields," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 35, no. 7, pp. 1206-1218, July 2016, doi: 10.1109/TCAD.2015.2501301.
- [3] Jerry R. Burch. 1991. Using BDDs to verify multipliers. In Proceedings of the 28th ACM/IEEE Design Automation Conference (DAC '91). Association for Computing Machinery, New York, NY, USA, 408–412. <https://doi.org/10.1145/127601.127703>