Improving Compiler Optimizations using Program Annotations

BY

NIKO ZARZANI
Laurea, Politecnico di Milano, Milan, Italy, 2011

THESIS

Submitted as partial fulfillment of the requirements
for the degree of Master of Science in Computer Science
in the Graduate College of the
University of Illinois at Chicago, 2014

Chicago, Illinois

Defense Committee:

Lenore D. Zuck, Chair and Advisor
V.N. Venkatakrishnan
Marco Santambrogio, Politecnico di Milano

To my family.

To my girlfriend.

To my friends.

ACKNOWLEDGEMENTS

I would like to thank:

Dr. Lenore D. Zuck, my advisor, for her guidance and advice throughout the course of this Master and the thesis. Thank you so much for believing in my abilities and supporting me.

Dr. Venkat N. Venkatakrishnan who was always available to meet and help me and greatly contributed to the development of this thesis. Dr. Rigel Gjomemo and Dr. Phu H. H. Phung who have been helping me since the beginning of my work.

My parents and my sister, for their precious support, encouragment and understanding through the past few years.

My girlfriend Camilla Muzi for her endless love and for making me feel like anything was possible. I could not have made through this journey without you by my side.

My closest friends Ilaria Stronati, Carolina Moroni, Elisa Biondini, Riccardo De Gennaro and Marco Sabbatini for our special long-distance friendship and all the laughing conversations. My current and past nerd roommates for their friendships and hacking support. The last few years have been quite an experience and you have all made it a memorable time of my life. I will miss you all.

Everyone who helped me and supported me during my Master Degree.

NZ

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

CHAPTER **PAGE**

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACSL ANSI/ISO C Specification Language. vii, 8, 11, 14–17

AST Abstract Syntax Tree. vii, 16, 17

CFG Control Flow Graph. vii, 30

CSFV Crowd Source Formal Verification. vii, 6

IR Intermediate Representation. vii, 3, 4, 7, 9, 10

JML Java Modeling Language. vii, 8

LLVM Low Level Virtual Machine. vii, 9, 10, 12, 17, 19, 20, 22, 28

RTTI Run-Time Type Information. vii, 17

SC Source Code. vii, 3, 4, 7

SSA Static Single Assignment. vii, 9, 20, 30

SUMMARY

In this work we describe a framework that combines the results of from program testing, formal verification and compiler optimization. We focus on how the informations manually provided by the developer, by crowd source formal verification or by static formal verification tools can be used to help the compilation process.

This framework is built on top of the LLVM architecture and can be useful to software developers as it will improve performance while significantly enhancing security. By using the results coming from program analyzer's analysis we show how our framework can reduce the overhead incurred to ensure array bounds checking and how it can help compiler analysis and improve compiler optimizations.

CHAPTER 1

INTRODUCTION

Many programming tools can help the programmer during the application development. Among them there are tools used to test program correctness, tools for program safety and tools for code optimization and transformation.

During the transformation of the source code into a target language compilers enable the code generated to work more efficient and use fewer resources. In addition they can also be used to enable program safety by inserting run-time checks to avoid common security flaws.

Formal verification tools can be helpful in proving the correctness of software expressed as source code. They allows to verify that the source code complies with a provided formal specification. These tools implement powerful analysis that can compute information automatically from the source code of a program, allowing the programmer to verify that the code satisfies a formal specification. This in turn, enables program verification faster and less risky than code review. Much research was done in program analysis in order to obtain formal proof of program behaviors. Unlike analysis implemented in compilers, this kind of analysis has a high time and space complexity.

Programmers often insert runtime checks in their programs and build assertion enabled version of their projects. This version is tested at runtime and programmers expect the

behavior of the program to comply with the properties specified in those assertions before the code will be removed in production.

The rest of the dissertation is organized as follows:

Chapter 2 describes what we mean for annotated code, its major sources and some of the basic compiler concepts needed to understand this work.

Chapter 3 describes in detail our approach and gives an overview of the framework.

Chapter 4 describes the framework implementation.

Chapter 5 presents an evaluation of this work.

Chapter 7 discusses the limitations and future work, and we conclude in Chapter 6.

CHAPTER 2

BACKGROUND

In this chapter we introduce the basic concepts underlying the rest of this thesis. We will give a general overview of what we mean by *program annotation* and the different sources of annotated code. In addition we briefly cover the necessary concepts of a compiler architecture that motivate the design choices during the implementation of this work.

2.1 Annotated Code

Programs may contain useful informations that is often ignored by modern compilers. *Program annotation* refers to annotation either in Source Code (SC) or Intermediate Representation (IR) with additional informations that does not affect the semantic of the program. Usually these annotations are inserted as comments in the program SC or as metadata informations in the program IR.

2.2 Sources of annotated code

There are several sources of annotations that can be used to improve compiler optimizations. We choose to classify them by the way they are generated:

- *Manually Generated*: this kind of annotations requires the programmer to specify the information inside the program SC.

  The programmer is responsible for the correctness of the information contained in each specified annotation.

- *Automatically Generated*: this kind of annotations comes from analysis programs and does not require any human effort during the generation of the annotated code. They can be generated both inside the program SC or IR.

  The correctness of the information contained in each annotation relies on the correctness of the program analysis and its implementation.

- *Crowd Generated*: this last kind of generation is somewhat in between manual and automatic generation but does not require any effort from the programmer. It relies on humans generating formal proved annotations by means of software tools. Therefore the program annotation is crowdsourced. These tools may not directly expose the program to the user, for example they may show an equivalent model with a different representation.

  The correctness of the information contained in the annotation relies on the correctness of the tool used by the crowd of human annotators.

In the next subsections we are going to give some examples of program annotation and their corresponding annotated code.

2.2.1 Programmer's annotation

Developer's annotation are usually inserted in the code in order to support the software design and to test the correct program behavior.

Common annotations that can be used to improve optimizations are:

- *Design by contract*: software designers commonly define formal, precise and verifiable interface specifications for software components, which extend the ordinary definition of abstract data types with preconditions, postconditions and invariants. In languages such as Eiffel[1] it is part of the design process and required in the implementation.

  Listing 2.1 presents a trivial C example showing a precondition that can be used to remove an if-else statement.

Listing 2.1: Precondition useful for optimization

```
1   /*@
2           requires x > y;
3           requires y > 0;
4   */
5   int foo(int x, int y){
6           if ( x > 0 ){
7                   return x+y;
8           }
9           else {
10                  return -1;
11          }
12  }
```

- *Assertions*: an assertion is a predicate (a statement containing a boolean expression) placed in a program to indicate that the developer believes the predicate to hold when control reaches this location. An assertion that evaluates to false at run-time typically causes execution to abort. Usually, developers expect the behavior of the program to comply with the properties specified in those assertions, so that code can be removed in production. The correct execution of the program relies on these properties, therefore they may be used to improve code optimizations.

In Listing 2.2 we present a trivial C example showing an assertion that can be used to remove an if-else statement.

Listing 2.2: Assertion useful for optimization

```
1     int foo(int x, int y){
2             assert( (x > y) && (y > 0) );
3             if ( x > 0 ){
4                     return x+y;
5             }
6             else {
7                     return -1;
8             }
9     }
```

2.2.2 Crowd Source Formal Verification

Nowadays crowd-sourcing problems that are hard to analyze seems to be a promising idea. Many interesting applications[2] such as OpenStreetMap and Recaptcha rely on volunteer work to solve complex analysis.

An example of crowd annotation generation is Crowd Source Formal Verification (CSFV)[3], a program that seeks to make formal program verification more cost-effective by reducing the skill set required for verification. An automated game-level builder transforms the program verification models into compelling games. The CSFV annotation process is shown in Figure 1. A particular game instance is a function of the program verification tool, the property to be verified and the program being verified. Each game instance is released to the crowd, either via the Web or through internal domain distribution. Game solutions collected in this way are then used to populate a database.

A reverse mapping is done to insert back into a program annotations sufficient to allow a verification tool to make progress toward verifying a specific program property.

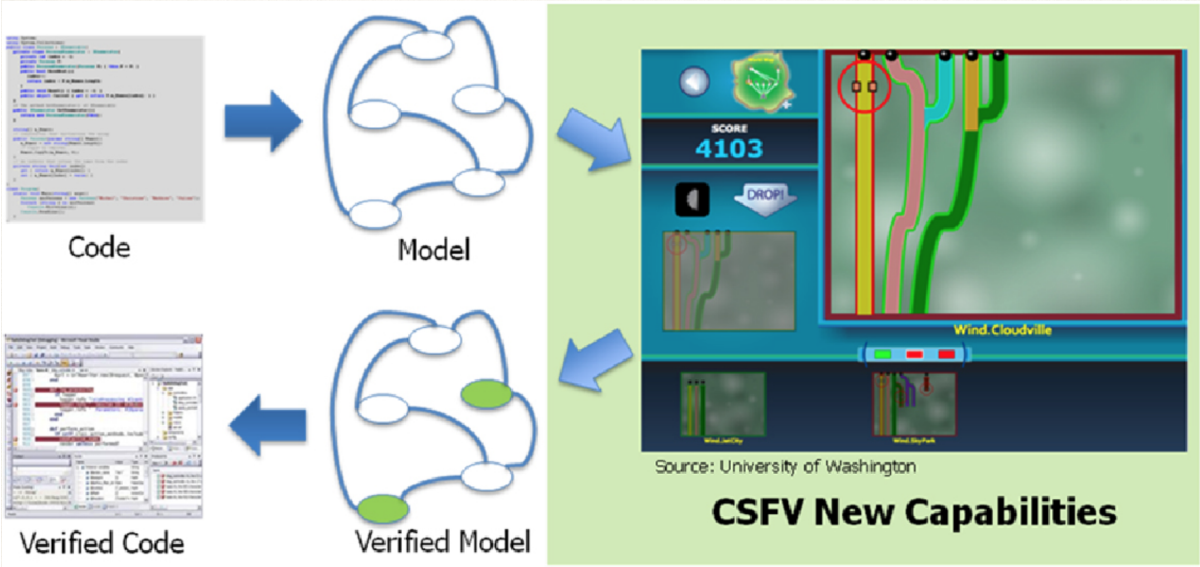

Figure 1: Crowd source formal verification

2.2.3 Program Analyzers

Program analyzers automatically analyze the behavior of programs. They are able to generate informations that can be automatically inserted in the program SC or IR. Different program analysis, such as weakest precondition calculus and value analysis, can be helpful both for testing the correctness of a program and for optimizing it. In addition, they can aid developers debugging.

In Chapter 3 we will describe a framework that uses the information coming from a program analyzer in order to improver the compilation process.

2.3 Annotation Language

By *annotation languages* we mean program behavioral specification languages. An annotation language should be able to express a wide range of functional properties. Standard annotation languages such as the ANSI/ISO C Specification Language (ACSL)[4] for C and the Java Modeling Language (JML)[5] for Java are widely used during software development.

Annotation languages offer a standard information representation that can be also used by program analyzers both as an input to verify properties and as an output to insert additional information in the code.

2.4 Compiler Architecture

A typical compiler structure is composed of two subsystems, the *front-end* and the *back-end*. This structure is shown in Figure 2.

The intermediate representation is independent of the specific source or machine languages and acts as an interface between the front-end and back-end.

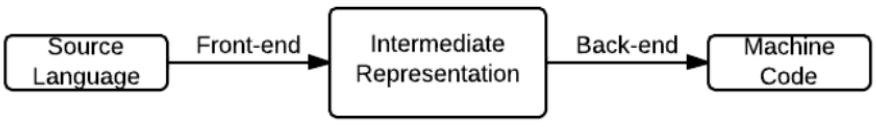

Figure 2: Typical compiler structure

The major advantage of this split are that it is easier to design back-ends that are independent of input source language and vice-versa for front ends with respect to machine properties: suppose there are N target source languages and M target machines. This approach allows for $N + M$ (front-end , back-end) pairs instead of $N \times M$ whole compilers for every (source language, machine) pair.

Section 2.4.2 describe the basic modules of the LLVM architecture used in our framework.

2.4.1 Static Single Assignment Form

The Static Single Assignment (SSA) form[6] is a property of an intermediate representation, where each variable is assigned exactly once. Existing variables in the original IR are split into multiple variables. These new variables typically indicated by the original name with a subscript in textbooks[7], so that every definition gets its own version. However, as we will see in later code examples, in LLVM they usually take the name of the operation that is performed. This form usually simplifies data-flow analysis and program optimizations and reduces the space and time complexity needed while following def-use chains.

In Listings 2.3, 2.4 and 2.5 follow a simple example of code translated into SSA form.

Listing 2.3: SSA Example

```
...
x = y * z;
y = x + 3;
x = y + 4;
z = y * 5;
x = x + z;
...
```

Listing 2.4: SSA Example Textbook IR

```
...
x1 = y1 * z1;
y2 = x1 + 3;
x2 = y2 + 4;
z2 = y2 * 5;
x3 = x2 + z2;
...
```

Listing 2.5: SSA Example LLVM IR

```
...
%mul = mul nsw i32 %y, %z
%add = add nsw i32 %mul, 3
%add1 = add nsw i32 %add, 4
%mul2 = mul nsw i32 %add, 5
%add3 = add nsw i32 %add1, %mul2
...
```

Usually compilers first convert the program into an IR SSA form, then perform the optimization passes and in the end they translate the IR into machine code.

2.4.2 LLVM

Since in our implementation we are using program written in C as benchmarks we choose to target the Low Level Virtual Machine (LLVM) Architecture[8][9]. The LLVM Project is a collection of modular and reusable compiler tools. In this work we show how we modified both the LLVM Core and the SAFECode project (that is built using the LLVM compiler infrastructure) so to reduce the trade-off between security and execution time of a compiled program and improve current compiler optimizations.

The main LLVM tools and concepts used here:

- *Clang*[10] is C, C++, Objective C and Objective C++ front-end for the LLVM compiler. It can be use to emit LLVM IR that can be later used to optimize and compile the code.
- *LLVM IR*[11] is a SSA based representation that allows many source languages to be mapped to them. It is the common code representation used throughout all phases of the LLVM compilation strategy and acts like an interface between the LLVM Core Passes.
- *LLVM Core*[12] are a set of libraries that provide a modern source-independent and target-independent optimizer, along with code generation support for many CPUs. These libraries are built around the LLVM IR. Optimizations are implemented as Passes[13] that traverse some portion of a program (such as functions, loops and basic blocks) to either collect information or transform the program.
- SAFECode[14] project is a memory safety compiler built on top of LLVM. It can be used to protect software from security attacks. It instruments code with run-time checks to detect memory safety errors (e.g., buffer overflows) at run-time.

CHAPTER 3

APPROACH

This Chapter describes what is the aim of this work.

3.1 Goals and challenges

We seek to demonstrate how the annotations in the source code can be used during the compilation process and how to achieve better code performances by relying on them.

We are not concerned with time of the compilation process. Of course, the generation of code with annotation can take time and analysis algorithm can have an high complexity, however here we are only focusing in taking advantage of already annotated code (that can come from different sources as seen in Section 2.2).

In order to test our approach we use formal verification tool for C programs, Frama-C[15]. In particular we use the results of Frama-C's *Value Analysis*[16] plug-in and embedding these results in the source code.

To make our framework more general and highly reusable we are supporting annotations written in the standard ACSL, so that our back-end can use also information from different kind of analyses or sources.

In addition we show how these achievements can be obtained in a real world state-of-the-art compiler such as LLVM and in some real-world C programs described in Sec-

tion 4.1.2. We will see in detail in Chapter 4 how we are facing the challenge of plugging our annotation in the IR in order to make them useful for optimization Passes.

3.2 Overview

This section describes two aspects of the compilation process that we are willing to enhance: program security and performance.

3.2.1 Lightweight Run-time Checks Injection

In order to strengthen security, the LLVM SAFECode Project is designed to prevent pointers from overflowing from one memory object into another by inserting run-time array bounds checks into the program code. This prevents buffer overflows, one of the major *mitre25*[17] vulnerabilities. However, this comes at the cost of a trade-off between security and code performance. In Section 3.3.2 we show how we used the informations coming from program annotation to reduce the cost of this trade-off.

3.2.2 Pushing Current Optimizations Forward

For efficiency's sake, the existing optimizations rely on mostly linear, rarely quadratic, analysis algorithm. This is especially true with the advent of just-in-time compilation. For example in the GCC Developer Wiki[18] there is specified not to add algorithms with quadratic or worse behavior.

Since we are relying on existing additional information that can be generated by more powerful kind of analysis, we believe that this information can be used for new optimizations or can improve already existing ones. We will focus on modifying current LLVM optimizations.

3.3 Details

This section generally illustrates the basic modules of our framework and how they are chained together to achieve the desired improvements.

3.3.1 Annotated Programs Generation

Frama-C[15] has a plug-in called *Value analysis*[16] that computes variation domains for variables. This plug-in uses abstract interpretation techniques and it handles a wide spectrum of C constructs. The Frama-C graphical user interface displays the inferred sets for possible values of a variable in each point of the analyzed program. This plug-in give us information about variables before and after the selected line of code.

A custom Frama-C plug-in captures the result from *Value analysis* plug-in, log them in a separate file and then reinsert them in the original C source code as ACSL annotations.

3.3.2 Lightweight Safecode Pipeline

Since we need to associate each information about index of array accesses to the correct array access instructions, we created the pipeline of passes showed in Figure 3. Information about the index in array accesses might allow us to remove the check if the variable is always in bounds.

After the memory to register promotion a pass will map the array index in the source code to the corresponding register in the IR. Then it will attach a metadata with the information about the range of the register used for the access (if any) to the instructions used for the access. The later Safecode passes are then modified so that these information are used to the inspect each injection and to decide if the checks are really needed or not.

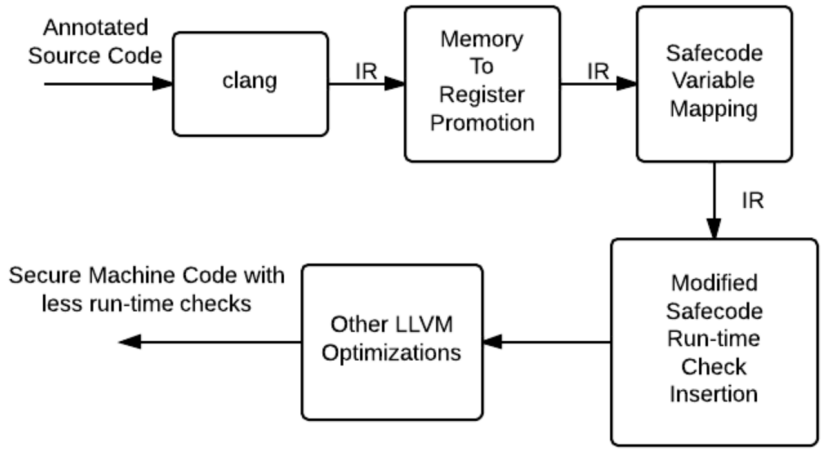

Figure 3: Lightweight safecode Pipeline

3.3.3 LLVM New Optimizations pipeline

In order to push the information in the source code annotations throughout the compiler architecture, we designed a pipeline of steps that is showed in Figure 4.

- *From source code to IR*

  The annotations placed in the source code as strings are translated by *clang* into the IR as global constant strings. An example is showed in Listing 3.1.

Listing 3.1: String Annotation Example

```
1 @.str = private unnamed_addr constant [15 x i8] c"@assert␣k␣==␣1\00", align 1
```

  Clang inserts debug informations that are later used during the following pipeline steps.

- *Memory to Register*

  The string declared and defined in the source code is removed after the memory to register promotion, hence we are justified in ignoring code size effects of the choice. However, the debug information is preserved at the same line of code where the strings were declared and defined, hence we still have additional informations in the IR ready to be used.

- *Mapping Annotation Variables to Registers*

  The annotations contain information about source code variables, however at this stage of the pipeline the source code variables are already associated to SSA registers. Our pass scans the debug information in the IR and performs and update the annotation variables accordingly to the correct mapping.

- *Modified Constant Propagation*

  We modified the LLVM Constant Propagation Transformation Pass so it depends on constant information from annotated source code.

- *Modified Lazy Value Informations*

  We modified the LLVM Lazy Value Info Analysis Pass so to consider constant and range informations from the annotated source code.

- *Run optimizations dependent on value analysis*

  We run both Correlated Value Propagation and Jump Threading since that depend on the modified Lazy Value Info Analysis.

- *Other LLVM Optimizations*

  We strip the debug informations and run the "normal" LLVM optimizations to obtain the optimized code. These later optimizations can also benefit by the improved modified optimizations and make more effective changes.

The choice of the passes order is a constraint due to the propagation of the annotation information throughout the transformation passes. In Chapter 7 we describe how to remove this constraint.

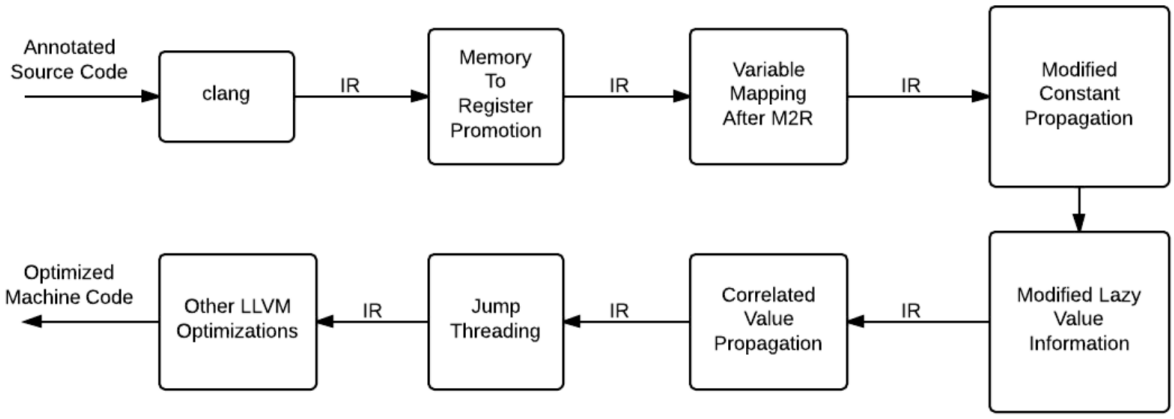

Figure 4: LLVM new optimizations pipeline

CHAPTER 4

IMPLEMENTATION

In this chapter we are going to present the most interesting details about the implementation of this work. We are going to explain how the annotated code was generated, the different components of the Safecode and optimization pipelines and some insights about how the engineering hurdles where handled.

4.1 Annotated Code Data Collection

Here we present how we are automatically generating some C programs with annotations to test our approach. The framework can take every program already annotated (also manually) and trust the additional informations coming from the annotation to improve the existing optimizations.

4.1.1 Frama-C Annotations

Frama-C annotations are only available via the GUI interface. To bring these information into the source code, we implemented a Frama-C plug-in to perform the work.

This plug-in visits every assignment and function call instruction in the AST tree in Frama-C, extracts all variables and queries the value analysis plug-in for each variable to get the possible values. In this work we are only interested in constant and range bounds of a variable, we ignored other information of complex variables such as structs, arrays or pointers. These information are inserted as string in ACSL language into the C source

code via a dummy string variable before and/or after the inspected instruction whenever the information from the Value Analysis plug-in is available.

Frama-C merges multiple file into a single file. This will change the multiple file programs structure and might causes compiling issues of large programs. In order to handle multiple files programs we log the value information into a file together with the location and type of instructions in original source file and then we inject the dummy string variable matching the location and type of an instruction stored in the log file via a custom CIL[19] plugin.

4.1.2 Benchmarks used

In order to evaluate this work we annotated some C programs using the custom plugin mentioned in Section 4.1.1. Here it follows a short description of the benchmarks used:

- CoreMark is a benchmark that aims to measure the performance of CPU used in embedded systems. The code contains implementations of list processing (find and sort) and matrix manipulation (common matrix operations) algorithms.
- SUSAN is a benchmark that implements algorithms based on Smallest Univalue Segment Assimilating Nucleus. The SUSAN algorithms cover image noise filtering, edge finding and corner findi
- MxM is a benchmark that computes matrix-matrix products in multiple different ways.

- Linpack is a benchmark that implements algorithms for vector sum, vector product, scaling vectors by a constant, matrix factorization, solving linear systems and random number generation.
- NEC-Matrix is a small benchmark that contains the implementation scalar product and some multiplication and addition over matrices.

4.2 Pushing the annotations through the CLANG front-end

The annotations inserted in the code as ACSL comments are ignored and removed by the clang C front-end. Therefore, in order to keep this informations in the very first stages of the back-end compilation process, the annotations are inserted in the C program as C strings. This choice was done because since these strings are just dead code they will be easily removed during later optimizations.

4.3 The ACSL Parser

To the extent of handling different kinds of annotations and parse them we wrote an ACSL parser that builds an Abstract Syntax Tree (AST) out of every annotation string in input. For our purposes we are supporting only a small set of annotation, however the grammar can be easily extended to support a broader variety of ACSL constructs.

4.3.1 ACSL Supported Subset

We are currently supporting preconditions (*@requires*), postconditions (*@ensures*) and assertions (*@assert*) containing boolean expressions about variable values. The supported grammar is showed in Appendix A.

In Listing 4.1 we present a simple assertion about variable ranges and constant values:

Listing 4.1: Supported ACSL Example

```
1      @assert i>=0 && i<=10   assert j==0     assert k==1 || k==2
```

4.3.2 Parser Generation

The ACSL parser is an automatically generated using *Flex* (a scanner generator) and *Bison* (a parser generator) tools. The reason to use these tools is that the code generated by them requires no compile-time dependencies, because they generate fully autonomous source code. In addition we do not need to rewrite all the ACSL parser but we only need to modify the files used from these tools to handle new ACSL constructs. Therefore it will be really easier to augment the parser just by learning how to use these common tools.

The output from the *Flex* scanner and *Bison* parser pair is encapsulated into classes in order to incorporate it into a modern C++ program as LLVM. Precisely the class that which puts together lexer and parser is the *Driver* class. The *Driver* class is independent from the automatically generated files and exposes methods to get the AST given as an input a string, a file or a stream.

4.3.3 The ACSL AST

The diagram of the classes that compose the ACSL AST are shown in Figure 5.

All the classes in the diagram implement the LLVM style Run-Time Type Information (RTTI) that can be used to runtime check the generated structure of the AST. In addition the *ACSLNode* class has a few methods useful for extracting the list of variables in the

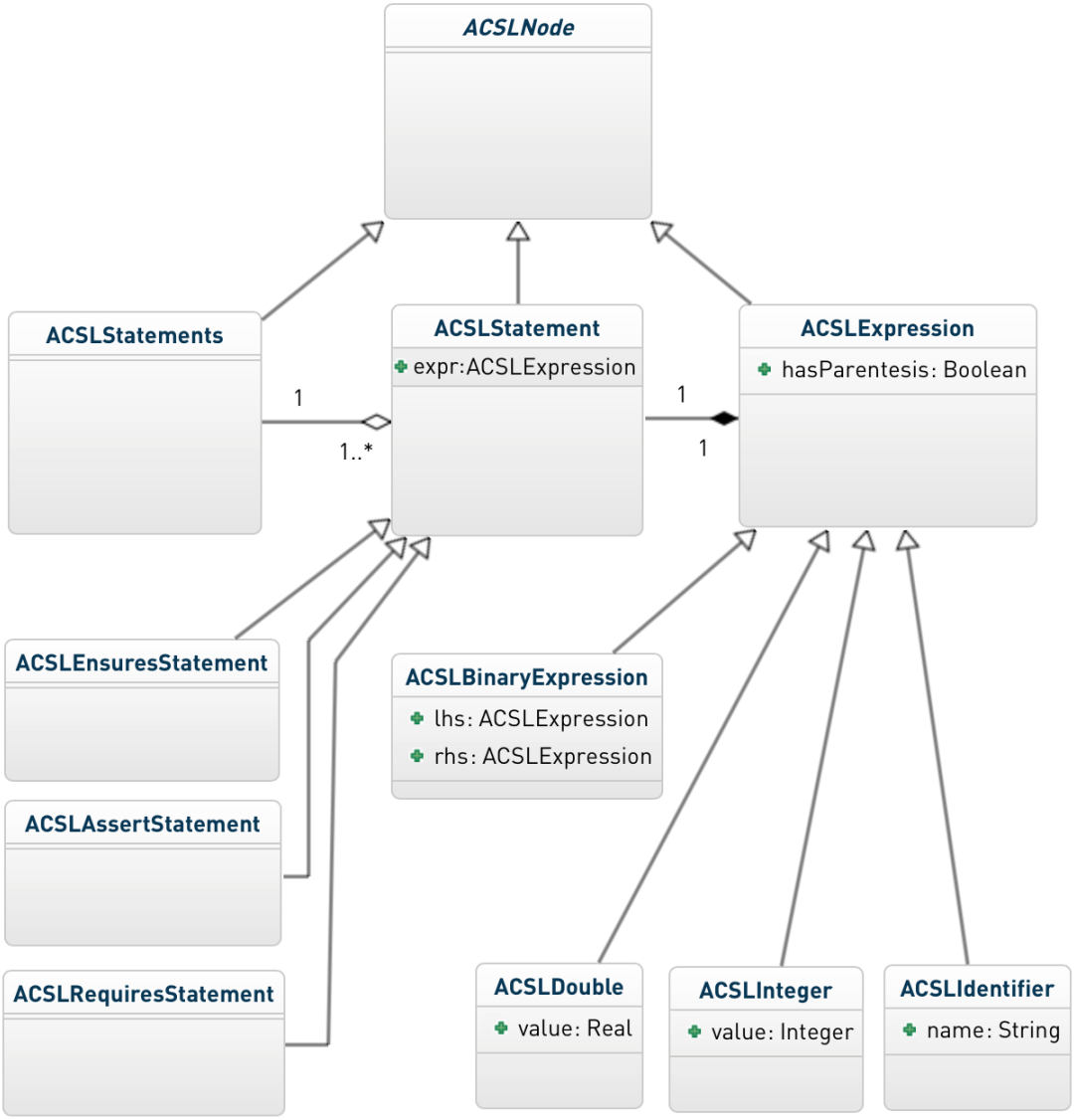

Figure 5: ACSL AST class diagram.

parsed annotation and to rename them (we will see in Section 4.4 why we need variable renaming).

4.4 Mapping Source Code Variables to IR Variables

During the front-end compilation into LLVM IR every source code variable declaration is associated a memory location. Every later access to that variable is done via load and store instruction. However if we have a nested scope with a variable name equal to the variable name in a scope on top of that the two memory location will get two different names. In Listing 4.2 and Listing 4.3 we show the issue with a trivial example.

Listing 4.2: Same Name Scope Example

```
int main() {
        //this will be named %x
        int x = 0;
        char * a1 = "@assert x==0";
        if ( x >= 0 ){
                //this will be named %x1
                int x = 1;
                char * a2 = "@assert x==1";
        }
        return x;
}
```

Listing 4.3: Same Name Scope Example IR

```
@.str = private unnamed_addr constant [13 x i8] c"@assert x==0\00", align 1
@.str1 = private unnamed_addr constant [13 x i8] c"@assert x==1\00", align 1
define i32 @main() nounwind ssp uwtable {
        %1 = alloca i32, align 4
        %x = alloca i32, align 4
        %a1 = alloca i8*, align 8
        %x1 = alloca i32, align 4
        %a2 = alloca i8*, align 8
        store i32 0, i32* %1
        store i32 0, i32* %x, align 4
        store i8* getelementptr inbounds ([13 x i8]* @.str, i32 0, i32 0), ...
        %2 = load i32* %x, align 4
        %3 = icmp sgt i32 %2, 0
        br i1 %3, label %4, label %5
        ; <label>:4                                     ; preds = %0
        store i32 1, i32* %x1, align 4
        store i8* getelementptr inbounds ([13 x i8]* @.str1, i32 0, i32 0), ...
        br label %5
        ; <label>:5                                     ; preds = %4, %0
        %6 = load i32* %x, align 4
        ret i32 %6
}
```

In order to map the names of the identifiers in our annotations to the correct names in the IR the *ACSLVarMap* Pass maps the variable to the correct name using debug informations[20] (by running clang with the -g argument). This pass is useful for every optimization that runs before memory to register promotion. In Section 4.4.1 we show how the mapping is done.

The most effective LLVM optimizations run after the *PromoteMemoryToRegister* Pass. This pass promotes memory locations to registers in SSA Form and inserts ϕ functions. In order to use the informations coming from the annotations the *ACSLVarMapAfterM2R* Pass maps every variable to the correct instruction name in the LLVM IR. In Section 4.4.2 we show how the mapping is done.

4.4.1 ACSL Variable Mapping Pass

The *ACSLVarMap* Pass implements an algorithm that decodes the debug information inserted by the front-end and uses them to map the variable names in the source code to the correct memory locations in the IR. This algorithm iterates three times over the function body.

Here follows the implementation details of the two loops:

- *Naming Instrucitons Without Names:*

  Since our implementations relies on instruction names to map variables in the annotations a first loop assign to unnamed instruction a fresh unique name.

- *Gathering Debug Informations:*

  To every allocation instruction (resulting in the memory location of the variable)

corresponds a call to the llvm.dbg.declare function.

The signature *is void %llvm.dbg.declare(metadata, metadata)*. This intrinsic provides information about a local element (e.g., variable): the first argument is metadata holding the allocation for the variable, the second argument is metadata containing a description of the variable. In Listing 4.4 we show a simple example of how it is translated simple *int x = 0;* C statement.

Listing 4.4: llvm.dbg.declare Example

```
1      %x = alloca i32, align 4
2      store i32 0, i32* %x, align 4, !dbg !19
3      ...
4      call void @llvm.dbg.declare(metadata !{i32* %x}, metadata !18), !dbg !19
5      ...
6      !18 = metadata !{i32 786688, metadata !5, metadata !"x", ...
7      !19 = metadata !{i32 7, i32 0, metadata !5, null}
```

In this first loop that iterates over the instructions in every function, we store in a data structure all the informations about:

- Source Code Name
- IR Name
- Source Code Scope

This mapping informations will be used in the following loop.

- *Collecting and Mapping Annotations:*

  To every string annotation in the source code corresponds an allocation instruction, then a store with the corresponding string content. In Listing 4.5 we show a simple

example of how it is translated a simple *char * a = "@assert y==100"* C statement.

Listing 4.5: String Annotation Example

```
1      @.str = private unnamed_addr constant [15 x i8] c"@assert y==100\00", align 1
2      %a = alloca i8*, align 8
3      ...
4      call void @llvm.dbg.declare(metadata !{i8** %a}, metadata !22), !dbg !25
5      ...
6      store i8* getelementptr inbounds ([15 x i8]* @.str, i32 0, i32 0), i8** %a,
           align 8, !dbg !25
```

Once we get the string content we parse it using the *Driver* Class of the ACSL Parser. On the AST we get the list of the variables in the annotations calling the *getTreeVariables* method on the root of the AST. For every variable we solve the mapping using the data structure created in the first loop.

In order to get the correct mapping we iteratively try to solve the variable mapping in the same scope of the annotation, then if we don't find a candidate we start over in the outer scope of the current one.

Finally we substitute in the AST the correct names calling the *changeTreeVariableName* method. This annotations are then attached as a string metadata to the instructions.

4.4.2 Handling Memory to Register Promotion

The LLVM *PromoteMemoryToRegister* Pass converts allocations to registers. An allocation is transformed by using iterated dominator frontiers to place ϕ nodes, then traversing the function in depth-first order to rewrite loads and stores as appropriate. It also propagates

the constant value of declarations immediately followed by a definition (i.e. *int x = 0;*).

A simple example of the IR produced after the *PromoteMemoryToRegister* Pass is showed in Listing 4.6 and Listing 4.7.

Listing 4.6: Memory to Register Example

```
1   int main() {
2
3           int y=100;
4           int x=0;
5
6           char * a1 = "@assert␣x==0";
7           x = y + 1;
8           char * a2 = "@assert␣x==101";
9
10          return x;
11  }
```

Listing 4.7: Memory to Register Example IR

```
1   ...
2   @.str = private unnamed_addr constant [13 x i8] c"@assert␣x==0\00", align 1
3   @.str1 = private unnamed_addr constant [15 x i8] c"@assert␣x==101\00", align 1
4
5   define i32 @main() nounwind ssp uwtable {
6   entry:
7     %add = add nsw i32 100, 1
8     ret i32 %add
9   }
```

In order to correctly map the identifiers in our annotations to the correct registers the *ACSLVarMapAfterM2R* Pass should be run immediately after the *PromoteMemoryToRegister* Pass. The implemented algorithm iterates three times over the function body.

Here follows the implementation details of the four loops:

- *Naming Instrucitons Without Names:*

  As we have seen before since our implementations relies on instruction names to map

variables in the annotations a first loop assign to unnamed instruction a fresh unique name.

- *Gathering Debug Informations:*

  The debug informations are similar to the ones in Section 4.4.1. The difference is that in addition to the llv.dbg.declare calls we are also keeping track of the llvm.dbg.value calls. The signature is *void %llvm.dbg.value(metadata, i64, metadata)*. This intrinsic provides information when a user source variable is set to a new value. The first argument is the new value (wrapped as metadata). The second argument is the offset in the user source variable where the new value is written. The third argument is metadata containing a description of the user source variable. The example in Listing 4.6 after the *PromoteMemoryToRegister* Pass with debug informations is showed Listing 4.8.

Listing 4.8: Debug Information in Memory to Register Example IR

```
1     ...
2     @.str = private unnamed_addr constant [13 x i8] c"@assert␣x==0\00", align 1
3     @.str1 = private unnamed_addr constant [15 x i8] c"@assert␣x==101\00", align 1
4
5     define i32 @main() nounwind ssp uwtable {
6     entry:
7       ;these debug informations are about y and x
8       call void @llvm.dbg.value(metadata !10, i64 0, metadata !11), !dbg !12
9       call void @llvm.dbg.value(metadata !2, i64 0, metadata !13), !dbg !14
10
11      ;this debug info is about the first annotation
12      call void @llvm.dbg.value(metadata !15, i64 0, metadata !16), !dbg !19
13
14      %add = add nsw i32 100, 1, !dbg !20
15
16      ;this debug information is about x
17      call void @llvm.dbg.value(metadata !{i32 %add}, i64 0, metadata !13), !dbg
            !20
18
19      ;this debug info is about the second annotation
20      call void @llvm.dbg.value(metadata !21, i64 0, metadata !22), !dbg !23
21
```

```
22        ret i32 %add, !dbg !32
23      }
24      ...
25      !2 = metadata !{i32 0}
26      ...
27      !10 = metadata !{i32 100}
28      !11 = metadata !{i32 786688, metadata !5, metadata !"y", metadata !6, i32 3,
            metadata !9, i32 0, i32 0}
29      !12 = metadata !{i32 3, i32 0, metadata !5, null}
30      !13 = metadata !{i32 786688, metadata !5, metadata !"x", metadata !6, i32 4,
            metadata !9, i32 0, i32 0}
31      !14 = metadata !{i32 4, i32 0, metadata !5, null}
32      !15 = metadata !{i8* getelementptr inbounds ([13 x i8]* @.str, i32 0, i32 0)}
33      ...
34      !21 = metadata !{i8* getelementptr inbounds ([15 x i8]* @.str1, i32 0, i32 0)}
35      ...
```

In each iteration of this first loop we store in a data structure all the informations about:

- Source Code Name
- IR Name
- Source Code Scope
- Basic Block
- Line of Code

This mapping informations will be used in the third loop.

- *Handling ϕ functions:*

  Registers associated to ϕ functions have no debug informations (since they are not in the original code). However they still are important because they can be the target name of a variable in our annotations.

  In order to handle ϕ functions we should update the data structure with other mapping informations. The source code name is obtained by looking at the arguments

of the ϕ function. Then we add the information in the data structure at the next line of code. In addition if the source code variable is not redefined in the current basic block we push at the beginning of the successors of the current basic block the information about the analyzed ϕ function in the data structure.

- *Collecting and Mapping Annotations:*

  As we can see in Listing 4.6 and Listing 4.7, the allocation and store instruction that we were able to use before the *PromoteMemoryToRegister* Pass to catch the annotations strings are no longer in the IR. Fortunately as we can see in Listing 4.8 we still have a *llvm.dbg.value* call for each annotation string.

  The retrieve annotation will be parsed as in Section 4.4.1. The only difference is in the algorithm to get the correct IR name mapping. We will search backward (looking for a smaller line number) if there is a correct mapping information in the same scope and basic block, if not, we will carry on backward searching in the predecessor to the current basic block until we find a candidate.

4.5 Reducing Safecode Checks

The LLVM BackendUtil class is modified to instrument the pipeline of passes to be run before the already existing Safecode Passes as previously showed in Figure 3. Using a modified version of the *ACSLVarMapAfterM2R* Pass that we called *SafecodeVarMap* Pass we where able to add metadata information to the GetElementPtr (GEP), load and store instructions. This information can be later used in the later Safecode Passes to avoid to check formally proven secure accesses.

4.5.1 Adding information to GEP, LOAD and STORE instructions

If a variable that is inside an annotation is later used in the same basic block as an operand of a GEP, LOAD or STORE instruction, to each of these instructions will be attached a named *acsl_safecode* metadata containing the annotation.

A simple example is showed in Listing 4.9 and Listing 4.10.

Listing 4.9: Array Access Example

```
int main() {
        int a[10];
        int i=0;
        char * a1 = "@assert␣i==0";
        for( i = 0 ; i < 10 ; i++ ){
            char * a2 = "@assert␣i>=0␣&&␣i<10";
            a[i]=i;
        }
        return i;
}
```

Listing 4.10: Array Access Example IR

```
@.str = private unnamed_addr constant [13 x i8] c"@assert␣i==0\00", align 1
@.str1 = private unnamed_addr constant [21 x i8] c"@assert␣i>=0␣&&␣i<10\00", align 1

define i32 @main() nounwind ssp uwtable {
entry:
  %a = alloca [10 x i32], align 16
  call void @llvm.dbg.declare(metadata !{[10 x i32]* %a}, metadata !10), !dbg !14
  ...
  br label %for.cond, !dbg !22

for.cond:                                         ; preds = %for.inc, %entry
  %i.0 = phi i32 [ 0, %entry ], [ %inc, %for.inc ]
  %cmp = icmp slt i32 %i.0, 10, !dbg !22
  br i1 %cmp, label %for.body, label %for.end, !dbg !22

for.body:                                         ; preds = %for.cond
  call void @llvm.dbg.value(metadata !24, i64 0, metadata !25), !dbg !27
  %idxprom = sext i32 %i.0 to i64, !dbg !28
  %arrayidx = getelementptr inbounds [10 x i32]* %a, i32 0, i64 %idxprom, !dbg !28
  store i32 %i.0, i32* %arrayidx, align 4, !dbg !28
  br label %for.inc, !dbg !29

for.inc:                                          ; preds = %for.body
  %inc = add nsw i32 %i.0, 1, !dbg !22
  call void @llvm.dbg.value(metadata !{i32 %inc}, i64 0, metadata !15), !dbg !22
  br label %for.cond, !dbg !22
```

```
27
28      for.end:                                          ; preds = %for.cond
29        ret i32 %i.0, !dbg !30
30      }
```

We are supporting accesses to arrays of fixed size created using statements of the type "*int array[10];*" and "*int * array = malloc(10 * sizeof(int));*" of any type.

In addition, if the index of the access is the result of an expression (for example "*array[i*j+2]*"), we are currently propagating the ranges information to the SSA registers following the annotation in the same basic block. This is done using simple interval operations described in Appendix B.

The same is done for array whose size is the result of an expression (for example "*int array[i*j]*"). The minimum size coming from the range information propagation is used. This means that we are not injecting the check only if the array index is in bound considering the smallest size.

We are also keeping into account the sign extension of integer types (SEXT) in order to attach the annotation to the correct GEP, LOAD or STORE instruction. The sign extension is needed for example when we are using in 32bit integer to access a 64bit indexed array. The resulting modified IR code is shown in Listing 4.11.

Listing 4.11: Array Access Example IR After SafecodeVarMap

```
1       ...
2       %arrayidx = getelementptr inbounds [10 x i32]* %a, i32 0, i64 %idxprom, !dbg !32, !
            acsl_safecode !30
3       store i32 %i.0, i32* %arrayidx, align 4, !dbg !32, !acsl_safecode !30
4       ...
5       !30 = metadata !{metadata !"assert␣i.0␣>=␣0␣&&␣i.0␣<␣10\0A"}
```

In Listing 4.12 we show an example of how, by attaching these metadatas to the single accesses, we are be able to instrument with our additional information also statement with multiple array accesses in a single line of code.

Listing 4.12: Multiple Array Access Example

```
...
char * a1 = "@assert␣i>=0␣&&␣i<=10";
char * a2 = "@assert␣j>=0␣&&␣j<=5";
array[i] = array[i]+array2[j];
...
```

Listing 4.13: Multiple Array Access Example IR

```
...
%array = alloca [10 x i32], align 16
%array2 = alloca [5 x i32], align 16
%idxprom = sext i32 %i to i64, !dbg !34
%arrayidx = getelementptr inbounds [10 x i32]* %array, i32 0, i64 %idxprom, !dbg
    !34, !acsl_safecode !35
%0 = load i32* %arrayidx, align 4, !dbg !34, !acsl_safecode !35
%idxprom1 = sext i32 %j to i64, !dbg !34
%arrayidx2 = getelementptr inbounds [5 x i32]* %array2, i32 0, i64 %idxprom1, !dbg
    !34, !acsl_safecode !36
%1 = load i32* %arrayidx2, align 4, !dbg !34, !acsl_safecode !36
%add = add nsw i32 %0, %1, !dbg !34
%idxprom3 = sext i32 %i to i64, !dbg !34
%arrayidx4 = getelementptr inbounds [10 x i32]* %array, i32 0, i64 %idxprom3, !dbg
    !34, !acsl_safecode !35
store i32 %add, i32* %arrayidx4, align 4, !dbg !34, !acsl_safecode !35
...
!35 = metadata !{metadata !"assert␣i␣>=␣0␣&&␣i␣<=␣10"}
!36 = metadata !{metadata !"assert␣j␣>=␣0␣&&␣j␣<=␣5"}
```

4.5.2 Modifying Safecode to use the annotations

The Safecode *InsertGEPChecks* Pass and the *visitLoad* and *visitStore* methods of the *InstrumentMemoryAccesses* Pass are modified in a way that every time they are trying to insert checks for an out of bounds access they will test if there is a metadata containing a variable range or constant value. If the access using the GEP, LOAD or STORE instruction

is safe (the operand is in the bounds of the array length) we can avoid to insert the check without loosing security margin.

4.6 Backend Optimizations

In this section we are analyzing existing LLVM optimizations and analysis and showing how to insert the additional informations coming from the existing annotations inside these Passes. These Passes runs after the *PromoteMemoryToRegister* Pass so we need our *ACSLVarMapAfterM2R* Pass to be run immediately after it and before the other Passes we modified. Another approach could also be writing new optimization Passes from scratch based on these annotations.

Here we focus on the LLVM *Simple Constant Propagation* Transformation Pass and the *Lazy Value Information* Analysis Pass.

4.6.1 Improving Simple Constant Propagation Transformation Pass

The *Simple Constant Propagation* Transformation Pass implements constant propagation and merging. It searches for instructions involving only constant operands and replaces them with a constant value instead of an instruction. An example is showed in Listing 4.14 and Listing 4.15.

Listing 4.14: Before Simple Constant Propagation

```
1     ...
2     add i32 3, 4
3     ...
```

Listing 4.15: After Simple Constant Propagation

```
...
i32 7
...
```

Since this pass could make definitions be dead the Dead Instruction Elimination is usually run after it.

This Pass runs on every function, it first inserts all the instructions in a work-list, then iterates on each of them and if their operands are constant it change them and propagates them replacing them in all their uses. A little code snippets is showed in Listing 4.16.

Listing 4.16: Simple Constant Propagation Implementation

```
while (!WorkList.empty()) {
        Instruction *I = *WorkList.begin();
        WorkList.erase(WorkList.begin());    // Get an element from the worklist...

        if (!I->use_empty())                 // Don't muck with dead instructions...
                if (Constant *C = ConstantFoldInstruction(I, TD, TLI)) {
                        // Add all of the users of this instruction to the worklist,
                             they might be constant propagatable now...
                        for (Value::use_iterator UI = I->use_begin(), UE = I->
                            use_end();
                             UI != UE; ++UI)
                          WorkList.insert(cast<Instruction>(*UI));

                        // Replace all of the uses of a variable with uses of the
                            constant.
                        I->replaceAllUsesWith(C);

                        // Remove the dead instruction.
                        WorkList.erase(I);
                        I->eraseFromParent();
                }
}
```

Since we can have some annotations in our code about constant variables (such as *"assert x==7"* that the after the mapping could become *"assert add == 7"*) we modified the implementation in order to improve the Pass optimization. The general annotation used is

shown in Listing 4.17.

Listing 4.17: Constant Annotation Used

```
1       @assert value == const
```

After the *PromoteMemoryToRegister* and *ACSLVarMapAfterM2R* Pass every annotation now is about an identifier in SSA form. This means that we can propagate that value in the current basic block and all the others reachable from that basic block. We cannot simply propagate the SSA register in all its uses since the annotation only holds from that point and in the other basic blocks that come after in the Control Flow Graph (CFG) flow.

Therefore we modified the Pass in order to check not only if the instruction was "constant foldable" but also if there is an annotation asserting that that instruction has a constant value. As it happens in the original code the instructions where the value is propagated will be again inserted in the work-list to enable other cascading propagations and if the value gets propagated in all its users it will be removed. In addition our modified constant propagation also take into account the annotations about function arguments. If an argument is always used with a certain constant value also that value can be propagated.

Listing 4.18: Constant Propagation Example

```
#include <stdio.h>
int greaterThanZero(int x)
{
    if (x > 0) return 1;
    return 0;
}

int main()
{
  int i = 0;
  int j = 10;
  int k = 0;
  int z = 0;
  while (i < j) {
    k = greaterThanZero(j);
    char * annotation = "@assert␣k␣==␣1";
    z = k + 9;
    if (k != 1) {
      printf("this␣should␣not␣be␣printed");
    }
    else {
      printf("k=%d",k);
    }
    i ++;
  }
  i += z;
  return i;
}
```

In Listing 4.18 we give an example of a simple annotated program. The Frama-C plugin described in Section 4.2 is able to produce the annotation *"@assert k == 1"*. In Listing 4.19 we can see that the normal costant propagation pass LLVM is not able to propagate any value. Instead, as we can see in Listing 4.20, our modified version is able to propagate the value of *k* (named %call in the IR) thus enabling both the propagation of *z* (named %add in the IR) and the propagation of the *if* condition (which is translated in a comprare instruction, named %cmp1 in the IR) which is always *false*. This will trigger the removal of the branch in a later Simplify CFG pass.

Listing 4.19: Normal Constant Propagation Example

```
...
while.cond:                                       ; preds = %if.end, %entry
  %i.0 = phi i32 [ 0, %entry ], [ %inc, %if.end ]
  %z.0 = phi i32 [ 0, %entry ], [ %add, %if.end ]
  %cmp = icmp slt i32 %i.0, 10
  br i1 %cmp, label %while.body, label %while.end
while.body:                                       ; preds = %while.cond
  %call = call i32 @greaterThanZero(i32 10)
  %add = add nsw i32 %call, 9
  %cmp1 = icmp ne i32 %call, 1
  br i1 %cmp1, label %if.then, label %if.else

if.then:                                          ; preds = %while.body
  %call2 = call i32 (i8*, ...)* @printf(i8* getelementptr inbounds ([27 x i8]* @.
      str1, i32 0, i32 0))
  br label %if.end

if.else:                                          ; preds = %while.body
  %call3 = call i32 (i8*, ...)* @printf(i8* getelementptr inbounds ([5 x i8]* @.str2
      , i32 0, i32 0), i32 %call)
  br label %if.end
...
```

Listing 4.20: Modified Constant Propagation Example

```
...
while.cond:                                       ; preds = %if.end, %entry
  %i.0 = phi i32 [ 0, %entry ], [ %inc, %if.end ]
  %z.0 = phi i32 [ 0, %entry ], [ 10, %if.end ]
  %cmp = icmp slt i32 %i.0, 10, !dbg !27
  br i1 %cmp, label %while.body, label %while.end, !dbg !27

while.body:                                       ; preds = %while.cond
  br i1 false, label %if.then, label %if.else, !dbg !37

if.then:                                          ; preds = %while.body
  %call2 = call i32 (i8*, ...)* @printf(i8* getelementptr inbounds ([27 x i8]* @.
      str1, i32 0, i32 0)), !dbg !38
  br label %if.end, !dbg !40

if.else:                                          ; preds = %while.body
  %call3 = call i32 (i8*, ...)* @printf(i8* getelementptr inbounds ([5 x i8]* @.str2
      , i32 0, i32 0), i32 1), !dbg !41
  br label %if.end

if.end:                                           ; preds = %if.else, %if.then
  %inc = add nsw i32 %i.0, 1, !dbg !43
  br label %while.cond, !dbg !44
...
```

4.6.2 Improving Lazy Value Information Analysis Pass

The *Lazy Value Information* Analysis Pass is an interface for lazy computation of value constraint information. It is lazy so it will perform the analysis only when a dependent Pass will ask for some information about a value. The analysis is performed on a lattice structure where every *LVILatticeVal* type is showed in Listing 4.21.

Listing 4.21: Lattice Information Type

```
1     enum LatticeValueTy {
2         /// undefined - This Value has no known value yet.
3         undefined
4         /// constant - This Value has a specific constant value.
5         constant,
6         /// notconstant - This Value is known to not have the specified value.
7         notconstant,
8         /// constantrange - The Value falls within this range.
9         constantrange,
10        /// overdefined - This value is not known to be constant, and we know that it
              has a value.
11        overdefined
12    };
```

This lazy analysis is done by using a cache (*LazyValueInfoCache* Class) on which the value informations are solved when needed. We store the informations about constant and constantrange lattice values coming from the annotations in the cache together with the basic block in which they holds.

When the Pass will be asked the information about a value, the *solveBlockValue(Value *, BasicBlock *)* method that gets called is modified to search if there is an annotation about that value and uses it to improve the analysis.

The modified pass uses annotations of the kind shown in Listing 4.22.

Listing 4.22: Value Info Annotation Supported

```
@assert value == const
@assert value >= const1 && val <= const2
@assert value == const1 || ... || val == constN
```

The choice to improve this kind of analysis is motivated by the most frequent pass run during the BIND compilation with LLVM. As we can see in Listing 4.23 the Jump Threading and the Correlated Value Propagation are among the most recurrent passes used and they both depend on the Lazy Value Information Analysis.

Listing 4.23: Most Frequent Passes during BIND compilation

```
31975 ***  Simplify the CFG ***
31975 ***  Combine redundant instructions ***
16728 ***  Remove unused exception handling info ***
16728 ***  Promote by reference arguments to scalars ***
16728 ***  Function Integration/Inlining ***
16728 ***  Deduce function attributes ***
14400 ***  Canonicalize natural loops ***
12843 ***  Loop-Closed SSA Form Pass ***
12790 ***  'Correlated Value Propagation' ***
12790 ***  SROA ***
12790 ***  'Jump Threading' ***
12790 ***  Early CSE ***
8258 ***  Tail Duplication ***
...
```

4.6.3 Cascading Effects in other Transformation Passes

The advantage of modifying Analysis Passes is that then every Transformation Pass that depends on it can take advantage of the analysis improvements in order to perform better optimizations. Here we give an overview of the two Transformation Passes that depends on the *Lazy Value Information* Analysis Pass:

- The first one is the *Correlated Value Propagation* Transformation Pass. This pass handles the propagation of ϕs, selects, memory access targets, it simplifies compare

instructions and switch cases that never fires. It uses the results from the *Lazy Value Information* Pass in order to test constant values.

In Listing 4.24 we show an simple example where correlated value propagation while analyzing the operands of a Phi node is able to propagate constant values inside these operands by means of the modified Lazy Value Info analysis. The normal one will simply left the IR code as it is in Listing 4.25. As we can see in Listing 4.26 the values are propagated inside *y.addr.0*.

Listing 4.24: Correlated Value Propagation Example

```
...
char * annotation1 = "@assert␣x␣==␣10";
if( x > y ){
        y = x;
        char * annotation2 = "@assert␣y␣==␣10";
} else {
        y = x+x;
        char * annotation3 = "@assert␣y␣==␣20";
}
z = y + x;
...
```

Listing 4.25: Correlated Value Propagation Example IR

```
...
%cmp = icmp sgt i32 %x, %y, !dbg !28
br i1 %cmp, label %if.then, label %if.else, !dbg !28

if.then:                                          ; preds = %entry
  br label %if.end, !dbg !35

if.else:                                          ; preds = %entry
  %add = add nsw i32 %x, %x, !dbg !36
  br label %if.end

if.end:                                           ; preds = %if.else, %if.then
  %y.addr.0 = phi i32 [ %x, %if.then ], [ %add, %if.else ]
  %add1 = add nsw i32 %y.addr.0, %x, !dbg !42
...
```

Listing 4.26: Modified Correlated Value Propagation Example

```
...
%cmp = icmp sgt i32 %x, %y, !dbg !27
  br i1 %cmp, label %if.then, label %if.else, !dbg !27

if.then:                                          ; preds = %entry
  br label %if.end, !dbg !34

if.else:                                          ; preds = %entry
  %add = add nsw i32 %x, %x, !dbg !35
  br label %if.end

if.end:                                           ; preds = %if.else, %if.then
  %y.addr.0 = phi i32 [ 10, %if.then ], [ 20, %if.else ]
  %add1 = add nsw i32 %y.addr.0, %x, !dbg !40
```

- The second one is the *Jump Threading* Transformation Pass. This Pass analyzes blocks that have multiple predecessors and multiple successors. If one or more of the predecessors of the block can be proven to always jump to one of the successors, it forwards the edge from the predecessor to the successor by duplicating the contents of the block. A trivial example is showed in Listing 4.27. Here the unconditional branch at the end of the first if can be forwarded to the else side of the second if.

Listing 4.27: Jump Threading Example

```
...
if (...) {
        ...
        x = 0;
        ...
}
if (x > 0) {
        ...
} else {
        ...
}
...
```

In addition if a block terminator (the last block instruction) is branching on a constant, it can simplify the terminator to an unconditional branch (this can occur due to threading in other blocks). This Pass uses the analysis to see if it can simplify

branches and if there are value that are known by the *Lazy Value Information* Pass to be a constant in a predecessor, it uses that information to try to thread the current block.

In Listing 4.28 we show a trivial C program example in which simple annotations can help the compiler during the Jump Threading optimization.

Listing 4.28: Detailed Jump Threading Example

```
1   int foo(int x){
2           if(x < 10){
3                   if(x > 8) {
4                           char * annotation1 ="@assert␣x==9";
5                           x++;
6                           char * annotation2 ="@assert␣x==10";
7                   }
8           }
9           if(x == 10){
10                  return 0;
11          }
12          return 1;
13  }
```

Figure 6 shows how the code is translated by the compiler in the IR after the memory to register promotion. Since the memory to register promotion pass does not modify the resulting CFG, the source code program structure is still preserved and easy to understand from the graph showed below.

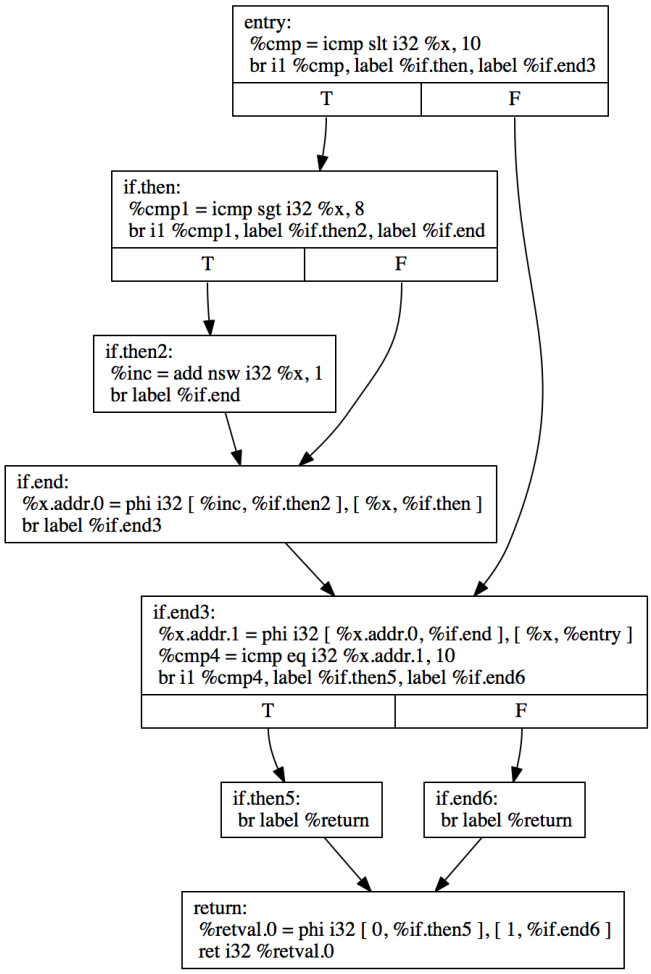

Figure 6: CFG Before Jump Threading

Figure 7 shows how the normal Jump Threading pass is able to thread a jump. It optimize the resulting code by removing two blocks (namely *if:end* and trivially *if:then5*) and making *if.then* block jump to *inf:end6* if the branch condition is false.

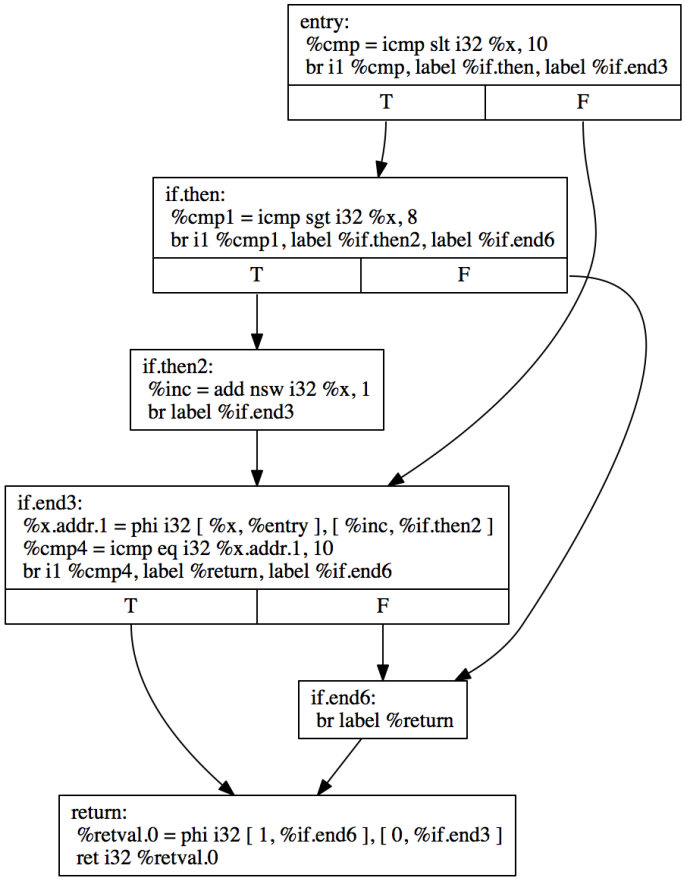

Figure 7: CFG After Jump Threading

Figure 8 shows how our modified Jump Threading Pass is able to thread an additional jump resulting in more optimized code compared to the normal one. As we can see in the picture below, the block *if.then2* gets removed and the jump from *if.then* is threaded to the *return* block.

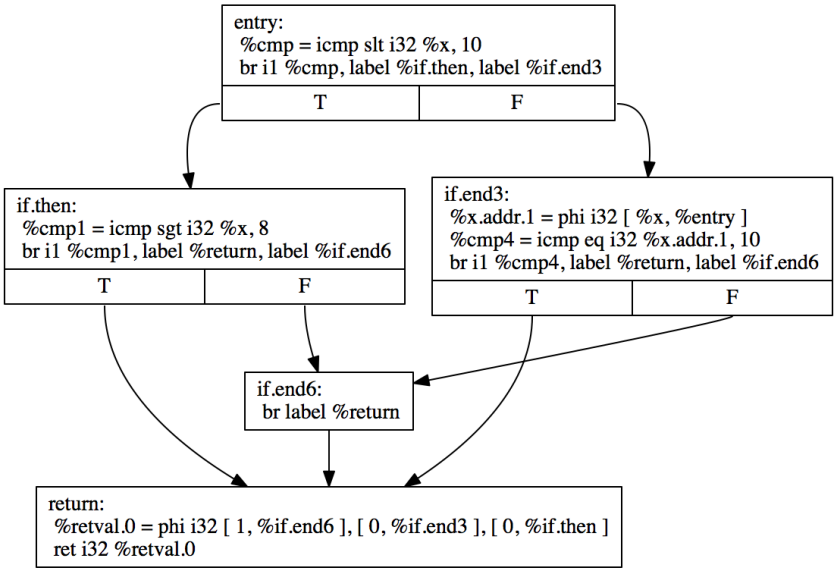

Figure 8: CFG After Modified Jump Threading

CHAPTER 5

EVALUATION

To evaluate this work we tested our changes in the LLVM and Safecode architecture. Here it follows a comparison between the new results and the ones without the modifications. We both compared the statistics during the compilation and the runtime benefits in terms of code and time reduction. In addition for every optimization we show the results both when they are run immediately after memory to register promotion and in the proposed pipeline.

5.1 Safecode Checks Reduction Results

Table I shows the number of checks the normal Safecode is injecting in the code compared to the number of checks our modified version is inserting. As we can see we are able to a pretty high percentage of the checks in almost all the benchmarks without loosing security margin.

TABLE I: SAFECODE CHECKS REDUCTION RESULT

Safecode Checks Reduction Results				
Benchmark	LOC	Safecode Version	# Run-time Checks	% Run-time Checks Removed
CoreMark	1831	Normal	309	
		Modified	241	22.0065%
Susan	1463	Normal	2251	
		Modified	2008	10.7952%
MxM	373	Normal	123	
		Modified	102	17.0731%
Linpack	579	Normal	318	
		Modified	286	10.0630%
NECMatrix	113	Normal	78	
		Modified	32	58.9744%

Table II show the impact of the check reduction in terms of code size. As expected our modified version is always generating smaller program since we are just avoiding the injection of additional checks.

TABLE II: SAFECODE EXECUTABLE SIZE REDUCTION RESULT

Safecode Executable Size Reduction Results			
Benchmark	Safecode Version	Code Size (bytes)	% Code Size Reduction
CoreMark	Normal	1319475	
	Modified	1315271	0.3186%
Susan	Normal	1375254	
	Modified	1366824	0.6130%
MxM	Normal	977852	
	Modified	969324	0.8721%
Linpack	Normal	1100586	
	Modified	1096384	0.3818%
NECMatrix	Normal	792426	
	Modified	788276	0.5237%

Table III shows the results in terms of execution time of the generated executable. The execution time depends mostly on the actual number of checks removed inside loops.

TABLE III: SAFECODE RUN-TIME REDUCTION RESULT

Safecode Run-time Reduction Results	
Benchmark	% Speed-Up
CoreMark	0.3163%
Susan	3.4483%
MxM	12.0531%
Linpack	95.9401%
NECMatrix	46.6666%

The poor results in the Coremark benchmarks is due to the fact that we do not have annotations for the relevant portion of code, which is the one that is executed most often.

The annotations that we have are about array accesses during initialization, which are executed only once.

Instead in the NEC-matrix benchmark, functions called only once from the main functions. At most double nested loops. No comand line arguments required, therefore Frama-C finds correct information about all the index bounds. On the LLVM end, the size of the arrays is easy to determine since they are all created as global arrays of a fixed known size

As NEC-matrix benchmark, Linpack Benchmark requires no command line arguments or user input, Frama-C gives useful information here if run with option -slevel 1000. The higher the slevel the more states Frama-C keeps in memory as it is going through the loops. In particular, the most useful information is that in a function (named *daxpy*) which is executed approx. 86% of the time according to the valgrind profiler. On the llvm end, many functions receive the name of the arrays as pointer input parameters, therefore there is no easy way to get the size of the arrays during the optimization pass. We enumerated the call sites where the function is called and tried to see if the array being passed in input to it is allocated via a malloc or in the stack inside the caller function. In addition, in the source code, parameter values are computed inside the function call, e.g., *foo(a +j*x)*, where a contains the starting address of the array. So, if we have annotations about j and x, we can compute the exact value of the input parameter.

Both Susan and MxM are run with command line arguments, Frama-C value analysis needs to be given information about the values of those arguments. If this is done, then the annotations produced are somewhat good.

5.2 Optimizations Improvements Results

In this section we describe the results of our modified optimizations compared to normal one in LLVM. First we are going to show how every single optimization pass behaves on the input benchmarks, then we show the results of all the passes chained together in a pipeline and we present some additional informations about the code size and execution time of the output executables.

5.2.1 Single Optimization Results

Table IV shows that the additional informations have an impact in the propagation of constant values. These is due to the fact Frama-C Value Analysis is able to identify much more constant values that the normal Constant Propagation pass. Almost in every benchmark the constant information inside the annotation holds only in some blocks of the code (such as when the annotation is inside an if statement branch) therefore the information cannot be substituted in all the uses as in the normal constant propagation. That is why the most of the constant values in the annotations are not killed. However the propagation of these values is able to have cascading effects in the propagation of other values in which these substitutions were done. In the NECMatrix benchmark Frama-C was not able to insert any information about constant values hence the modified optimization was not able to improve the results.

TABLE IV: CONSTANT PROPAGATION RESULTS

Constant Propagation Results				
Benchmark	Version	#Annot. Substituted	#Instr. Killed by Annot.	# Instr. Killed
CoreMark	Normal			3
	Modified	18	0	73
Susan	Normal			1
	Modified	4	1	15
Linpack	Normal			0
	Modified	6	0	10
NECMatrix	Normal			0
	Modified	0	0	0

Table V shows how both in Susan and Linkpack benchmarks the additional informations in the annotated code are able to trigger the propagation of phi or comparison instructions. These results are poor, however they still confirm that these informations can be effective in some cases.

TABLE V: CORRELATED VALUE PROPAGATION RESULTS

Correlated Value Propagation Results					
Benchmark	Version	# Phi Prop.	# Select Prop.	# Cases Rem.	# Cmp Simpl.
CoreMark	Normal	5	0	0	0
	Modified	5	0	0	0
Susan	Normal	0	0	0	1
	Modified	1	0	0	1
Linpack	Normal	0	0	0	0
	Modified	2	0	0	0
NECMatrix	Normal	0	0	0	0
	Modified	0	0	0	0

Table VI shows that the annotations were not able to have an effect on trading jumps in any of the benchmarks. The modified version is still conservative and does not perform worse than the modified one. Hence, at least there is nothing to loose in trying to use the informations in the annotations.

TABLE VI: JUMP THREADING RESULTS

Jump Threading Results			
Benchmark	Version	# Jumps Threaded	# Terminators Folded
CoreMark	Normal	12	1
	Modified	12	1
Susan	Normal	12	1
	Modified	12	1
Linpack	Normal	0	0
	Modified	0	0
NECMatrix	Normal	0	0
	Modified	0	0

5.2.2 Optimization Pipeline Results

Since the Constant Propagation pass is the first in our pipeline of passes the results its result in the pipeline are the same as the one reported in Table IV. However, the results in Table VII shows that the instructions propagated in Susan and Linpack benchmarks in the

previous Table V are already propagated during the constant propagation pass leaving the Correlated Value transformation unchanged.

TABLE VII: PIPELINE CORRELATED VALUE PROPAGATION RESULTS

Pipeline Correlated Value Propagation Results					
Benchmark	Version	# Phi Prop.	# Select Prop.	# Cases Rem.	# Cmp Simpl.
CoreMark	Normal	5	0	0	0
	Modified	5	0	0	0
Susan	Normal	0	0	0	0
	Modified	0	0	0	0
Linpack	Normal	0	0	0	0
	Modified	0	0	0	0
NECMatrix	Normal	0	0	0	0
	Modified	0	0	0	0

The results coming from the modified version of the jump threading are not better than the normal one as seen before in Table VI. In addition from these benchmarks the constant propagation in the first pipeline step seems not to enable better jump threading. The results in Table VIII shows that the results coming from the constant propagation pass have

just a little impact in code size. The additional propagation of values and the instruction killed reduces the code size of the benchmarks. The last line of the table is left blank since we have no improvements on the NECMatrix benchmark. The Susan benchmark seems not to have any improvement, however the resulting IR is different and even if after the translation in machine code they have the same size the executable differ.

TABLE VIII: EXECUTABLE SIZE PIPELINE REDUCTION RESULTS

Executable Size Pipeline Reduction Results			
Benchmark	Version	Code Size (bytes)	% Code Size Reduction
CoreMark	Normal	21,844	
	Modified	21,733	0.0505%
Susan	Normal	37,313	
	Modified	37,313	0.0000%
Linpack	Normal	16,209	
	Modified	16,214	0.0310%
NECMatrix	Normal	//	
	Modified	//	0.0000%

The performance results about Susan and Linpack benchmarks were taken over a 1000 iterations of the executables. Since the Unix *time* command seemed to be not reliable we slightly modified the benchmark logging the execution time at the beginning and the end of the main function and then averaging the result. To measure CoreMark List and CoreMark Matrix execution time we rely on the built-in Makefile that additionally logs the performance of the executables.The last line of the table is left blank since we have no improvements on the NECMatrix benchmark. However since the performance improvement is almost negligible in the benchmarks and the percentage of measurement error is higher than the performance speed-up we do not show the result table.

The effectiveness of the modified optimizations is correlated to the information on the SCannotations. We inspected the resulting IR code and we have seen that the modified optimization are too few to make a real difference and that after all the other LLVM optimizations the resulting code is almost the same. In particular Function Inlining combined with Interprocedural Sparse Conditional Constant Propagation is already able to eneable the same optimization that the most of the additional constant informations inserted by the Frama-C Value Analysis plug-in enables.

CHAPTER 6

CONCLUSIONS

In this thesis we described the concept of program annotation, the different sources of annotated code and how nowadays compilers are ignoring these additional informations. We described the approach we followed to build our framework, which allows the compiler to take advantage of the annotations to improve different aspects of the compilation process. Namely, our framework is able to reduce both the trade-off between security and execution time of a compiled program and to improve current compiler optimizations. In this work we inspected different ways to use additional value informations so that the compilation can be more effective. We presented in detail how our approach can be useful in a state of the art compiler such as LLVM and how the framework was built in order to be highly reusable with different kind of program annotation sources. We evaluated the effectiveness of the approach on real world benchmarks using some information coming from the Frama-C Value Analysis plug-in. We showed how our framework is able to have a slight impact both on the executable code size and execution time by removing the SafeCode checks. However, we still need to improve different aspects on the modified optimizations side so that the additional compilation time overhead motivates the use of the framework.

CHAPTER 7

FUTURE WORK

Currently the implementation of the modified optimization passes depends on the order of their execution. This order is a constraint and it is due to the fact that the we have to guarantee that the informations in the annotations still hold after the transformation passes changes. The order may influence also later optimizations and it is not always guaranteed that the previous optimizations wil not disable better later optimizations. Therefore one of the major drawbacks of our current approach is that we need a way to propagate the changes in annotations to remove this constraint.

In *Witnessing Program Transformations*[21] it is described how we can use witnesses both to validate the pass transformation and to correctly propagate invariants inside the code (for example our annotations). By implementing a transformation witness inside of the modified passes it will be possible to propagate the changes inside the annotations and to guarantee the correctness of their informations. This will enable a broader range of passes that could be modified in order to take advantage of the informations inside the annotations without worrying about the correctness of the changes in the annotations. These changes are automatically certified by the theorem prover by checking the witness, the input and the output program.

In addition to the new optimizations that can take into account the *Value Analysis* information it could be interesting to use other kind of analysis that can be helpful for different

optimizations. Our framework design makes it easy to exploit different kind of analysis since it relies on a standard annotation language (and the a pass that map this information to the IR values) that act as an interface between the back-end and the different kind of analysis before the front-end.

Eventually merging the achievements from run-time checks removal, witness generation and optimization improvements we will be able to build a compiler able to both perform aggressive optimizations and defend code against security flaws.

APPENDICES

Appendix A

ACSL SUPPORTED GRAMMAR

⟨*annotation*⟩ → ⟨*stmts*⟩ END

⟨*stmts*⟩ → ⟨*stmt*⟩

| ⟨*stmts*⟩ ⟨*stmt*⟩

⟨*stmt*⟩ → TASSERT ⟨*expr*⟩

| TREQUIRES ⟨*expr*⟩

| TENSURES ⟨*expr*⟩

⟨*expr*⟩ → ⟨*ident*⟩

| ⟨*numeric*⟩

| TLPAREN ⟨*expr*⟩ TRPAREN

| ⟨*expr*⟩ TCEQ ⟨*expr*⟩

| ⟨*expr*⟩ TCNE ⟨*expr*⟩

| ⟨*expr*⟩ TCLT ⟨*expr*⟩

| ⟨*expr*⟩ TCGT ⟨*expr*⟩

| ⟨*expr*⟩ TCLE ⟨*expr*⟩

| ⟨*expr*⟩ TCGE ⟨*expr*⟩

| ⟨*expr*⟩ TCANDAND ⟨*expr*⟩

| ⟨*expr*⟩ TCOROR ⟨*expr*⟩

Appendix A (Continued)

⟨*ident*⟩ → TIDENTIFIER

⟨*numeric*⟩ → TINTEGER

| TDOUBLE

| TMINUS TINTEGER

| TMINUS TDOUBLE

Appendix B

INTERVAL ALGEBRAIC STRUCTURE

In this chapter we describe the algebraic structure used to model the range computation for SSA variables. The underlying set, the contiguous interval of the possible value for an integer variable, is the set of integers (positive and negative) pairs *NXN*.

In Listing B.1 follow a series of range and constant information about integer variables modeled as intervals:

Listing B.1: Interval Examples

```
1     i<=0 && i<=1000          -> i in [0,1000]
2     j==-50                   -> j in [-50,-50]
3     k==0 || k==1 || k==2     -> k in [0,2]
```

On this carrier set we define the internal sum and multiplication operations as follow:

- *Interval Sum* (+):

  $\forall x, y, w, z \in N, [x, y] + [w, z] = [x + w, y + z]$

- *Interval Multiplication* (*):

  $\forall x, y, w, z \in N, [x, y] + [w, z] = [i, j]$

  where $i = min(x * w, x * z, y * w, y * z)$ and $j = max(x * w, x * z, y * w, y * z)$

Listing B.2 shows how these operations are useful to propagate range information during SSA assignments in a basic block.

Appendix B (Continued)

Listing B.2: Interval Operation Examples

```
suppose holds:

        %i<=0 && %i<=10         -> %i in [0,10]
        %j==-5                  -> %j in [-5,-5]
        %k<=-2 && %k<=3         -> %k in [-2,3]

basicblock instructions:

        %add1 = add %i %j       -> %add1 in [0,10]+[-5,-5] = [-5,5]
        %mul1 = mul %k %i       -> %mul1 in [-2,3]*[0,10] = [-20,30]
        %mul2 = add 3 5         -> %mul2 in [3,3]*[5,5] = [15,15]
        %sub1 = sub %add1 %mul2 -> %sub1 in [-5,5]+([-1,-1]*[15,15]) = [-20,-10]
```

CITED LITERATURE

1. Meyer, B.: Eiffel: the language. Prentice-Hall, Inc., 1992.
2. Schenk, E. and Guittard, C.: Crowdsourcing: What can be outsourced to the crowd, and why? In Workshop on Open Source Innovation, Strasbourg, France, 2009.
3. Crowd Source Formal Verification (CSFV). http://www.darpa.mil/Our_Work/I2O/Programs/Crowd_Sourced_Formal_Verification_(CSFV).aspx. [Online; accessed 3-November-2013].
4. ANSI/ISO C Specification Language. http://frama-c.com/acsl.html. [Online; accessed 20-November-2013].
5. Burdy, L., Cheon, Y., Cok, D. R., Ernst, M. D., Kiniry, J. R., Leavens, G. T., Leino, K. R. M., and Poll, E.: An overview of jml tools and applications. International Journal on Software Tools for Technology Transfer, 7(3):212–232, 2005.
6. Cytron, R., Ferrante, J., Rosen, B. K., Wegman, M. N., and Zadeck, F. K.: Efficiently computing static single assignment form and the control dependence graph. ACM Transactions on Programming Languages and Systems, 13(4):451–490, Oct 1991.
7. Muchnick, S.: Advanced compiler design and implementation. 1997.
8. Lattner, C. and Adve, V.: Llvm: A compilation framework for lifelong program analysis & transformation. In Code Generation and Optimization, 2004. CGO 2004. International Symposium on, pages 75–86. IEEE, 2004.
9. The LLVM Compiler Infrastructure. http://llvm.org. [Online; accessed 5-November-2013].
10. clang: a C language family frontend for LLVM. http://clang.llvm.org/. [Online; accessed 20-November-2013].
11. LLVM Language Reference Manual. http://llvm.org/docs/LangRef.html. [Online; accessed 5-November-2013].
12. Lattner, C.: LLVM: An Infrastructure for Multi-Stage Optimization. Master's thesis, Computer Science Dept., University of Illinois at Urbana-Champaign, Urbana, IL, Dec 2002.
13. LLVM Analysis and Transform Passes. http://llvm.org/docs/Passes.html. [Online; accessed 6-November-2013].
14. SAFECode: Static Analysis For safe Execution of Code. http://safecode.cs.illinois.edu/index.html. [Online; accessed 5-November-2013].

15. Cuoq, P., Kirchner, F., Kosmatov, N., Prevosto, V., Signoles, J., and Yakobowski, B.: Frama-c. In Software Engineering and Formal Methods, pages 233–247. Springer, 2012.

16. Canet, G., Cuoq, P., and Monate, B.: A value analysis for c programs. In Source Code Analysis and Manipulation, 2009. SCAM'09. Ninth IEEE International Working Conference on, pages 123–124. IEEE, 2009.

17. Top 25 Most Dangerous Software Errors. `http://cwe.mitre.org/top25/`. [Online; accessed 11-November-2013].

18. GCC Wiki. `http://gcc.gnu.org/wiki`. [Online; accessed 5-November-2013].

19. Necula, G. C., McPeak, S., Rahul, S. P., and Weimer, W.: Cil: Intermediate language and tools for analysis and transformation of c programs. In Compiler Construction, pages 213–228. Springer, 2002.

20. Source Level Debugging with LLVM. `http://llvm.org/docs/SourceLevelDebugging.html`. [Online; accessed 5-November-2013].

21. Namjoshi, K. and Zuck, L.: Witnessing program transformations. In Static Analysis, eds. F. Logozzo and M. Fahndrich, volume 7935 of Lecture Notes in Computer Science, pages 304–323. Springer Berlin Heidelberg, 2013.

VITA

Niko Zarzani

Education

B.S., Engineering of Computing Systems
Politecnico di Milano, Milano, Italy
2011

M.S., Computer Science
University of Illinois at Chicago, Chicago, IL
2014

M.S., Engineering of Computing Systems
Politecnico di Milano, Milano, Italy
2014

Working experience

Software Engineering Laboratory Tutor at Politecnico di Milano
Spring 2012

Research Assistant at University of Illinois at Chicago
Fall 2012, Spring 2013, Fall 2013