

Compiler Optimization Notes

December 4, 2022

Contents

1 Local Optimizations	2
1.1 Basic Blocks/Flow graphs	2
1.1.1 Basic Blocks	2
1.1.2 Flow graphs	2
1.1.3 Partitioning into Basic Blocks	2
1.1.4 Reachability of Basic Blocks	3
1.2 Local optimizations	4
1.2.1 common subexpression elimination	4
1.3 Abstraction 1:DAG	4
1.3.1 How well do DAGs hold up across statements?	5
1.4 Abstraction 2:Value numbering	5
1.4.1 Algorithm	6
1.4.2 Example	7
2 Introduction to Data Flow Analysis	8
2.1 Motivation for Dataflow Analysis	8
2.1.1 What is Data Flow Analysis?	8
2.1.2 Static Program vs. Dynamic Execution	9
2.1.3 Data Flow Analysis Schema	9
3 Live Variable Analysis	11
3.1 Motivation	11
3.2 Problem formulation	11
3.3 Semantic vs. syntactic	11
4 Reaching Definitions	13
4.1 Iterative Algorithm	13
4.2 Worklist Algorithm	13
4.3 Example	13

5 Available Expressions Analysis	14
5.1 Motivation	14
5.2 Backgroud Knowledge	14
5.3 Problem Formulation	14
5.4 Semantic vs. Syntactic	15
6 Foundations of Data Flow Analysis	17
6.1 A Unified Framework	17
6.2 Partial Order	17
6.3 Lattice	17
6.4 Complete Lattice	18
6.5 Semi-Lattice	18
6.6 Meet Operator	18
6.7 Descending Chain	19
6.8 Transfer Functions	19
6.9 Monotonicity	20
6.10 Distributivity	20
7 Introduction to Static Single Assignment	21
7.1 Definition-Use and Use-Definition Chains	21
7.2 Static Single Assignment(SSA)	22
7.2.1 Why SSA is useful?	22
7.3 How to represent SSA?	22
7.3.1 How does the ϕ -function know which edge was taken?	23
7.4 Converting to SSA form	23
7.4.1 Trivial SSA	23
7.4.2 Minimal SSA	24
7.4.3 Path-convergence criterion	25
7.4.4 Dominance property of SSA form	25
7.5 Computing the dominance frontier	28
7.6 Inserting Φ -functions	29
7.7 Renaming the variables	30
7.7.1 Example	30
7.8 Edge Splitting	35
8 SSA-Style optimizations	37
8.1 Constant Propagation	37
8.2 Conditional Constant Propagation	37
8.2.1 Example	38
8.3 Copy Propogation	40
8.4 Aggressive Dead Code Elimination	40
8.4.1 Problems within algorithm 9	41
8.4.2 Control Dependence	42
8.4.3 Aggressive Dead Code Elimination(Fixed Version)	42
8.4.4 Finding the Control Dependence Graph	43
9 The LLVM project	45

10 Loop Invariant Computation and Code Motion	46
10.1 Finding natural loops	46
10.2 Algorithm to Find Natural Loops	47
10.2.1 Step 1. Finding Dominators	47
10.2.2 Step 2. Finding Back Edges	48
10.2.3 Step 3. Constructing Natural Loops	49
10.3 Inner Loops	50
10.4 Loop-Invariant Computation and Code Motion	50
10.5 LICM Algorithm	50
10.6 Find invariant expressions	51
10.7 Conditions for Code Motion	52
10.8 More Aggressive Optimizations	53
10.8.1 Gamble on: most loops get executed	53
10.8.2 Landing pads	53
11 Induction Variables and Strength Reduction	55
11.1 Motivation	55
11.2 Definitions	57
11.3 Optimizations	57
11.3.1 Strength Reduction	57
11.3.2 Optimizing non-basic induction variables	57
11.3.3 Optimizing basic induction variables	57
11.4 Further Details	58
11.5 Finding Induction Variable Families	59
12 Partial Redundancy Elimination	60
12.1 Finding Partially Available Expressions	60
12.2 Finding Anticipated Expression	62
12.3 Where Do we Want to Insert Computations?	65
12.3.1 Safety	67
12.4 Perform	67
12.5 Limitations	67
12.6 A new way to think about partial redundancy	67
13 Lazy Code Motion	68
13.1 Big Picture	68
13.2 PRE vs. LCM	69
13.3 Preprocessing: Preparing the Flow Graph	70
13.4 Pass 1: Anticipated Expression	71
13.5 Where to insert/move instructions?	71
13.5.1 Choice 1 : frontier of anticipation	71
13.6 Pass 2: Place As Early As Possible	73
13.7 Pass 3: Lazy Code Motion	73
13.8 Pass 4: Cleaning Up	75

14 A Variation of Knoop, Ruthing, and Steffen’s Lazy Code Motion	76
14.1 Where to Insert?	76
14.1.1 Earliest Placement	77
14.1.2 Latest Placement	78
14.1.3 Where to Insert Computations?	79
14.2 Modify CFG	80
14.3 Which Computations to Remove?	80
14.4 A fully explained example	81
15 Region-Based Analysis	86
15.1 Motivating Example	86
15.2 Algorithm	87
15.2.1 Operations on Transfer Functions	87
15.2.2 Structure of Nested Regions (An Example)	89
15.2.3 Transfer Functions for T2 Rule	89
15.2.4 Transfer Functions for T1 Rule	90
15.2.5 Example: Reaching Definitions	90
16 Pointer Analysis	93
16.1 Background	93
16.2 Flow-Sensitivity	94
16.3 Context-sensitive	94
16.4 Modeling Aggregates	95
16.5 Andersen’s Points-To Analysis	95
16.5.1 Field-Sensitive Analysis	97
16.6 Steensgaard’s Points-To Analysis	98
16.7 Adding Context Sensitivity to Andersen’s Algorithm	103
17 Profile Guided Optimizations	107
17.1 Efficient Path Profiling	107
17.2 Improved Basic Block Reordering	107
17.2.1 Contribution	108
17.2.2 New ideas	108
17.2.3 Algorithm	110

1 Local Optimizations

Local Optimizations never goes away because this is always a piece of what happens even when we talk about even more sophisticated types of optimizations.

First we will talk about how to represent the code within a function or procedure, that's using something called a flow graph which is made of basic blocks. Next we will contrast two different abstractions for doing local optimizations.

1.1 Basic Blocks/Flow graphs

1.1.1 Basic Blocks

A basic block is a sequence of instructions(3-address statements). There are some requirements for basic block:

- **Only the first instruction can be reached from outside the block.** The reason why this property is useful is that within a basic block, we just march instruction by instruction through the block, this simplifies things at least within a basic block.
- **All the statements are executed consecutively if the first one is.**
- **The basic block must be maximal.** i.e., they cannot be made larger without violating conditions.

1.1.2 Flow graphs

Flow graph is a graph representation of the procedure. In flow graph, basic blocks are the nodes, and the edge for $B_i \rightarrow B_j$ stands for a path from node B_i to node B_j . So how will $B_i \rightarrow B_j$ happen? There are two possibilities:

- Either first instruction of B_j is the target of a goto at end of B_i .
- B_j physically follows B_i which doesn't end in an unconditional goto.

1.1.3 Partitioning into Basic Blocks

- Identify the leader of each basic block
 - First instruction
 - Any target of a jump
 - Any instruction immediately following a jump
- Basic block starts at leader and ends at instruction immediately before a leader(or the last instruction).

An example of flow graph is shown below:

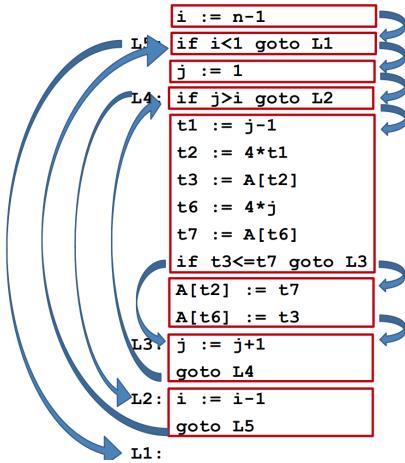


Figure 1: Example of a flow graph

1.1.4 Reachability of Basic Blocks

There is one thing interesting need to mention here. So the source code is below:

```

1 if x {
2     ...
3     return;
4 } else {
5     ...
}
```

Listing 1: An example

The corresponding flow graph is shown in 2:

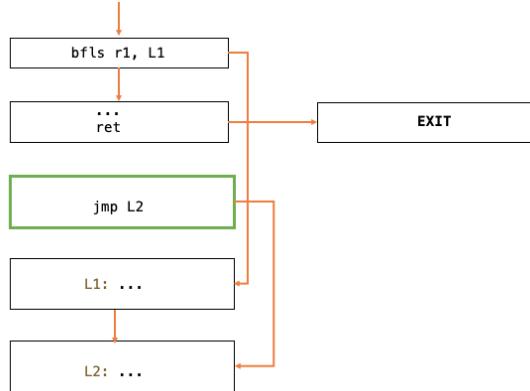


Figure 2: Example of a flow graph

We can see that the box in green is unreachable from the entry. So why is that interesting? Typically, after compilers construct the control flow graph, they will go through and remove any unreachable nodes. Just do depth first traversal of the graph from the entry node and mark all those visited nodes. So unmarked nodes will be deleted. This will help the compiler get a better optimization result.

So why do these unreachable nodes appear? The answer is it is not the job of the front-end of the compiler to clean up the unreachable nodes.

1.2 Local optimizations

Local optimizations are those occur **within the basic blocks**.

1.2.1 common subexpression elimination

There're some types of local optimizations. One is called **common subexpression elimination**. Subexpressions are some arithmetic expressions that occur on the right hand of the instructions. The goal of this common subexpression elimination is to identify expressions that are guaranteed to produce identical values at runtime and arrange to only perform the associated computation once (when the first instance of the expression is encountered).

```
a = b + c;
2 d = b + c;
```

Listing 2: Subexpression example

In the example 2, $b + c$ is so called coomon subexpression, we could replace the instruction containing common subexpression with an assign expression.

```
a = b + c;
2 d = a
```

Listing 3: code snippet applied common subexpression elimination to 2

You may wonder why this kind of redundancy can occure in code? Are we programmers stupid to do so? In fact, the redundancy most comes from the stage when compilers turn your source code. For example, **when you use arrays**, you need to do some arithmetic to generate the address of the array element you are accessing. So every time you referece the same array element, compiler will calculate the same address again. Similarly, if you **access offsets within fields**. Last example is **access to parameters** in the stack.

1.3 Abtraction 1:DAG

DAG is the acronym for Directed Acyclic Graph. The Directed Acyclic Graph (DAG) is used to represent the structure of basic blocks, to visualize the flow of values between basic blocks, and to provide optimization techniques in the basic block. DAG is an efficient method for identifying common sub-expressions.¹

The parse tree and DAG of the expression $a + a * (b + c) + (b + c) * d$ is shown in 3.

In DAG, some of the computation are reused. So we can generate optimizaed code based on DAG.

¹copied from <https://wildpartyofficial.com/what-is-dag-in-compiler-construction>

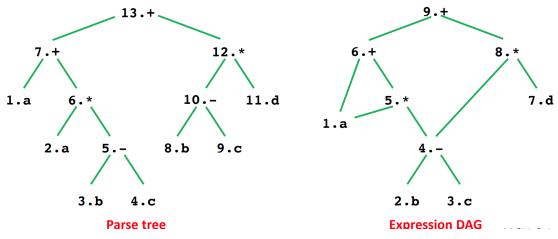


Figure 3: Example of a DAG

The optimized code for the DAG3 is:

```

2   t1 = b - c;
3   t2 = a * t1;
4   t3 = a + t2;
5   t4 = t1 * d;
6   t5 = t3 + t4;

```

Listing 4: code

1.3.1 How well do DAGs hold up across statements?

We have seen that DAGs can be useful in a long arithmetic expression. So how well do DAGs perform in sequence of instructions?

```

1   a = b + c;
2   b = a - d;
3   c = b + c;
4   d = a - d;

```

Listing 5: code

The corresponding DAG is shown in 4.

Based on the DAG4, one optimized code is 6

```

1   a = b+c;
2   d = a-d;
3   c = d+c;

```

Listing 6: code

6 is not correct. B need to be overwritten but not yet. So if using DAGs, you need to be very careful.

DAGs make sense if you just have one long expression, but once you have sequence of instructions overwriting variables , DAGs are less appealing because this abstraction doesn't really include the concept of time.

1.4 Abstraction 2:Value numbering

We have seen drawbacks of DAGs. One way to fix the problem is to attach variable name to latest value. Value numbering is such abstraction.

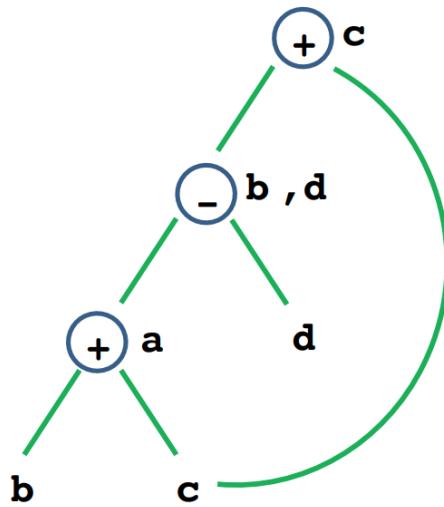


Figure 4: Example of a DAG

The idea behind value numbering is there is a mapping between variables(static) to values(dynamic). So common subexpression means same value number.

1.4.1 Algorithm

```

1 Data structure:
  VALUES = Table of
    expression /* [OP, valnum1, valnum2] */
    var /* name of variable currently holding expr */
5 For each instruction (dst = src1 OP src2) in execution order
  valnum1=var2value(src1); valnum2=var2value(src2)
7
  IF [OP, valnum1, valnum2] is in VALUES
    v = the index of expression
    Replace instruction with: dst = VALUES[v].var
11 ELSE
12   Add
13     expression = [OP, valnum1, valnum2]
14     var = tv
15   to VALUES
16   v = index of new entry; tv is new temporary for v
17   Replace instruction with: tv = VALUES[valnum1].var OP VALUES[valnum2].var
18   dst = tv
19   set_var2value (dst, v)

```

Listing 7: code

1. $w = a^1 * b^2$ 2. $x = w^3 + c^4$ 3. $d = a^1$ 4. $e = b^2$ 5. $y = d^1 * e^2$ 6. $z = y^3 + c^4$	$\langle *, 1, 2 \rangle = 3; VN(w) = 3$ $\langle +, 3, 4 \rangle = 5; VN(x) = 5$ $VN(d) = VN(a) = 1$ $VN(e) = VN(b) = 2$ $\langle *, 1, 2 \rangle$ redundant! $VN(y) = 3$ $\langle +, 3, 4 \rangle$ redundant! $VN(z) = 5$
--	--

Figure 5: An example of value numbering.

1.4.2 Example

Figure 5 shows a concrete example of how VN identifies computation redundancies within a basic block. The VN processes each instruction statically. It obtains the previously computed symbolic value of each operand on the RHS, assigning a unique number on encountering a new operand. Then, it hashes the symbolic values assigned to operands together with the operator to obtain a symbolic value for the computation. If the computed symbolic value for a computation is already present in the table of previously computed values, then the current computation is redundant. In this basic block, computations on Line 5 and 6 are redundant since the computations are already computed by instruction on Line 1 and 2.²

²copied from https://www.researchgate.net/publication/283214075_Runtime_Value_Numbering_A_Profiling_Technique_to_Pinpoint_Redundant_Computations

2 Introduction to Data Flow Analysis

2.1 Motivation for Dataflow Analysis

Some optimizations³, however, require more "global" information. For example, consider the code 8

```
1  a = 1;
2  b = 2;
3  c = 3;
4  if (...) x = a + 5;
5  else x = b + 4;
6  c = x + 1;
```

Listing 8: An

In this example, the initial assignment to c (at line 3) is useless, and the expression $x + 1$ can be simplified to 7, but it is less obvious how a compiler can discover these facts since they cannot be discovered by looking only at one or two consecutive statements. A more global analysis is needed so that the compiler knows at each point in the program:

- which variables are guaranteed to have constant values, and
- which variables will be used before being redefined.

To discover these kinds of properties, we use dataflow analysis.

2.1.1 What is Data Flow Analysis?

Local Optimizations only consider optimizations within a node in CFG. Data flow analysis will take edges into account, which means composing effects of basic blocks to derive information at basic block boundaries. Data-flow analysis is a technique for gathering information about the possible set of values calculated at various points in a computer program. A program's control-flow graph (CFG) is used to determine those parts of a program to which a particular value assigned to a variable might propagate. The information gathered is often used by compilers when optimizing a program.

Typically, we will do local optimization for the first step to know what happens in a basic block, step 2 is to do data flow analysis. In the third step, we will go back and revisit the individual instructions inside of the blocks.

Data flow analysis is **flow-sensitive**, which means we take into account the effect of control flow. It is also a **intraprocedural analysis** which means the analysis is within a procedure. Data-flow analysis computes its solutions over the paths in a control-flow graph. The well-known, meet-over-all-paths formulation produces safe, precise solutions for general dataflow problems. All paths-whether feasible or infeasible, heavily or rarely executed-contribute equally to a solution.

Here are some examples of intraprocedural optimizations:

- **constant propagation.** Constant propagation is a well-known global flow analysis problem. The goal of constant propagation is to discover values that are constant on all possible executions of a program and to propagate these constant values as far forward through the program

³based on <https://pages.cs.wisc.edu/~horwitz/CS704-NOTES/2.DATAFLOW.html>

as possible. Expressions whose operands are all constants can be evaluated at compile time and the results propagated further.

- **common subexpression elimination**

- **dead code elimination.** Actually, source code written by programmers doesn't contain a lot of dead code, dead code happens to occur partly because of how the front end translates code into the IR. Doing optimizations will also turn code into dead.

2.1.2 Static Program vs. Dynamic Execution

Program is statically finite, but there can be infinite many dynamic execution paths. On one hand, analysis need to be precise, so we will take into account as much dynamic execution as possible. On the other hand, analysis need to do the analysis quickly. For a compromise, the analysis result is **conservative** and what it does is for each point in the program, combines information of all the instances of the same program point.

2.1.3 Data Flow Analysis Schema

Before thinking about how to define a dataflow problem, note that there are two kinds of problems:

- Forward problems (like constant propagation) where the information at a node n summarizes what can happen on paths from "enter" to n. So if we care about what happened in the past, it's a forward problem.
- Backward problems (like live-variable analysis), where the information at a node n summarizes what can happen on paths from n to "exit". So if we care about what will happen in the future, it's a backward problem.

In what follows, we will assume that we're thinking about a forward problem unless otherwise specified.

Another way that many common dataflow problems can be categorized is as may problems or must problems. The solution to a "may" problem provides information about what may be true at each program point (e.g., for live-variables analysis, a variable is considered live after node n if its value may be used before being overwritten, while for constant propagation, the pair (x, v) holds before node n if x must have the value v at that point).

Now let's think about how to define a dataflow problem so that it's clear what the (best) solution should be. When we do dataflow analysis "by hand", we look at the CFG and think about:

- What information holds at the start of the program.
- When a node n has more than one incoming edge in the CFG, how to combine the incoming information (i.e., given the information that holds after each predecessor of n, how to combine that information to determine what holds before n).
- How the execution of each node changes the information.

This intuition leads to the following definition. An instance of a dataflow problem includes:

- a *CFG*,
- a domain D of "dataflow facts",
- a dataflow fact "init" (the information true at the start of the program for forward problems, or at the end of the program for backward problems),
- an operator \wedge (used to combine incoming information from multiple predecessors),
- for each CFG node n , a dataflow function $f_n : D \rightarrow D$ (that defines the effect of executing n).

For constant propagation, an individual dataflow fact is a set of pairs of the form (var, val), so the domain of dataflow facts is the set of all such sets of pairs (the power set). For live-variable analysis, it is the power set of the set of variables in the program.

For both constant propagation and live-variable analysis, the "init" fact is the empty set (no variable starts with a constant value, and no variables are live at the end of the program).

For constant propagation, the combining operation \wedge is set intersection. This is because if a node n has two predecessors, p_1 and p_2 , then variable x has value v before node n iff it has value v after both p_1 and p_2 . For live-variable analysis, \wedge is set union: if a node n has two successors, s_1 and s_2 , then the value of x after n may be used before being overwritten iff that holds either before s_1 or before s_2 . In general, for "may" dataflow problems, \wedge will be some union-like operator, while it will be an intersection-like operator for "must" problems.

For constant propagation, the dataflow function associated with a CFG node that does not assign to any variable (e.g., a predicate) is the identity function. For a node n that assigns to a variable x , there are two possibilities:

- 1. The right-hand side has a variable that is not constant. In this case, the function result is the same as its input except that if variable x was constant the before n , it is not constant after n .
- 2. All right-hand-side variables have constant values. In this case, the right-hand side of the assignment is evaluated producing constant-value c , and the dataflow-function result is the same as its input except that it includes the pair (x, c) for variable x (and excludes the pair for x , if any, that was in the input).

For live-variable analysis, the dataflow function for each node n has the form: $f_n(S) = Gen_n \cup (S - Kill_n)$, where $Kill_n$ is the set of variables defined at node n , and Gen_n is the set of variables used at node n . In other words, for a node that does not assign to any variable, the variables that are live before n are those that are live after n plus those that are used at n ; for a node that assigns to variable x , the variables that are live before n are those that are live after n except x , plus those that are used at n (including x if it is used at n as well as being defined there).

An equivalent way of formulating the dataflow functions for live-variable analysis is: $f_n(S) = (S \cap NOT - Kill_n) \cup Gen_n$, where $NOT - Kill_n$ is the set of variables not defined at node n . The advantage of this formulation is that it permits the dataflow facts to be represented using bit vectors, and the dataflow functions to be implemented using simple bit-vector operations (and or).

It turns out that a number of interesting dataflow problems have dataflow functions of this same form, where Gen_n and $Kill_n$ are sets whose definition depends only on n , and the combining operator \wedge is either union or intersection. These problems are called GEN/KILL problems, or bit-vector problems.

3 Live Variable Analysis

In compilers, live variable analysis (or simply liveness analysis) is a classic data-flow analysis to calculate the variables that are live at each point in the program. A variable is live at some point if it holds a value that may be needed in the future, or equivalently if its value may be read before the next time the variable is written to.⁴

3.1 Motivation

Programs may contain

- code which gets executed but which has no useful effect on the program's overall result;
- occurrences of variables being used before they are defined;
- many variables which need to be allocated registers and/or memory locations for compilation.

The concept of variable liveness is useful in dealing with all three of these situations.

3.2 Problem formulation

Liveness is a data-flow property of variables: "Is the value of this variable needed?" We therefore usually consider liveness from an instruction's perspective: each instruction (or node of the flowgraph) has an associated set of live variables.

3.3 Semantic vs. syntactic

⁵

There are two kinds of variable liveness : Semantic liveness and Syntactic liveness.

A variable x is **semantically** live at a node n if there is some execution sequence starting at n whose (externally observable) behaviour can be affected by changing the value of x . Semantic liveness is concerned with the execution behaviour of the program.

A variable is **syntactically** live at a node if there is a path to the exit of the flow graph along which its value may be used before it is redefined. Syntactic liveness is concerned with properties of the syntactic structure of the program.

So what is the difference between Semantic liveness and Syntactic liveness? syntactic liveness is a computable approximation of semantic liveness.

Consider the example

```
2   int t = x * y;
3   if ((x+1)*(x+1) == y) {
4       t = 1;
5   }
6   if (x*x + 2*x + 1 != y) {
7       t = 2;
8   }
9   return t;
```

Listing 9: An

⁴based on Wikipedia

⁵based on slides from Cambridge University

In fact, `t` is dead in node `int t = x;` because one of the conditions will be true, so on every execution path `t` is redefined before it is returned. The value assigned by the first instruction is never used.

But on read path from 6 through the flowgraph, `t` is not redefined before it's used, so `t` is syntactically live at the first instruction. Note that this path never actually occurs during execution.

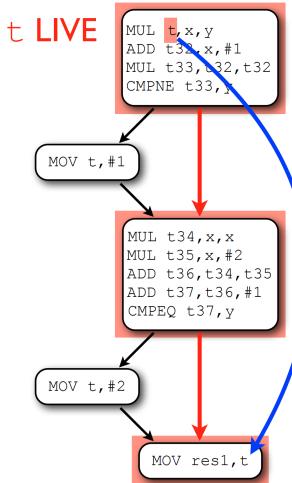


Figure 6: CFG

4 Reaching Definitions

The Reaching Definitions Problem is a data-flow problem used to answer the following questions: Which definitions of a variable X reach a given use of X in an expression? Is X used anywhere before it is defined? A definition d reaches a point p if there exists path from the point immediately following d to p such that d is not killed (overwritten) along that path.

4.1 Iterative Algorithm

Here is the iterative algorithm.

Algorithm 1 Reaching Definitions: Iterative Algorithm

Input: control flow graph $\text{CFG} = (\text{N}, \text{E}, \text{Entry}, \text{Exit})$

```

out[Entry] =  $\emptyset$                                      ▷ Boundary condition
for each basic block B other than Entry do
    out[B] =  $\emptyset$                                 ▷ Initialization for iterative algorithm
end for
while Changes to any out[] occur do
    for each basic block B other than Entry do
        in[B] =  $\cup(out[p])$ , for all predecessors p of B
        out[B] =  $f_B(in[B])$                          ▷  $out[B] = gen[B] \cup (in[B] - kill[B])$ 
    end for
end while

```

4.2 Worklist Algorithm

4.3 Example

Here comes an example of reaching definition.

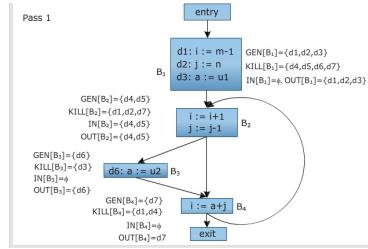


Figure 7: Pass 1

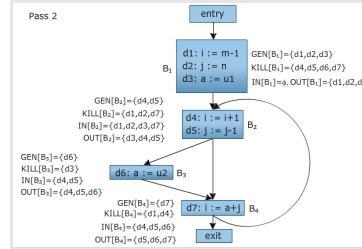


Figure 8: Pass 2

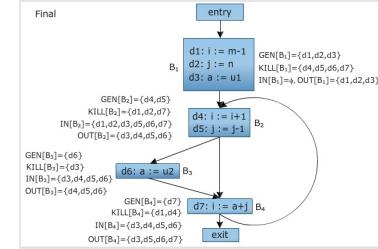


Figure 9: Pass 3

Algorithm 2 Reaching Definitions:Worklist Algorithm

Input: control flow graph CFG = (N, E, Entry, Exit)

```
out[Entry] =  $\emptyset$                                  $\triangleright$  Boundary condition
ChangedNodes = N
for each basic block B other than Entry do
    out[B] =  $\emptyset$                                  $\triangleright$  Initialization for iterative algorithm
end for
while ChangedNodes  $\neq \emptyset$  do
    Remove i from ChangedNodes
    in[B] =  $\cup$ (out[p]), for all predecessors p of B
    oldout = out[i]
    out[i] =  $f_i$ (in[i])                                 $\triangleright$   $out[i] = gen[i] \cup (in[i] - kill[i])$ 
    if oldout  $\neq$  out[i] then
        for all successors s of i do
            add s to ChangedNodes
        end for
    end if
end while
```

5 Available Expressions Analysis

5.1 Motivation

Programs may contain code whose result is needed, but in which some computation is simply a redundant repetition of earlier computation within the same program. The concept of expression availability is useful in dealing with this situation.

5.2 Backgroud Knowledge

Any given program contains a finite number of expressions (i.e. computations which potentially produce values), so we may talk about the set of all expressions of a program. Consider the program in

```
2 int z = x * y;
   print s + t;
   int w = u / v;
```

Listing 10: An

This program contian expression x*y,s+t,u/v.

5.3 Problem Formulation

Availability is a data-flow property of expressions: “Has the value of this expression already been computed?” At each instruction, each expression in the programis either available or unavailable. So each instruction(or node of the flowgraph) has an associated set of available expression.

5.4 Semantic vs. Syntactic

An expression is *semantically* available at a node n if its value gets computed (and not subsequently invalidated) along every execution sequence ending at n.

```
int x = y * z;
:
return y * z; y*z AVAILABLE
```

Figure 10: Available expression example

```
int x = y * z;
:
y = a + b;
:
return y * z; y*z UNAVAILABLE
```

Figure 11: unavailable expression example

An expression is *syntactically* available at a node n if its value gets computed (and not subsequently invalidated) along every path from the entry of the flowgraph to n.

```
if ((x+1) * (x+1) == y) {
    s = x + y;
}
if (x*x + 2*x + 1 != y) {
    t = x + y;
}
return x + y; x+y AVAILABLE
```

Figure 12: $x+y$ is semantically available

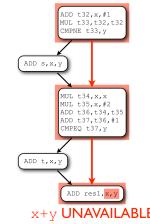


Figure 13: $x+y$ is syntactically unavailable

On the path in red from Figure 13 through the flowgraph, $x + y$ is only computed once, so $x + y$ is syntactically unavailable at the last instruction.

Whereas with live variable analysis we found safety in assuming that more variables were live, here we find safety in assuming that fewer expressions are available. Because if an expression is deemed to be available, we may do something dangerous (e.g. remove an instruction which recomputes its value). So sometimes safe means more, but sometimes means less.

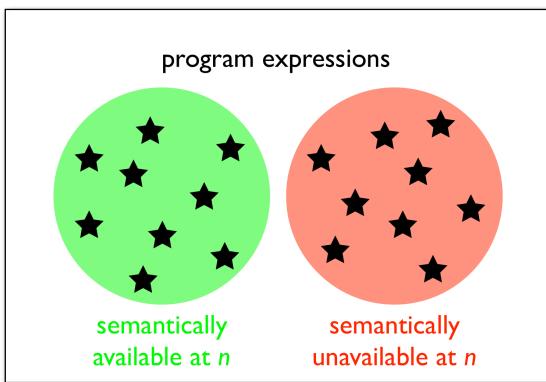


Figure 14: Semantic vs. syntactic

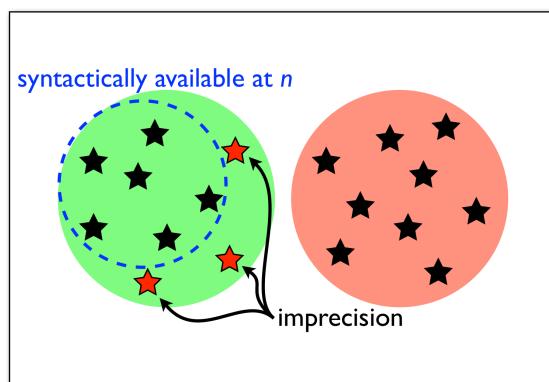


Figure 15: Semantic vs. syntactic

6 Foundations of Data Flow Analysis

We saw a lot of examples of data flow analysis, eg. reaching definitions etc. Although there were differences between different types of data flow analysis, they did share number of things in common. Our goal is to develop a general purpose data flow analysis framework.

There are some questions that we want to answer about a framework that performs data flow analysis.

- Correctness: Do we get a correct answer?
- Precision: How good is the answer?⁶
- Convergence: Will the analysis terminate?
- Speed: How fast is the convergence?

6.1 A Unified Framework

Data flow problems are defined by

- Domain of values V (eg, variable names for liveness, the instruction numbers for reaching definitions)
- Meet operator $V \wedge V \rightarrow V$ to deal with the join nodes.
- Initial value. Once we have defined the meet operator, it will tell us how to initialize all of the non-entry or exits nodes and the boundary conditions for entry and exit nodes.
- A set of transfer functions $V \rightarrow V$ to define how information flows across basic blocks.

Why we bother to define such a framework?

- First, if meet operator, transfer function and the domains of values are specified in proper way, we will know about correctness, precision and so on.
- From practical engineering perspective, it allows us to reuse code.

6.2 Partial Order

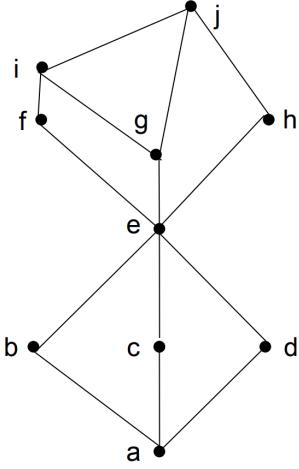
A relation R on a set S is called a **partial order** if it is

- **Transitivity** if $x \preceq y$ and $y \preceq z$ then $x \preceq z$
- **Antisymmetry** if $x \preceq y$ and $y \preceq x$ then $x = y$
- **Reflexivity** $x = x$

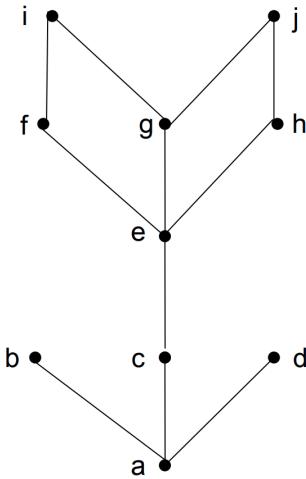
6.3 Lattice

A lattice is a partially ordered set in which every pair of elements has both a least upper bound (lub) and a greatest lower bound(glb).

⁶We want a safe solution but as precise as possible.



(a) This is a lattice example.



(b) This is not a lattice example because the pair b, c does not have a lub.

Figure 16: Two examples

6.4 Complete Lattice

A lattice A is called a complete lattice if every subset S of A admits a glb and a lub in A .

6.5 Semi-Lattice

A semilattice (or upper semilattice) is a partially ordered set that has a least upper bound for any nonempty finite subset.

6.6 Meet Operator

Meet operator must hold the following properties:

- **commutative:** $x \wedge y = y \wedge x$. No ordering in the incoming edges.
- **idempotent:** $x \wedge x = x$
- **associative :** $x \wedge (y \wedge z) = (x \wedge y) \wedge z$
- there is a Top element T such that $x \wedge T = x$. Partly due to the way we initialize everything we need.

Meet Operator defines a partial ordering on values. This is important in ensuring the analysis converges. So what does it mean ? $x \preceq y$ if and only if $x \wedge y = x$. The \preceq not means less or equal to or subset, but it really means lattice inclusion. So if $x \preceq y$, this means x is more conservative



Figure 17: Meet Operator

or constrained. In another word, x is lattice included in y . Partial ordering will also lead to some other properties

- **Transitivity** if $x \preceq y$ and $y \preceq z$ then $x \preceq z$
- **Antisymmetry** if $x \preceq y$ and $y \preceq x$ then $x = z$
- **Reflexivity** $x = x$

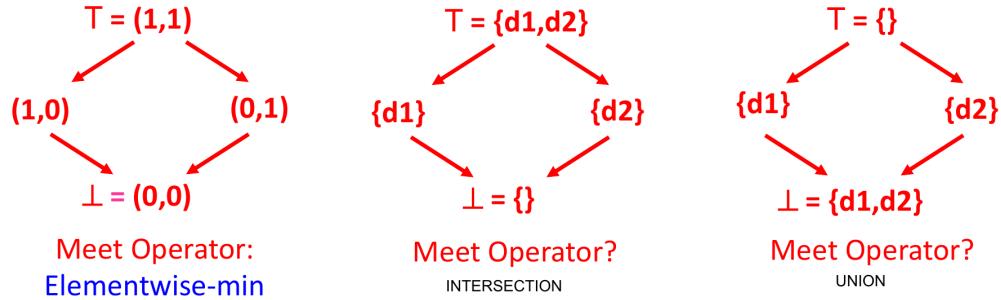


Figure 18: Different meet operator defines different lattice

For our data flow analysis, values and meet operator define a semi-lattice, which means \top exists, but not necessarily \perp .

6.7 Descending Chain

The height of a lattice is the largest number of \succ relations that will fit in a descending chain.
eg. $x_0 \succ x_1 \succ x_2 \succ \dots$

So, for reaching definitions, the height is the number of definitions.

Finite descending chain will ensure the convergence. If we don't have finite descending chain, there is a possibility that the analysis will never terminate. But an infinite lattice still can have a finite descending chain. I want to note that infinite lattice doesn't always mean a non-convergence.

So consider the constant propagation, the infinite lattice has finite descending chain, so this can converge.

6.8 Transfer Functions

Transfer function dictates how information propagates across a basic block. So what we need for our transfer function? **First**, it must have an identity function which means there exists an f such

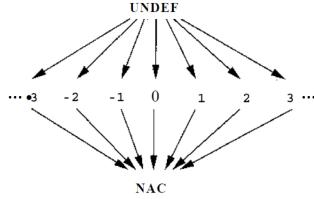


Figure 19: The lattice of constant propagation

that $f(x) = x$ for all x . For example, in Reaching Definitions and Liveness, when $\text{Gen}, \text{KILL} = \Phi$, this transfer function satisfies $f(x) = x$. **Second**, when we compose transfer functions, it must be consistent with the transfer function. So if $f_1, f_2 \in F$, the $f_1 \cdot f_2 \in F$.

For example,

$$\begin{aligned}
 f_1(x) &= G_1 \cup (x - K_1) \\
 f_2(x) &= G_2 \cup (x - K_2) \\
 f_2(f_1(x)) &= G_2 \cup [(G_1 \cup (x - K_1)) - K_2] \\
 &= [G_2 \cup (G_1 - K_2)] \cup [x - (K_1 \cup K_2)] \\
 G &= G_2 \cup (G_1 - K_2) \\
 K &= K_1 \cup K_2
 \end{aligned}$$

6.9 Monotonicity

A framework (F, V, \wedge) is monotone if and only if $x \preceq y$ implies $f(x) \preceq f(y)$. This means that a "smaller(more conservative) or equal" input to the same function will always give a "smaller(more conservative) or equal" output.

Alternatively, (F, V, \wedge) is monotone if and only if $f(x \wedge y) \preceq f(x) \wedge f(y)$. So merge input, then apply f is small(more conservative) or equal to apply the transfer function individually and then merge the result. Values are defined by semi-lattice, the meet operator only ever moves down the lattice from top towards the bottom. So we need to constrain the transfer function.

I will show you a unmonotone example.

Let top be 1 and bottom be 0 and the meet operator is \cap . $f(0) = 1, f(1) = 0$

Let's check whether reaching definitions is monotone.

Note that monotone framework does not mean $f(x) \preceq x$.

6.10 Distributivity

Reaching definitions is distributive but constant propagation is not.

7 Introduction to Static Single Assignment

Many dataflow analyses need to find the use-sites of each defined variable or the definition-sites of each variable used in an expression. The *def-use chain* is a data structure that makes this efficient: for each statement in the flow graph, the compiler can keep a list of pointers to all the use sites of variables defined there, and a list of pointers to all definition sites of the variables used there. An improvement on the idea of def-use chains is static single-assignment form, or SSA form, an intermediate representation in which each variable has only one definition in the program text. SSA is very useful for many optimizations such as Loop-Invariant Code Motion and Copy Propagation.

7.1 Definition-Use and Use-Definition Chains

Use-Definition (UD) Chains

For a given definition of a variable X, what are all of its uses?

Definition-Use (DU) Chains

For a given use of a variable X, what are all of the reaching definitions of X?

Unfortunately, it is expensive to use UD and DU chains, because if we have N defs, and M uses, the space complexity is $O(NM)$. An example is in 20

```
foo(int i, int j) {
    ...
    switch (i) {
        case 0: x=3; break;
        case 1: x=1; break;
        case 2: x=6; break;
        case 3: x=7; break;
        default: x = 11;
    }
    switch (j) {
        case 0: y=x+7; break;
        case 1: y=x+4; break;
        case 2: y=x-2; break;
        case 3: y=x+1; break;
        default: y=x+9;
    }
}
```

Figure 20: If a variable has N uses and M definitions (which occupy about $N + M$ instructions in a program), it takes space (and time) proportional to $N \cdot M$ to represent def-use chains – a quadratic blowup.

7.2 Static Single Assignment(SSA)

Static Single Assignment

Static Single Assignment is an IR where every variable is assigned a value at most once in the program text.

the Φ function

Φ merges multiple definitions along multiple control paths into a single definition. At a basic block with p predecessors, there are p arguments to the Φ functions.

$$x_{\text{new}} \leftarrow \Phi(x_1, x_2, x_3, \dots, x_p)$$

7.2.1 Why SSA is useful?

Useful for Dataflow Analysis Dataflow analysis and optimization algorithms can be made simpler when each variable has only one definition.

Less space and time complexity If a variable has N uses and M definitions (which occupy about $N + M$ instructions in a program), it takes space (and time) proportional to $N \cdot M$ to represent def-use chains – a quadratic blowup. For almost all realistic programs, the size of the SSA form is linear in the size of the original program.

Simplify some algorithms Uses and defs of variables in SSA form relate in a useful way to the dominator structure of the control-flow graph, which simplifies algorithms such as interference-graph construction.

Eliminate needless relationships Unrelated uses of the same variable in the source program become different variables in SSA form, eliminating needless relationships shown in 11.

```
1 for i <- 1 to N do A[i] <- 0
3 for i <- 1 to M do s <- s + B[i]
```

Listing 11: An example

7.3 How to represent SSA?

In straight-line code, such as within a basic block, it is easy to see that each instruction can define a fresh new variable instead of redefining an old one shown in 21

But when two control-flow paths merge together, it is not obvious how to have only one assignment for each variable. To solve this problem we introduce a notational fiction, called a Φ function. Figure 22 shows that we can combine a_1 (defined in block 1) and a_2 (defined in block 3) using the function $a_3 \leftarrow \Phi(a_1, a_2)$.

unlike ordinary mathematical functions, $\Phi(a_1, a_2)$ yields a_1 if control reaches block 4 along the edge $2 \rightarrow 4$, and yields a_2 if control comes in on edge $3 \rightarrow 4$.

$$\begin{array}{ll}
a \leftarrow x + y & a_1 \leftarrow x + y \\
b \leftarrow a - 1 & b_1 \leftarrow a_1 - 1 \\
a \leftarrow y + b & a_2 \leftarrow y + b_1 \\
b \leftarrow x \cdot 4 & b_2 \leftarrow x \cdot 4 \\
a \leftarrow a + b & a_3 \leftarrow a_2 + b_2
\end{array}$$

(a) A straight-line program.
(b) The program in single-assignment form.

Figure 21: SSA for straight-line code

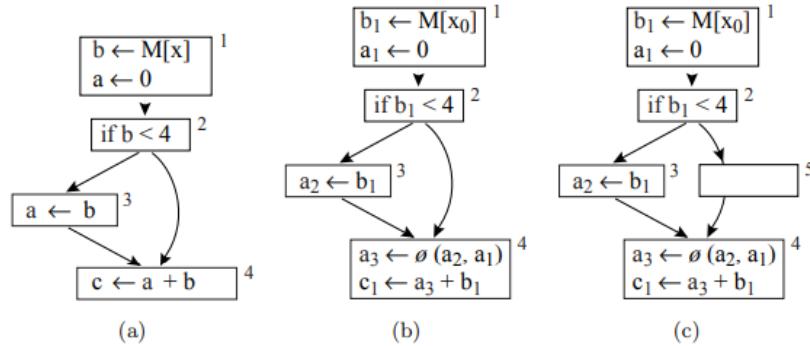


Figure 22: (a) A program with a control-flow join; (b) the program transformed to single-assignment form; (c) edge-split SSA form.

7.3.1 How does the ϕ -function know which edge was taken?

If we must execute the program, or translate it to executable form, we can “implement” the Φ -function using a move instruction on each incoming edge as shown in Figure 23. However, in many cases, we simply need the connection of uses to definitions and don’t need to “execute” the Φ -functions during optimization. In these cases, we can ignore the question of which value to produce.

7.4 Converting to SSA form

The algorithm for converting a program to SSA form is roughly as follows:

- 1. adds Φ functions for the variables, and then
- 2. renames all the definitions and uses of variables using subscripts.

7.4.1 Trivial SSA

Trivial SSA form is based on a simple observation: Φ functions are only needed for variables that are “live” after the Φ function.

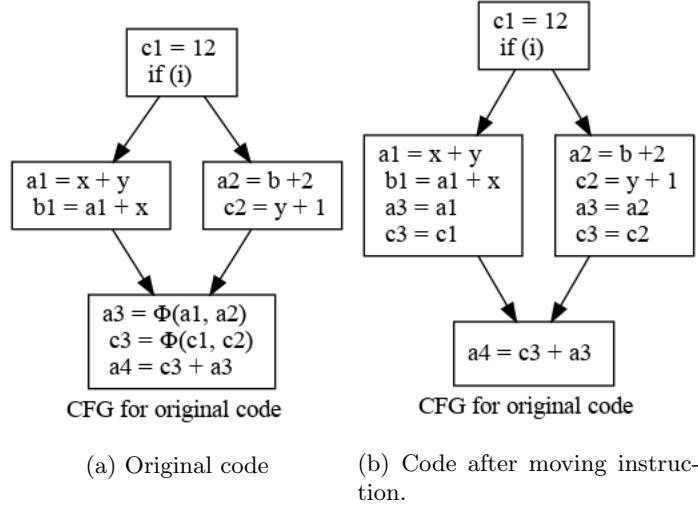


Figure 23: Implementing Φ -function

- Each assignment generates a fresh variable.
 - At each join point insert Φ for all live variables.

Trivial SSA will generate some useless Φ functions. An example is shown in Figure 24 So a Φ -function is not needed for every variable at each point.

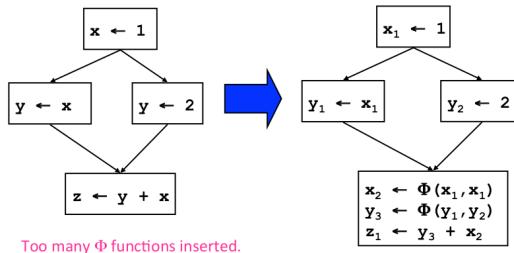


Figure 24: $x2 \leftarrow \Phi(x1, x1)$ is useless because $x2$ is equal to $x1$.

7.4.2 Minimal SSA

Minimal SSA is an updated version compared to trivial SSA.

- Each assignment generates a fresh variable.
 - At each join point insert Φ for all live variables with multiple outstanding defs.

7.4.3 Path-convergence criterion

There should be a Φ -function for variable a at node z of the flow graph exactly when all of the following are true:

- 1. There is a block x containing a definition of a ,
- 2. There is a block y (with $y \neq x$) containing a definition of a ,
- 3. There is a nonempty path P_{xz} of edges from x to z ,
- 4. There is a nonempty path P_{yz} of edges from y to z ,
- 5. Paths P_{xz} and P_{yz} do not have any node in common other than z , and
- 6. The node z does not appear within both P_{xz} and P_{yz} prior to the end, though it may appear in one or the other.

We consider the start node to contain an implicit definition of every variable, either because the variable may be a formal parameter or to represent the notion of $a \leftarrow$ uninitialized without special cases. A Φ -function itself counts as a definition of a , so the path-convergence criterion must be considered as a set of equations to be satisfied. As usual, we can solve them by iteration as shown in 3.

Algorithm 3 Iterated path-convergence criterion

```
while there are nodes  $x, y, z$  satisfying conditions 1–5 and  
z does not contain a  $\Phi$ -function for a do  
    insert  $a \leftarrow \Phi(a, a, \dots, a)$  at node Z  
end while
```

7.4.4 Dominance property of SSA form

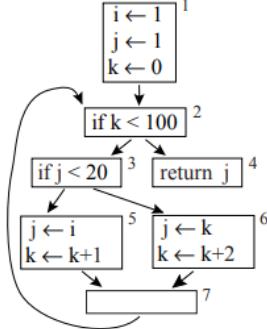
The iterated path-convergence algorithm for placing Φ -functions is not practical, since it would be very costly to examine every triple of nodes x, y, z , and every path leading from x and y . A much more efficient algorithm using the dominator tree of the flow graph as shown in Figure 25.

```

 $i \leftarrow 1$ 
 $j \leftarrow 1$ 
 $k \leftarrow 0$ 
while  $k < 100$ 
    if  $j < 20$ 
         $j \leftarrow i$ 
         $k \leftarrow k + 1$ 
    else
         $j \leftarrow k$ 
         $k \leftarrow k + 2$ 
    return  $j$ 

```

(a) Program



(b) CFG

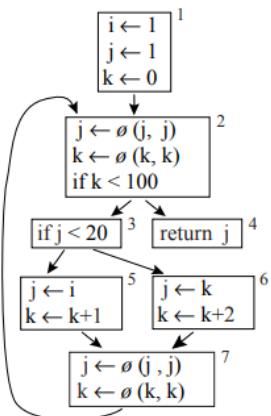
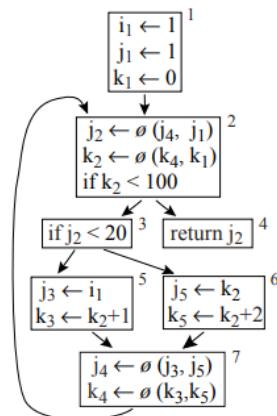


(c) Dominator tree

n	$DF(n)$
1	{}
2	{2}
3	{2}
4	{}
5	{7}
6	{7}
7	{2}

(d) Dominance frontiers

Variable j defined in node 1, but $DF(1)$ is empty. Variable j defined in node 5, $DF(5)$ contains 7, so node 7 needs $\phi(j, j)$. Now j is defined in 7 (by a ϕ -function), $DF(7)$ contains 2, so node 2 needs $\phi(j, j)$. $DF(6)$ contains 7, so node 7 needs $\phi(j, j)$ (but already has it). $DF(2)$ contains 2, so node 2 needs $\phi(j, j)$ (but already has it). Similar calculation for k . Variable i defined in node 1, $DF(1)$ is empty, so no ϕ -functions necessary for i .

(e) Insertion criteria for ϕ -functions(f) ϕ -functions inserted

(g) Variables renamed

Figure 25: Conversion of a program to static single-assignment form. Node 7 is a postbody node, inserted to make sure there is only one loop edge; such nodes are not strictly necessary but are sometimes helpful.

Strictly dominance

x strictly dominates w (x sdom w) iff impossible to reach w without passing through x first.

Dominance

x dominates w ($x \text{ dom } w$) iff $x \text{ sdom } w$ or $x = w$.

$$\text{Dom}(n) = \begin{cases} \{n\} & \text{if } n = n_0 \\ \{n\} \cup \left(\bigcap_{p \in \text{preds}(n)} \text{Dom}(p) \right) & \text{if } n \neq n_0 \end{cases}$$

Dominance tree

$x \text{ sdom } w$ iff x is a proper ancestor of w.

Dominance Frontier

The dominance frontier of a node x is the set of all nodes w such that x dominates a predecessor of w, but does not strictly dominate w.

$$F(x) = \{w \mid x \text{ dom pred}(w) \text{ AND } !(x \text{ sdom } w)\}$$

An essential property of static single assignment form is that definitions dominate uses; more specifically,

- If x is the ith argument of a Φ -function in block n, then the definition of x dominates the ith predecessor of n.
- If x is used in a non- Φ statement in block n, then the definition of x dominates n

Dominance Property of SSA

In SSA,

- If x_i is used in $x \leftarrow \Phi(\dots, x_i, \dots)$, then $BB(x_i)$ dominates ith predecessor of $BB(\Phi)$
- If x is used in $y \leftarrow \dots x \dots$, then $BB(x)$ dominates $BB(y)$

Dominance frontier criterion. Whenever node x contains a definition of some variable a, then any node z in the dominance frontier of x needs a Φ -function for a.

Iterated dominance frontier. Since a Φ -function itself is a kind of definition, we must iterate the dominance-frontier criterion until there are no nodes that need Φ -functions.

Theorem. The iterated dominance frontier criterion and the iterated path convergence criterion specify exactly the same set of nodes at which to put Φ -functions

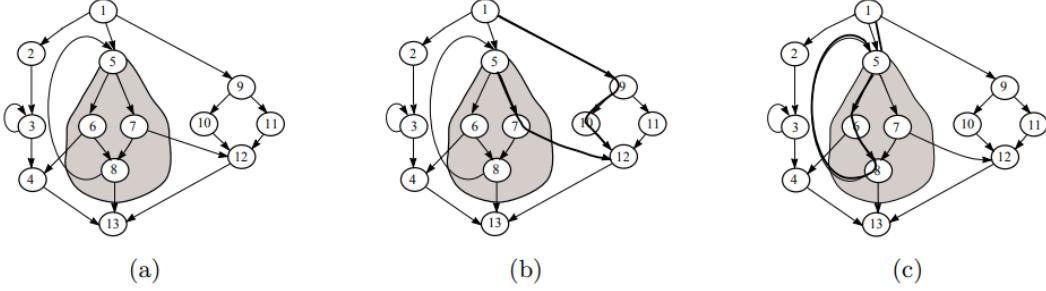


Figure 26: Node 5 dominates all the nodes in the grey area. (a) Dominance frontier of node 5 includes the nodes (4, 5, 12, 13) that are targets of edges crossing from the region dominated by 5 (grey area including node 5) to the region not strictly dominated by 5 (white area including node 5). (b) Any node in the dominance frontier of n is also a point of convergence of nonintersecting paths, one from n and one from the root node. (c) Another example of converging paths $P_{1,5}$ and $P_{5,5}$.

Proof

The sketch of a proof that shows if w is in the dominance frontier of a definition, then it must be a point of convergence.

Suppose there is a definition of variable a at some node n (such as node 5 in Figure 26b), and node w (such as node 12 in Figure 26b) is in the dominance frontier of n . The root node implicitly contains a definition of every variable, including a . There is a path P_{rw} from the root node (node 1 in Figure 26) to w that does not go through n or through any node that n dominates; and there is a path P_{nw} from n to w that goes only through dominated nodes. These paths have w as their first point of convergence.

7.5 Computing the dominance frontier

To insert all the necessary Φ -functions, for every node n in the flow graph we need $DF[n]$, its dominance frontier. Given the dominator tree, we can efficiently compute the dominance frontiers of all the nodes of the flow graph in one pass. We define two auxiliary sets

- $DF_{local}[n]$ The successors of n that are not strictly dominated by n ;
- $DF_{up}[n]$ Nodes in the dominance frontier of n that are not dominated by n 's immediate dominator.

The dominance frontier of n can be computed from $DF_{local}[n]$ and $DF_{up}[n]$

$$DF[n] = DF_{local}[n] \cup \bigcup_{c \in \text{children}[n]} DF_{up}[c]$$

where $\text{children}[n]$ are the nodes whose immediate dominator (idom) is n .

To compute $DF_{local}[n]$ ⁴ more easily (using immediate dominators instead of dominators), we use the following theorem: $DF_{local}[n] =$ the set of those successors of n whose immediate dominator is not n . The following `computeDF` function should be called on the root of the dominator tree (the start node of the flow graph). It walks the tree computing $DF[n]$ for every node n : it computes $DF_{local}[n]$ by examining the successors of n , then combines $DF_{local}[n]$ and (for each child c) $DF_{up}[n].a$

Algorithm 4 `computeDF`

```

 $S \leftarrow \{\}$ 
for each node  $y$  in  $\text{succ}[n]$  do                                 $\triangleright$  This loop computes  $DF_{local}[n]$ 
    if  $\text{idom}(y) \neq n$  then
         $S \leftarrow S \cup \{y\}$ 
    end if
end for
for each child  $c$  of  $n$  in the dominator tree do
    computeDF[ $c$ ]
    for each element  $w$  of  $DF[c]$  do                 $\triangleright$  This loop computes  $DF_{up}[n]$ 
        if  $n$  does not dominate  $w$  then
             $S \leftarrow S \cup \{w\}$ 
        end if
    end for
end for

```

This algorithm is quite efficient. It does work proportional to the size (number of edges) of the original graph, plus the size of the dominance frontiers it computes. Although there are pathological graphs in which most of the nodes have very large dominance frontiers, in most cases the total size of all the DFs is approximately linear in the size of the graph, so this algorithm runs in “practically” linear time.

7.6 Inserting Φ -functions

Starting with a program not in SSA form, we need to insert just enough Φ -functions to satisfy the iterated dominance frontier criterion. To avoid re-examining nodes where no Φ -function has been inserted, we use a work-list algorithm.

Algorithm 5 starts with a set V of variables, a graph G of controlflow nodes – each node is a basic block of statements – and for each node n a set $A_{orig}[n]$ of variables defined in node n . The algorithm computes $A_\Phi[a]$, the set of nodes that must have Φ -functions for variable a . Sometimes a node may contain both an ordinary definition and a Φ -function for the same variable; for example, in Figure 26b, $a \in A_{orig}[2]$ and $2 \in A_\Phi[a]$.

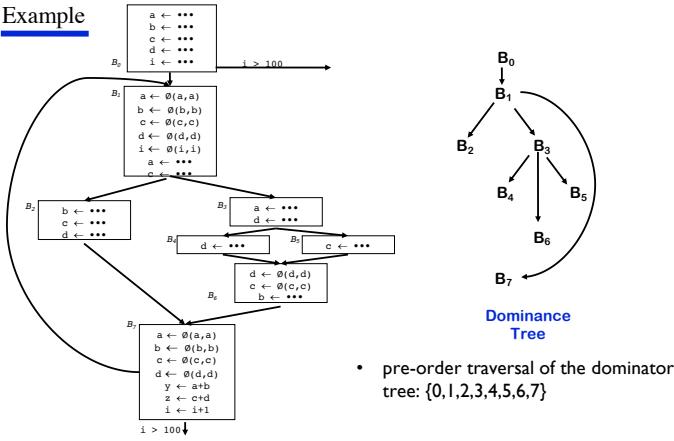
This algorithm does a constant amount of work (a) for each node and edge in the control-flow graph, (b) for each statement in the program, (c) for each element of every dominance frontier, and (d) for each inserted Φ -function. For a program of size N , the amounts a and b are proportional to N , c is usually approximately linear in N . The number of inserted Φ -functions (d) could be N^2 in the worst case, but empirical measurement has shown that it is usually proportional to N . So in practice, Algorithm 5 runs in approximately linear time.

7.7 Renaming the variables

After the Φ -functions are placed, we can walk the dominator tree, renaming the different definitions (including Φ -functions) of variable a to a_1, a_2, a_3 and so on. Rename each use of a to use the closest definition d of a that is above a in the dominator tree. Algorithm renames all uses and definitions of variables, after the Φ -functions have been inserted by Algorithm 6. In traversing the dominator tree, the algorithm “remembers” for each variable the most recently defined version of each variable, on a separate stack for each variable. Although the algorithm follows the structure of the dominator tree – not the flow graph – at each node in the tree it examines all outgoing flow edges, to see if there are any Φ -functions whose operands need to be properly numbered.

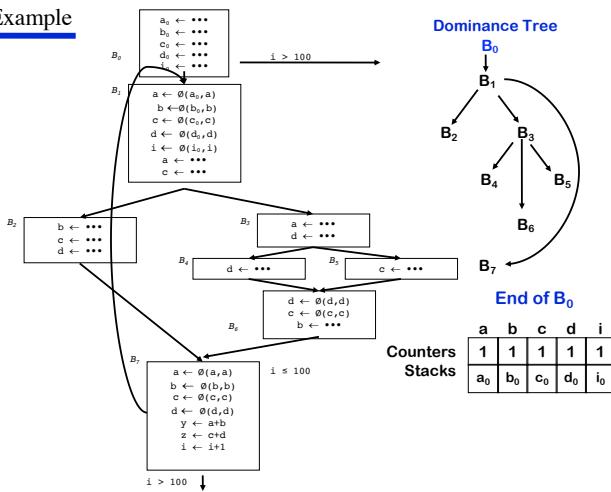
7.7.1 Example

Example



- pre-order traversal of the dominator tree: {0,1,2,3,4,5,6,7}

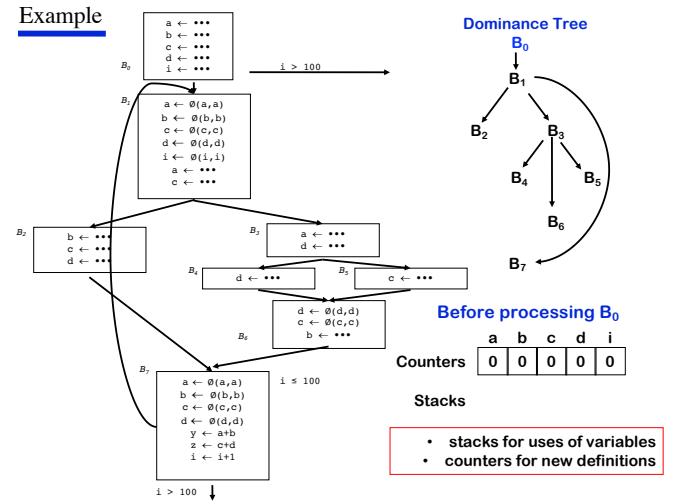
Example



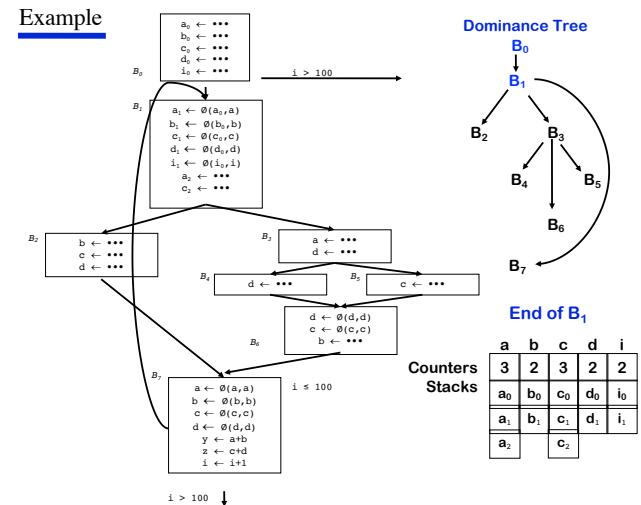
Counters
Stacks

a	b	c	d	i
1	1	1	1	1
a_0	b_0	c_0	d_0	i_0

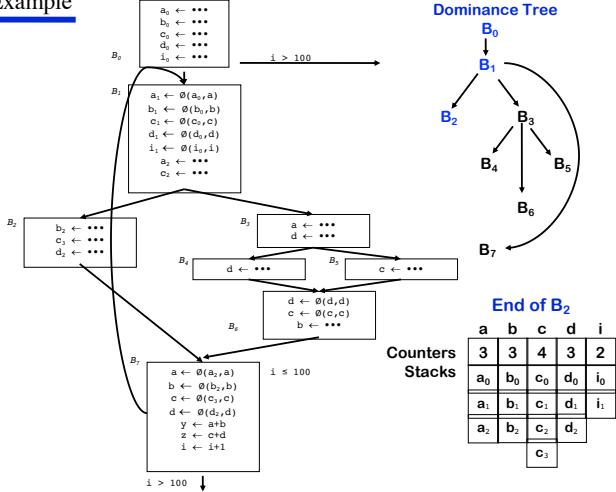
Example



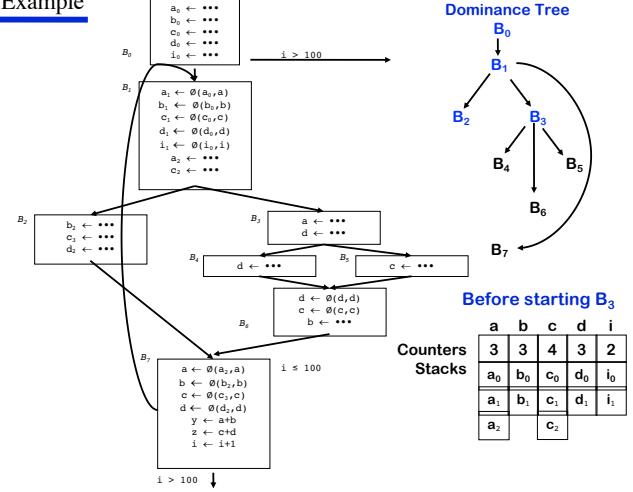
Example



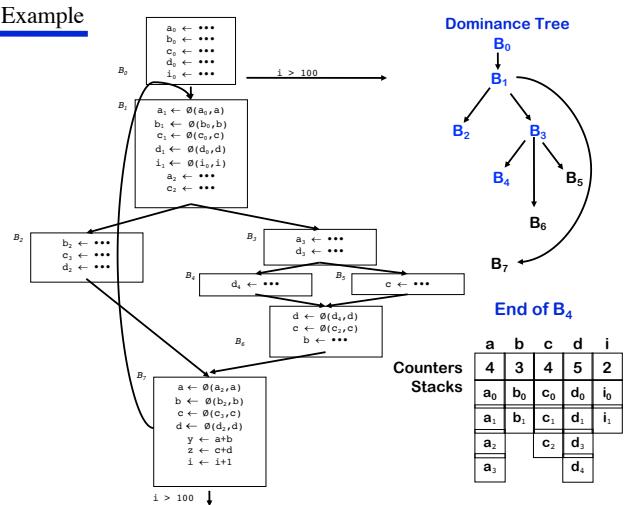
Example



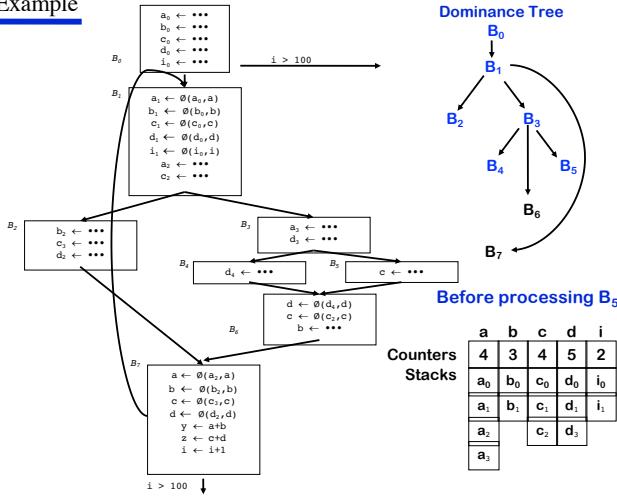
Example



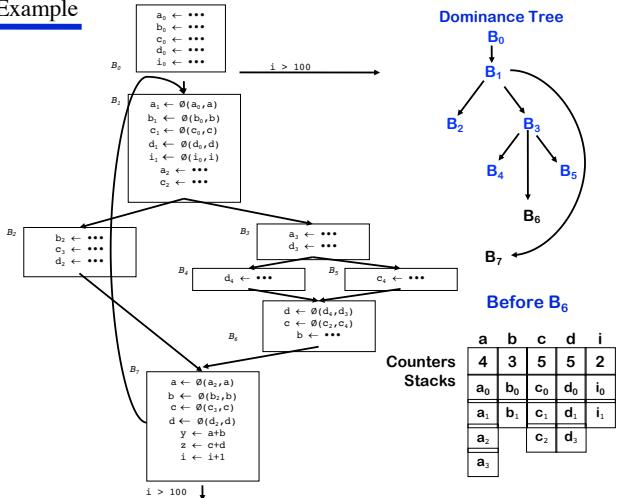
Example



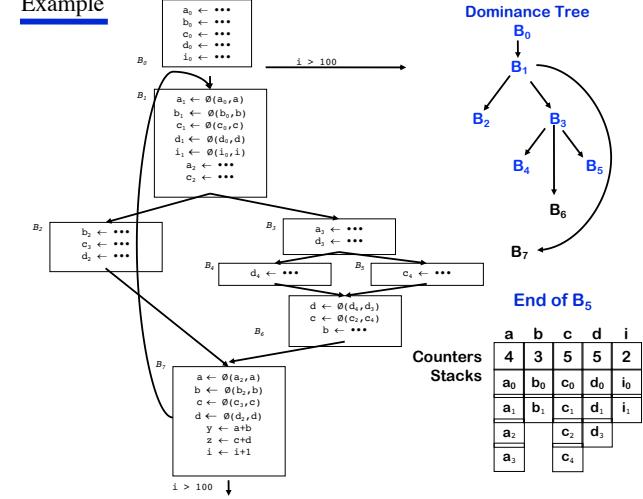
Example



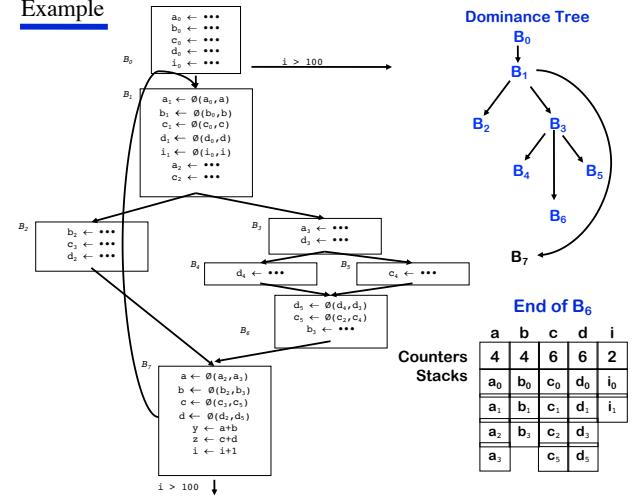
Example



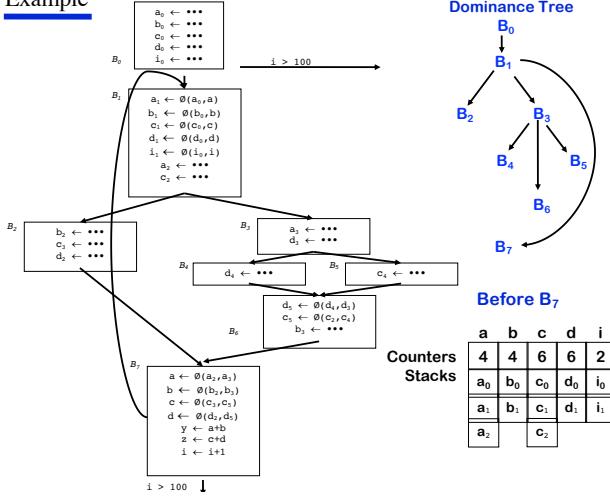
Example



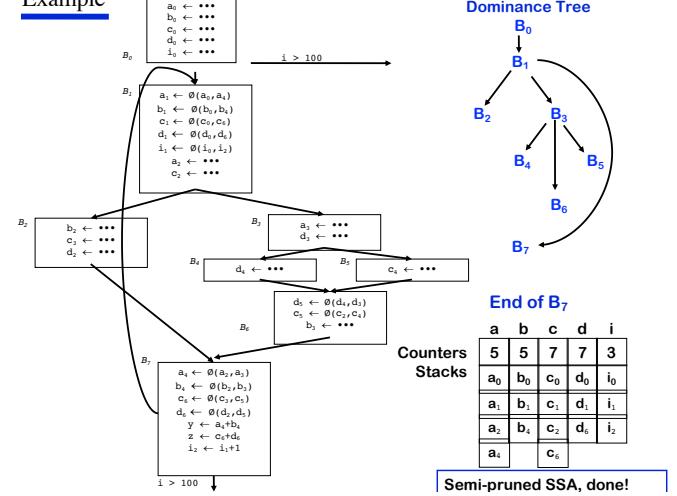
Example



Example



Example



End of B₇

	a	b	c	d	i
a ₀	5	5	7	7	3
b ₀	a ₀	b ₀	c ₀	d ₀	i ₀
a ₁	b ₁	c ₁	d ₁	i ₁	
a ₂	b ₄	c ₂	d ₆	i ₂	
a ₃		c ₆			

Semi-pruned SSA, done!

Algorithm 5 Place- Φ -Functions

```
for each node n do
    for each variable a in  $A_{orig}[n]$  do
        defsites[a]  $\leftarrow$  defsites[a]  $\cup \{n\}$ 
    end for
end for
for each variable a do
    W  $\leftarrow$  defsites[a]
    while W not empty do
        remove some node n from W
        for each y in DF[n] do
            if y  $\notin A_\Phi[a]$  then
                insert the statement  $a \leftarrow \Phi(a, a, \dots, a)$  at the top of block y, where the  $\Phi$ -function
                has as many arguments as y has predecessors
                 $A_\Phi[a] \leftarrow A_\Phi[a] \cup \{y\}$ 
                if a  $\notin A_{orig}[y]$  then
                    W  $\leftarrow W \cup \{y\}$ 
                end if
            end if
        end for
    end while
end for
```

7.8 Edge Splitting

Some analyses and transformations including reverse transformation from SSA back into a normal form are simpler if there is never a controlflow edge that leads from a node with multiple successors to a node with multiple predecessors. To give the graph this unique successor or predecessor property, we perform the following transformation: For each control-flow edge $a \leftarrow b$ such that a has more than one successor and b has more than one predecessor, we create a new, empty controlflow node z , and replace the $a \leftarrow b$ edge with an $a \leftarrow z$ edge and a $z \leftarrow b$ edge.

An SSA graph with this property is in edge-split SSA form. Figure 22 illustrates edge splitting. Edge splitting may be done before or after insertion of Φ -functions.

Algorithm 6 Renaming variables.

Initialization:

for each variable a **do**

- Count[a] \leftarrow 0
- Stack[a] \leftarrow empty
- push 0 onto Stack[a]

end for

Rename(n)

for each statement S in block n **do**

- if** S is not a Φ -function **then**
- for** each use of some variable x in S **do**

 - i \leftarrow top(Stack[x])
 - replace the use of x with x_i in S

- end for**
- end if**
- for** each definition of some variable a in S **do**

 - Count[a] \leftarrow Count[a]+1
 - i \leftarrow Count[a]
 - push i onto Stack[a]
 - replace definition of a with definition of a_i in S

- end for**

end for

for each successor Y of block n, **do**

- Suppose n is the jth predecessor of Y
- for** each Φ -function in Y **do**

 - suppose the jth operand of the Φ -function is a
 - i \leftarrow top(Stack[a])
 - replace the jth operand with a_i

- end for**

end for

for each child X of n **do**

- Rename(X)

end for

for each definition of some variable a in the original S **do**

- pop Stack[a]

end for

8 SSA-Style optimizations

8.1 Constant Propagation

notes

- If $v \leftarrow c$, replace all uses of v with c
- If $v \leftarrow \Phi(c, c, c)$ (each input is the same constant), replace all uses of v with c

Algorithm 7 SSA-CP

```
W ← ist of all defs
while !W.isEmpty do
    Stmt S ← W.removeOne
    if (S has form  $v \leftarrow c$ ) or (S has form  $v \leftarrow \Phi(c, \dots, c)$ ) then
        delete S
        for each stmt U that uses v do
            replace v with c in U
            W.add(U)
        end for
    end if
end while
```

8.2 Conditional Constant Propagation

Wegman and Zadeck's Sparse Conditional Constant (SCC) algorithm was used to find constant expressions, constant conditions, and unreachable code [WZ91]. The output of the SCC algorithm is an association of variables to one of $\{\perp, c, \top\}$, where \perp marks a variable that can hold different values at different times, and \top means the variable is not executed. In addition, every flow-graph node (corresponding to a quadruple) is marked as executable or non-executable. We then walk the flow-graph, eliminating dead-code (quadruples marked non-executable), replacing constant variables with their values, and changing constant conditional branches to goto statements.

notes

- Assume all blocks unexecuted until proven otherwise
- Assume all variables are not executed (only with proof of assignment of a non-constant value do we assume not constant)

8.2.1 Example

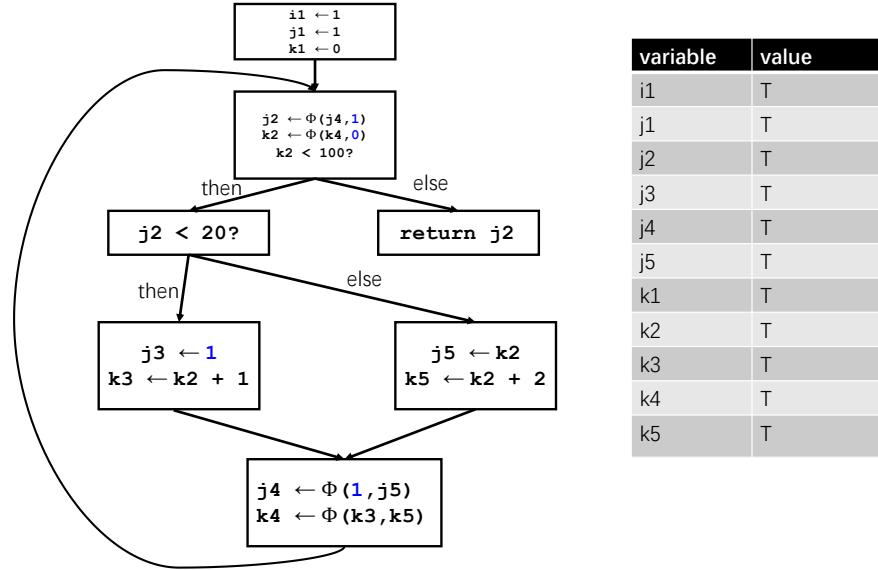


Figure 27: Original code. The black block is marked as unexecuted

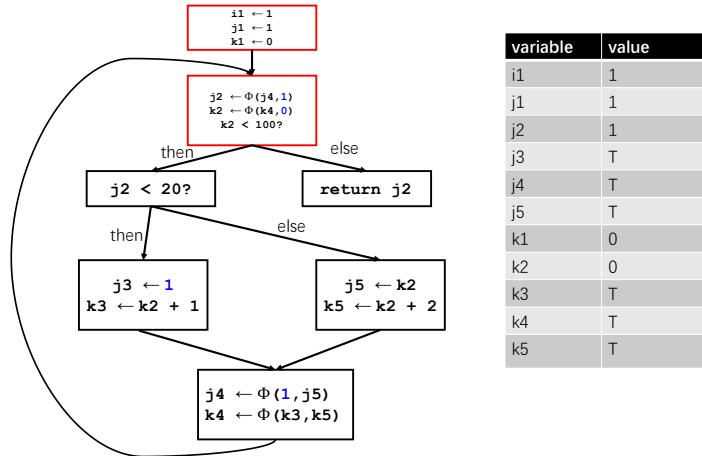


Figure 28: The read block is marked as executed. After walking the first two blocks, the value is shown above.

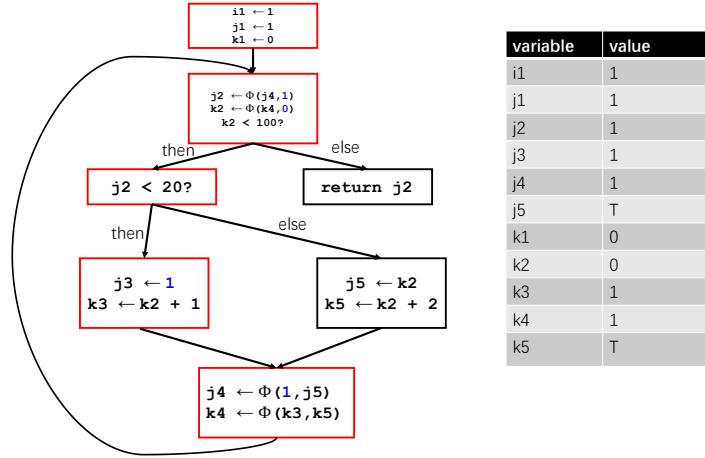


Figure 29: After walking 5 blocks.

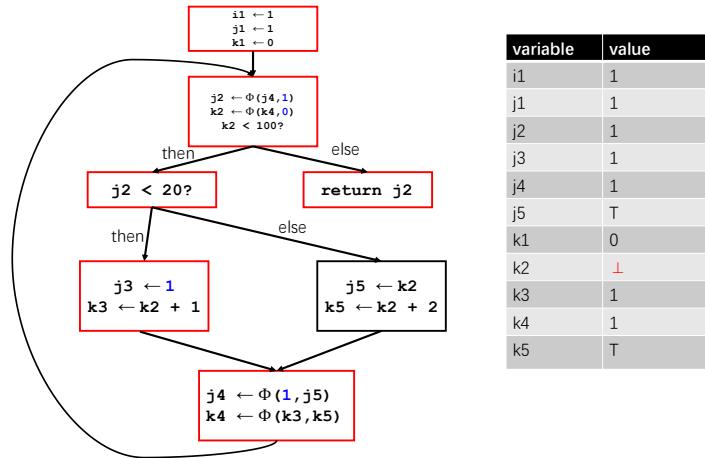


Figure 30: Now $k2$ is \perp , so the $\text{return } j2$ is reachable.

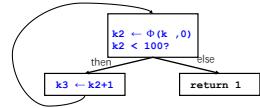


Figure 31: Code after applied SCC.

8.3 Copy Propagation

notes

- delete $x \leftarrow \Phi(y, y, y)$ and replace all x with y
- delete $x \leftarrow y$ and replace all x with y

8.4 Aggressive Dead Code Elimination

We can easily define the standard algorithm 8 below, but this algorithm may leave zombies. Look at the example in Figure 32

Algorithm 8 Dead Code Elimination

```

W ← list of all defs
while !W.isEmpty do
    Stmt S ← W.removeOne
    if |S.users| = 0 then
        continue
    end if
    if S.hasSideEffects() then
        continue
    end if
    for def in S.operands.definers do
        def.users ← def.users - {S}
        if |def.users| == 0 then
            W ← W UNION {def}
        end if
    end for
    delete S
end while

```



(a) Original code. We can easily find that use chain so we can not remove instructions relating to i are dead and can relate to i because i_1 uses i_2 , and i_2 uses i_1 .
(b) SSA format code. Since there is a circle

Figure 32: An example to illustrate standard DCE can leave zombies.

So instead of assuming everything is live until proven dead, we go another way: assuming everything is dead until proven live shown in algorithm 9.

Algorithm 9 Aggressive Dead Code Elimination

```

function INIT
    mark as live all stmts that have side-effects:
        I/O
        stores into memory
        returns
        calls a function that MIGHT have side-effects
    As we mark S live, insert S.operands.definers into W
    while |W| > 0 do
        S ← W.removeOne()
        if (S is live) then
            continue
        end if
        mark S live, insert S.operands.definers into W
    end while
end function

```

8.4.1 Problems within algorithm 9

After ADCE 9 shown in 33c, there is only one `return` statement left. However, control flow is undecidable in general, so possibly the loop in 33b will iterate indefinitely and the `return` instruction will never be executed. The problem here is we simply mark the branch statement dead.

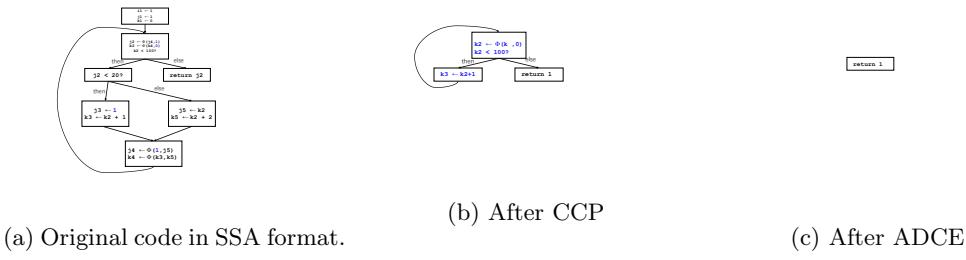


Figure 33: An example to illustrate the algorithm 9 has a problem.

Also when we apply this algorithm to 32, we can find that $j2 < 10$ is marked dead which is wrong. Of course, we can simply mark all branches live in the initialize stage, but this is not the ideal solution.

Now we need to carefully consider which conditional branches need to be marked live.

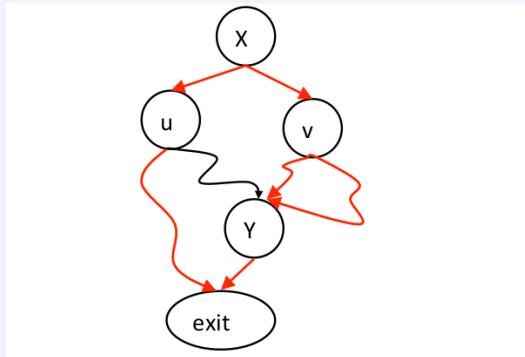
8.4.2 Control Dependence

control dependence

Y is control-dependent on X if

- X branches to u and v
- \exists a path $u \rightarrow \text{exit}$ which does not go through Y
- \forall paths $v \rightarrow \text{exit}$ go through Y

This means X can determine whether or not Y is executed.



8.4.3 Aggressive Dead Code Elimination(Fixed Version)

So we make a little modification 10. When we mark S is live, we should also mark live those conditional branches upon which S is control dependent.

Algorithm 10 Aggressive Dead Code Elimination(Fixed Version)

```
function INIT
    mark as live all stmts that have side-effects:
        I/O
        stores into memory
        returns
        calls a function that MIGHT have side-effects
    As we mark S live, insert S.operands.definers into W
    S.CD-1 into W
    while |W| > 0 do
        S ← W.removeOne()
        if (S is live) then
            continue
        end if
        mark S live, insert S.operands.definers into W
        S.CD-1 into W
    end while
end function
```

8.4.4 Finding the Control Dependence Graph

- Construct CFG
- Add entry node and exit node
- Add (entry, exit) edge
- Create G' , the reverse CFG
- Compute D-tree in G' (post-dominators of G)
- Compute $DF'_G(y)$ for all $y \in G'$ (post-DF of G)
- Add $(x,y) \in G$ to CDG if $x \in DF'_G(y)$

So let us calculate the control dependence for Figure 32a which is shown in Figure 34. Since Block1 is control dependent on Block1, so the conditional branch in Block1 $j2 < 10 ?$ should be marked live now.

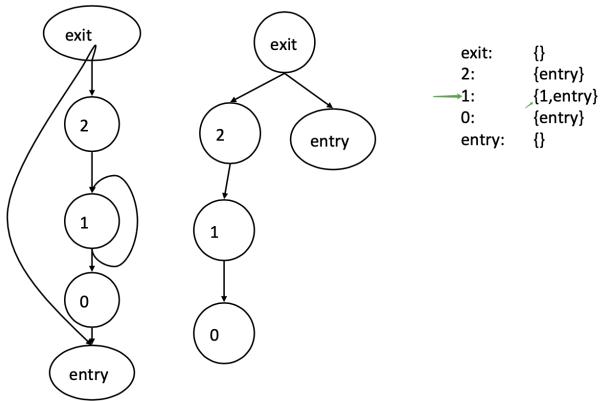


Figure 34: From left to right are G_t , post-dominators of G and post-DF of G respectively.

9 The LLVM project

LLVM is an open-source framework providing a modern collection of modular and reusable compiler and toolchain technologies [20]. The project stemmed from the work of Chris Lattner, who first implemented core elements of LLVM to support the research of his master thesis in 2002 [26]. One of the key strengths of LLVM is that it faces active development from an expert community of contributors, and is widely used across the industry and academia alike [11]. The project received the ACM Software System Award in 2012 [4] as an acknowledgement of its contribution to compiler research and implementation.

LLVM officially acknowledges more than 10 main sub-projects [20], which range in diversity from a debugger [9] to a symbolic execution tool [8]. In addition to these, the official website presents a long list of miscellaneous projects that are based on components of the LLVM infrastructure [19].

All projects which are part of the LLVM ecosystem are built upon the core libraries, which are arguably the centrepiece of LLVM. They host the source- and target-independent optimizer (Section 3.3), the implementation of the LLVM intermediate representation (Section 3.2), and a suite of command-line tools useful for code manipulation (Section 3.4). The core libraries also implement various back-end passes that translate IR to machine code for different platforms (x86, PowerPC, Nvidia GPUs). For building a complete compiler for a source language, the LLVM core libraries readily provide the optimizing pass and code generation for common architectures, the frontend being the only missing component. Clang is by far the most prominent front-end implemented in LLVM [5], and it targets the family of C languages (C/C++ and Objective-C/C++). Coupled with the core libraries, Clang is a powerful compiler producing high-performance code, and positions itself as a direct competitor to both gcc and the Intel compiler.

10 Loop Invariant Computation and Code Motion

Loop-Invariant Code Motion (LICM) recognizes computations within a loop that produce the same result each time the loop is executed. These computations are called loop-invariant code and can be moved outside the loop body without changing the program semantics. The positive effects of LICM are:

- The shifted loop invariants exhibit a reduced execution frequency.
- The transformation may shorten variable live ranges leading to a decreased register pressure. This circumstance may in turn reduce the number of required spill code instructions.
- Moving code outside a loop reduces the loop's size which may be beneficial for the I-cache behavior since more loop code can reside in the cache.

Besides these positive effects on the code, LICM may also degrade performance. This is mainly due to two reasons. First, the newly created variables to store the loop-invariant results outside the loop, may increase the register pressure in the loops since their live ranges span across the entire loop nest. As a result, possibly additional spill code is generated. Second, LICM might lengthen other paths of the control flow graph. This situation can be observed if the invariants are moved from a less executed to a more frequently executed path, e.g., moving instructions above a loop's zero-trip test.

10.1 Finding natural loops

Not every cycle is a loop in CFG. From a intuitive perspective, a loop must has a single entry and edges must from at least one circle.

Back Edge

A back edge is an arc $t \rightarrow h$ whose head h dominates its tail t

Natural Loop

The natural loop of a back edge $t \rightarrow h$ is the smallest set of nodes that includes t and h , and has no predecessors outside the set, except for the predecessors of the header h .

Reducible

A flow graph is reducible if every retreating edge in any DFST (Deep-First Spanning Tree) for that flow graph is a back edge.

Testing reducibility Take any DFST for the flow graph, remove the back edges, and check that the result is acyclic.

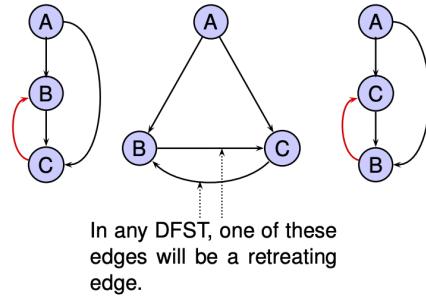


Figure 35: Example: Nonreducible Graph

10.2 Algorithm to Find Natural Loops

10.2.1 Step 1. Finding Dominators

We can formulate this as Data Flow Analysis problem. Since Node d dominates node n in a graph ($d \text{ dom } n$) if every path from the start node to n goes through d. So if $d \text{ dom } n$ iff $\text{dom } p \text{ for all pred } p \text{ of } n$.

Direction	Forward
Values	Basic Blocks
Meet operator	\cap
Top(T)	Universal Set
Bottom	ϕ
Boundary condition for entry node	ϕ
Initialization for internal nodes	T
Finitude ascending chain?	✓
Transferfunction	$\text{OUT} [b] = \{b\} \cup (\cap_{\{p=\text{pred}(b)\}} \text{OUT} [p])$
Monotone&Distributive?	✓

With rPostorder, most flow graphs (reducible flow graphs) converge in 1 pass.

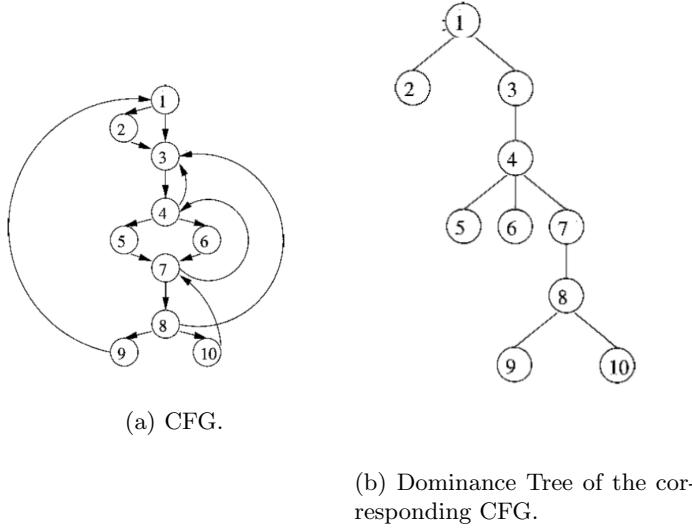


Figure 36: An example of Dominance tree.

10.2.2 Step 2. Finding Back Edges

Depth-first spanning tree Edges traversed in a depth-first search of the flow graph form a depth-first spanning tree. We categorize edges in CFG as follows:

- Forward edges (node to proper descendant).
- Retreating edges (node to ancestor).
- Cross edges (between two nodes, neither of which is an ancestor of the other.)

This is something difficult to understand. Let's make it simpler. We can number each node when we visit it. So each edge should be satisfied the following property:

Forward/Advancing edges $n_1 \rightarrow n_2$	$\text{num}(n_1) < \text{num}(n_2)$ and n_1 is ancestor of n_2
Cross edges $n_1 \rightarrow n_2$	$\text{num}(n_1) > \text{num}(n_2)$ and neither n_1 is ancestor of n_2 nor n_2 is ancestor of n_1
Retreating edges $n_1 \rightarrow n_2$	$\text{num}(n_1) > \text{num}(n_2)$ and n_2 is ancestor of n_1

Of these edges, only retreating edges go from high to low in DF order.

Algorithm

- Perform a depth first search
- For each retreating edge $t \rightarrow h$, check if h is in t 's dominator list

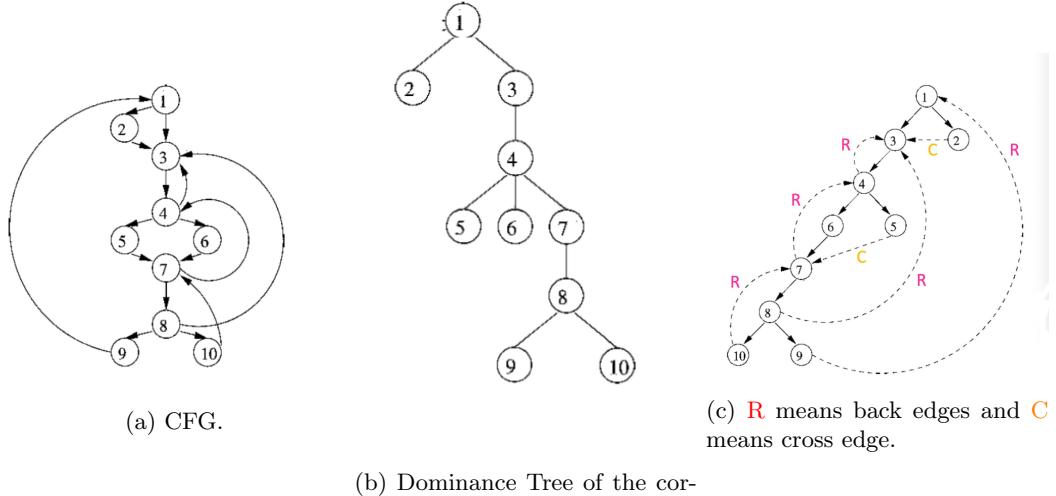


Figure 37: An example of Back Eges.

10.2.3 Step 3. Constructing Natural Loops

Algorithm For each back edge $t \rightarrow h$:

- delete h from the flow graph
 - find those nodes that can reach t (those nodes plus h form the natural loop of $t \rightarrow h$)

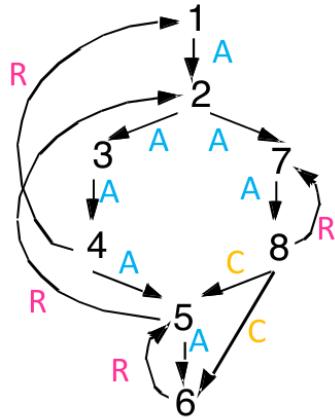


Figure 38: For this flow graph, for back edge $8 \rightarrow 7$, natural loop is $\{ 7,8 \}$, for back edge $5 \rightarrow 2$, natural loop is $\{ 2,3,4,5,6,7,8 \}$, back edge $4 \rightarrow 1$, natural loop is $\{ 1,2,3,4,5,6,7,8 \}$.

10.3 Inner Loops

If two different loops don't have the same header, they are either disjoint or one is entirely contained the other (inner loop is the one that contains no other loop.). If two loops share the same header shown in reffig:p65, it is hard to tell which is the inner loop. But we can combine and treat as one loop.

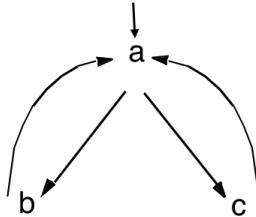


Figure 39: Two loops share the same header.

10.4 Loop-Invariant Computation and Code Motion

Loop-Invariant Computation

A loop-invariant computation is a computation whose value doesn't change as long as control stays within the loop. loop invariant whose operands are defined outside loop or invariant themselves.

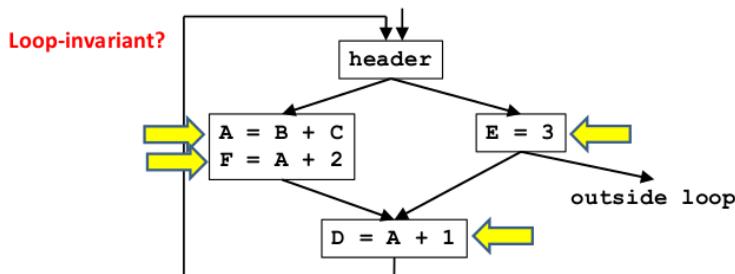


Figure 40: For this CFG, $A = B + C$, $F = A + 2$, $E = 3$ are Loop-Invariant Computation, but $D = A + 1$ is not.

Not all loop invariant instructions can be moved to preheader.

10.5 LICM Algorithm

- Find invariant expressions
- Conditions for code motion

- Code transformation

10.6 Find invariant expressions

- Compute reaching definitions
- Repeat: mark $A = B + C$ as invariant if
 - All reaching definitions of B are outside the loop or there is exactly one reaching definition for B and it is from a loop-invariant statement inside the loop.
 - Check the same for C.
- Code transformation

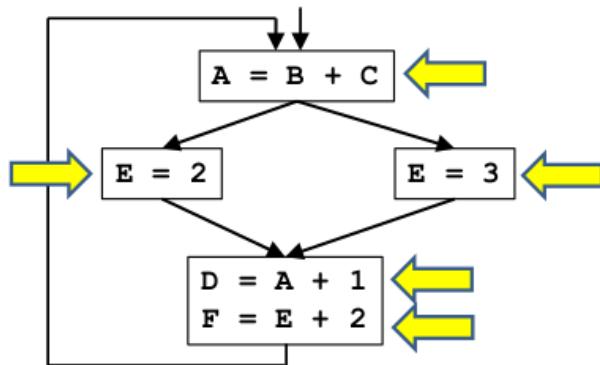


Figure 41: For this CFG, $A = B+C$, $E = 2$, $E = 3$, $D = A + 1$ are Loop-Invariant Computation, but $F = E + 2$ is not because two definitions of E reach $F = E + 2$.

10.7 Conditions for Code Motion

Algorithm 11 Code Motion Algorithm

Given: a set of nodes in a loop
Compute reaching definitions
Compute loop invariant computation
Compute dominators
Find the exits of the loop (i.e. nodes with successor outside loop)
Candidate statement for code motion:
loop invariant
in blocks that dominate all the exits of the loop shown in 42
assign to variable not assigned to elsewhere in the loop
in blocks that dominate all blocks in the loop that use the variable assigned shown in 43
Perform a depth-first search of the blocks
Move candidate to preheader if all the invariant operations it depends upon have been moved

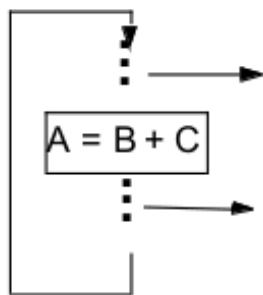


Figure 42: It is not safe to move $A = B + C$ outside the loop because we can jump out of the loop before executing $A = B + C$

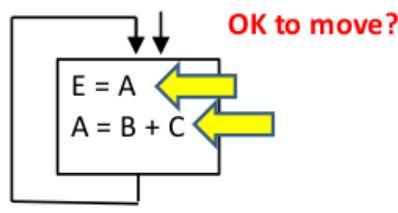


Figure 43: It is not safe to move $A = B + C$ outside the loop because if so, the first time we enter the loop $E = A$ will not be the same as before.

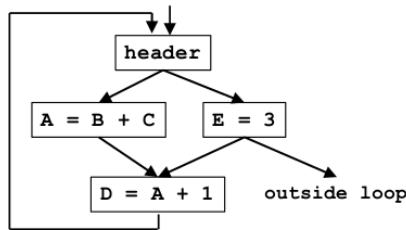


Figure 44: Only $E = 3$ can be moved outside the loop.

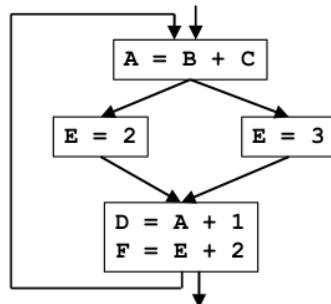


Figure 45: Only $A = B + C$, $D = A + 1$ can be moved outside the loop.

10.8 More Aggressive Optimizations

10.8.1 Gamble on: most loops get executed

We can relax constraint of dominating all exits on some cases.

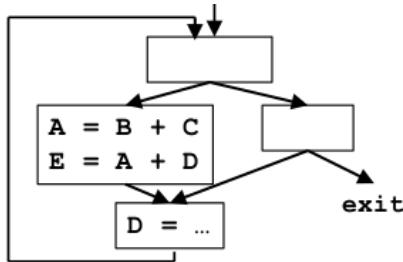


Figure 46: $A = B + C$ cannot be removed outside the loop because it doesn't dominate the exit. But if A is not live after the loop, we can actually move it to the preheader. The only thing we need to consider is that this statement can cause an exception.

10.8.2 Landing pads

`while` loop is not very convenient for optimization since it checks before entering the loop. We can use landing pads to solve this.

```
While p do loop-body    →    if p {  
                                preheader  
                                repeat  
                                    loop-body  
                                until not p;  
                            }
```

Figure 47: Transforms for while loops.

11 Induction Variables and Strength Reduction

Strength reduction is an optimization technique which substitutes expensive operations with computationally cheaper ones. For example, a very weak strength reduction algorithm can substitute the instruction $b = a * 4$ with $b = a \ll 2$.

11.1 Motivation

Opportunities for strength reduction arise routinely from details that the compiler inserts to implement source-level abstractions. To see this, consider the simple code fragment shown in Figure 74. Figure 48a shows source code and the same loop in a low-level intermediate code. Notice the instruction sequence that begins at the label L2. The compiler inserted this code (with its multiply) as the expansion of $A[i]$. Figure 48b shows the code that results from applying Strength Reduction, Figure 48c is followed by dead-code elimination. The compiler created a new variable, $t2'$, to hold the value of the expression $i * 4 + A$. Its value is computed directly, by incrementing it with the constant 4, rather than recomputing it on each iteration as a function of i . Strength reduction automates this transformation.

```

        i = 0
L2: IF i>=100 GOTO L1
for(i=0; i<100; i++)
    A[i] = 0;
        t1 = 4 * i
        t2 = &A + t1
        *t2 = 0
        i = i+1
        GOTO L2
L1:

```

(a) Origianl code.

```

t1' = 0
t2' = &A
L2: IF t1'>=400 GOTO L1
    t1 = t1'
    t2 = t2'
    *t2 = 0
    t1' = t1'+4
    t2' = t2'+4
    GOTO L2
L1:

```

(b) After induction variable substitute.

```

t2' = &A
t3' = &A + 400
L2: IF t2'>t3' GOTO L1 *t2'= 0
    t2' = t2'+ 4
    GOTO L2
L1:

```

56
(c) Final code.

Figure 48: An example of strength reduction.

11.2 Definitions

Basic Induction Variable

A basic induction variable (e.g., i as shown in Figure 48a) is a variable X whose only definitions within the loop are assignments of the form: $X = X + c$ or $X = X - c$, where c is either a constant or a loop-invariant variable.

Induction Variable

An induction variable is either a basic induction variable B , or a variable defined once within the loop (e.g., $t1, t2$ as shown in Figure 48a), whose value is a linear function of some basic induction variable at the time of the definition: $A = c_1 * B + c_2$

The FAMILY of a basic induction variable B is the set of induction variables A such that each time A is assigned in the loop, the value of A is a linear function of B . (e.g., $t1, t2$ is in family of i as shown in Figure 48a)

11.3 Optimizations

11.3.1 Strength Reduction

Algorithm 12 Strength Reduction Optimizations

A is an induction variable in family of basic induction variable B (i.e., $A = c_1 * B + c_2$)

Create new variable A'

Initialize in preheader $A' = c_1 * B + c_2$

Track value of B : add after $B = B + x$: $A' = A' + x * c_1$

Replace assignment to A : replace lone $A = \dots$ with $A = A'$

11.3.2 Optimizing non-basic induction variables

- copy propagation

- dead code elimination

11.3.3 Optimizing basic induction variables

Eliminate basic induction variables used only for calculating other induction variables and loop tests.

Algorithm 13 Optimizing basic induction variables

Select an induction variable A in the family of B , preferably with simple constants ($A = c_1 * B + c_2$).

Replace a comparison such as `if B > X goto L1` with `if (A' > c1 * X + c2) goto L1` (assuming c_1 is positive)

if B is live at any exit from the loop, recompute it from A' . After the exit, $B = (A' - c_2)/c_1$

11.4 Further Details

```

k = 0;
for (i = 0; i < n; i++){
    k = k+3 ;
    ... = m;
    if(x<y)
        k = k+4
    if(a < b)
        m = 2 * k;
    k = k - 2;
    ... = m;
}

```

- (a) A more complex example. k and i are both basic induction variables.
 m is in the family of k .

```

k = 0;
m' = 0;
for (i = 0; i < n; i++){
    k = k+3 ;
    m' = m'+6;
    ... = m;
    if(x<y)
        k = k+4
        m' = m'+8;
    if(a < b)
        m = m' ;
    k = k - 2;
    m' = m'-4;
    ... = m;
}

```

- (b) After induction variable substitute.

Figure 49: A more complex example of strength reduction.

11.5 Finding Induction Variable Families

Let B be a basic induction variable, A is in the family of B if it satisfies one the following conditions

- **Condition C1** A has a single assignment in the loop L of the form $A = B*c$, $c*B$, $B+c$, etc
- **Condition C2** A is in family of B if $D = c_1 * B + c_2$ for basic induction variable B and:
 - Rule 1: A has a single assignment in the loop L of the form $A = D*c$, $D+c$, etc
 - Rule 2: No definition of D outside L reaches the assignment to A
 - Rule 3: Every path between the lone point of assignment to D in L and the assignment to A has the same sequence (possibly empty) of definitions of B

```

L2: IF i>=100 GOTO L1
    t2 = t1 + 10
    t1 = 4 * i
    t3 = t1 * 8
    i = i + 1
    goto L2
L1:

```

Figure 50: i is a basic induction variable, t1 t2 are in family of i, but t2 is not because it violates the condition C2 rule 2.

```

L3: IF i>=100 GOTO L1
    t1 = 4 * i
    IF t1 < 50 GOTO L2
    i = i + 2
L2: t2 = t1 + 10
    i = i + 1
    goto L3
L1:

```

Figure 51: i is a basic induction variable, t1 is in the family of i. t2 is not because it violates the Condition2 rule3(some path reaches t2 includes $i = i+1$ but some not.).

12 Partial Redundancy Elimination

Partial redundancy elimination (PRE) is a global optimization introduced by Morel and Renvoise[1]. It combines and extends two other techniques: common subexpression elimination and loop-invariant code motion.

An expression is partially redundant at point p if it is redundant along some, but not all, paths that reach p. PRE converts partially-redundant expressions into redundant expressions. The basic idea is simple. First, it uses data-flow analysis to discover where expressions are partially redundant. Next, it solves a data-flow problem that shows where inserting copies of a computation would convert a partial redundancy into a full redundancy. Finally, it inserts the appropriate code and deletes the redundant copy of the expression.

A key feature of PRE is that it never lengthens an execution path. To see this more clearly, consider the example shown in Figure 52. In the fragment on the left, the second computation of $x + y$ is partially redundant; it is only available along one path from the if. Inserting an evaluation of $x + y$ on the other path makes the computation redundant and allows it to be eliminated, as shown in the right-hand fragment. Note that the left path stays the same length while the right path has been shortened.

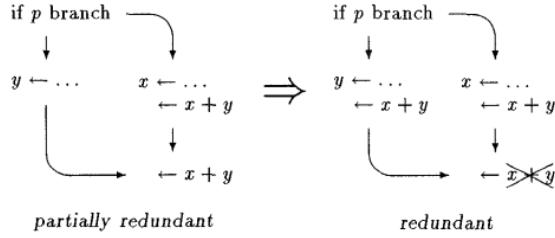


Figure 52

Loop-invariant expressions are also partially redundant, as shown in Figure 53. On the left, $x + y$ is partially redundant since it is available from one predecessor (along the back edge of the loop), but not the other. Inserting an evaluation of $x + y$ before the loop allows it to be eliminated from the loop body.

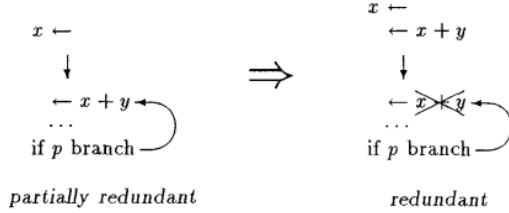


Figure 53

12.1 Finding Partially Available Expressions

For every expression, we can do a dataflow analysis.

Direction	Forward
Meet operator	\cup
Lattice	$\{0, 1\}$
Top(T)	0
Bottom	1
Boundary condition for entry node	0
Initialization for internal nodes	T
Finitied ascending chain?	✓
Transferfunction	$PAVOUT[i] = (PAVIN[i] - KILL[i]) \cup AVLOC[i]$
Monotone&Distributive?	✓
AVLOC	Expression is locally available (AVLOC) if downwards exposed.
KILL	Expression is killed (KILL) if any assignments to operands.

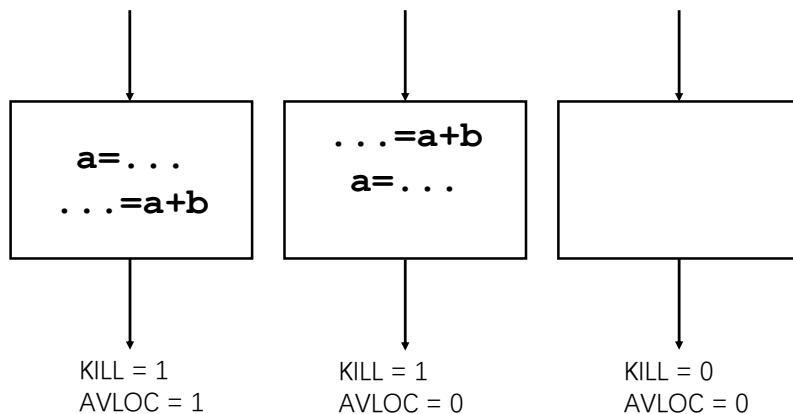


Figure 54: For $a+b$, the result of Partially Available Expressions's transfer function within a basic block.

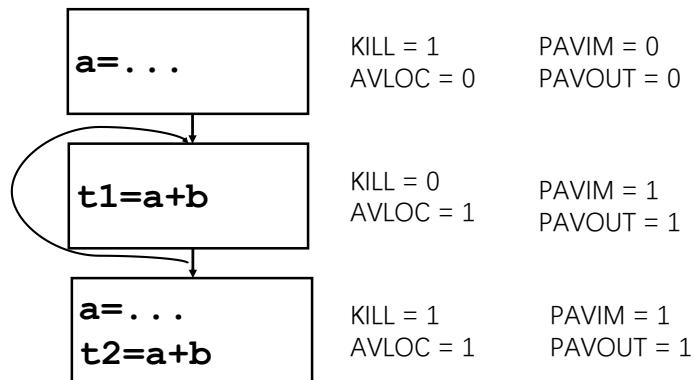


Figure 55: For $a+b$, the result Partially Available Expressions of dataflow analysis.

12.2 Finding Anticipated Expression

For PRE, care must be taken that the hoisting would do no harm: Never introduce a new expression along any path. Otherwise the hoisting will lengthen at least one trace of the program, defying optimality; even worse, if the hoisted instruction throws an exception, the program's semantics change.

Local Anticipability(ANTLOC)

An expression may be locally anticipated in a block i if there is at least one computation of the expression in the block i , and if the commands appearing in the block before the first computation of the expression do not modify its operands.

Direction	backward
Meet operator	\cap
Lattice	$\{0, 1\}$
Top(T)	1
Boundary condition for exit node	0
Initialization for internal nodes	T
Finitized ascending chain?	✓
Transferfunction	$ANTIN[i] = ANTLOC[i] \cup (ANTOUT[i] - KILL[i])$
Monotone&Distributive?	✓
ANTLOC	Expression is locally anticipated(ANTLOC) is upward exposed.

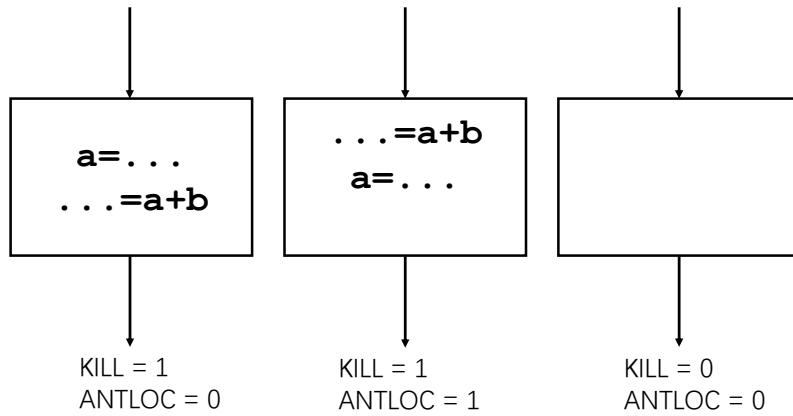


Figure 56: For $a+b$, the result of Anticipated Expression's transfer function within a basic block.

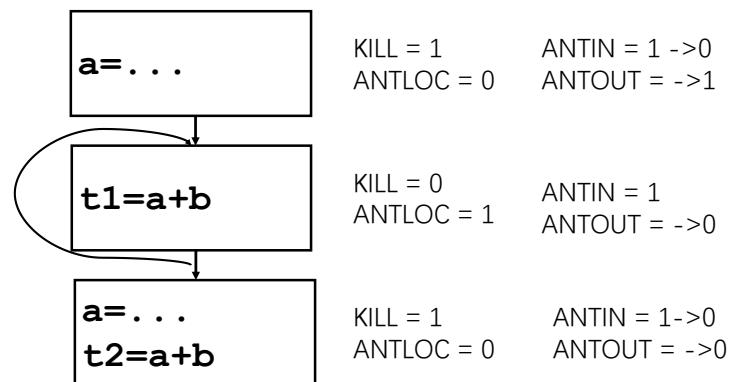


Figure 57: For $a+b$, the result Anticipated Expression of dataflow analysis.

12.3 Where Do we Want to Insert Computations?

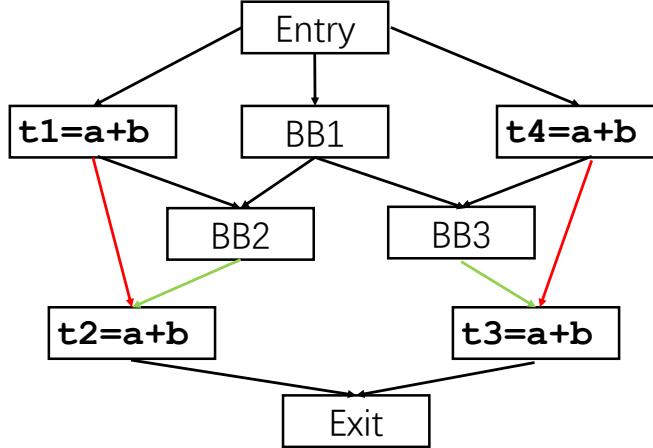


Figure 58: For $a+b$, $t_2 = a + b$ and $t_3 = a + 4$ are both partially redundant. But where can we insert the new computation $a + b$ in order to optimally eliminate redundancy? The best choice is BB1 because this will make $a + b$ fully redundant. But if we insert to BB2 and BB3, there are some path that calculate $a + b$ more than once (e.g. Entry → $t_1 = a+b$ → BB2 → $t_2 = a+b$)

We define "**Placement Possible**"(PP) dataflow analysis. First of all, we are only going to place computations at the end of the blocks. We want to insert the computation at the earliest place where our **Placement Possible** is true. If the **Placement Possible** is true output of a block(PPOUT), it means it is fine to insert at the end of this block or earlier. If it is true at the beginning of the block, it means we could insert it at the beginning of the block or earlier. Because we want to insert it at the end of the block, so if **Placement Possible** is true at the beginning of the block(PPIN), you won't insert it in the block, it means you need to take care of something before. So when PPIN is true, it really means is for every predecessor block, it is either possible to keep moving it back and make it fully redundant by placing in that block or earlier or it is not necessary because it is already generated in one of those blocks.

We insert if PPOUT is true and either PPIN is false so we cannot move it back any further or if we locally kill it then clearly we have to insert it here because trying to insert it earlier would not work. And we only want to insert it if it is not already available.

We want to delete an expression where PPIN is true (somehow we make it fully redundant) and it is anticipated locally.

For safety reasons, if we want to place at output of a block, we want to place at entry of all successors. (PPOUT)

$$PPOUT[i] = \begin{cases} 0 & i = \text{entry} \\ \bigcap_{s \in \text{succ}(i)} PPIN[s] & \text{otherwise} \end{cases}$$

When PPIN is true, it means

- we have a local computation to place, or a placement at the end of this block which we can move up
- we want to move computation to output of all predecessors where expression is not already available (don't insert at input) (for every predecessor,)
- we gain something by moving it up (PAVIN heuristic) (not too far)

$$PPIN[i] = \begin{cases} 0 & i = \text{exit} \\ \left(\left[\text{ANTLOC}[i] \cup (PPOUT[i] - KILL[i]) \right] \cap \bigcap_{p \in \text{preds}(i)} (\text{PPOUT}[p] \cup \text{AVOUT}[p]) \cap \text{PAVIN}[i] \right) & \text{otherwise} \end{cases}$$

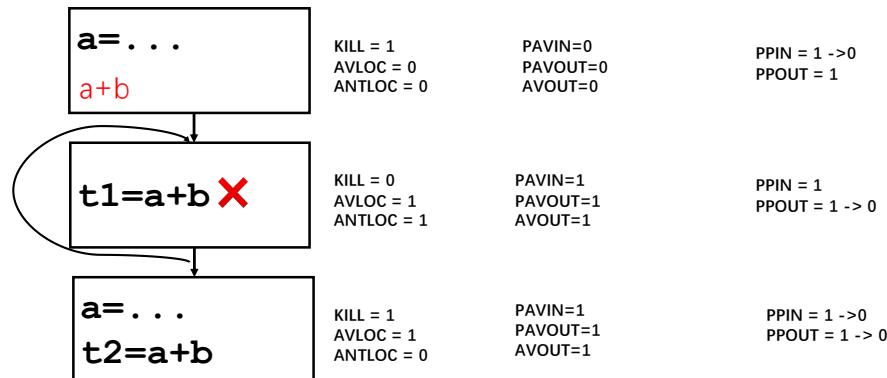


Figure 59: Example for PRE for $a+b$

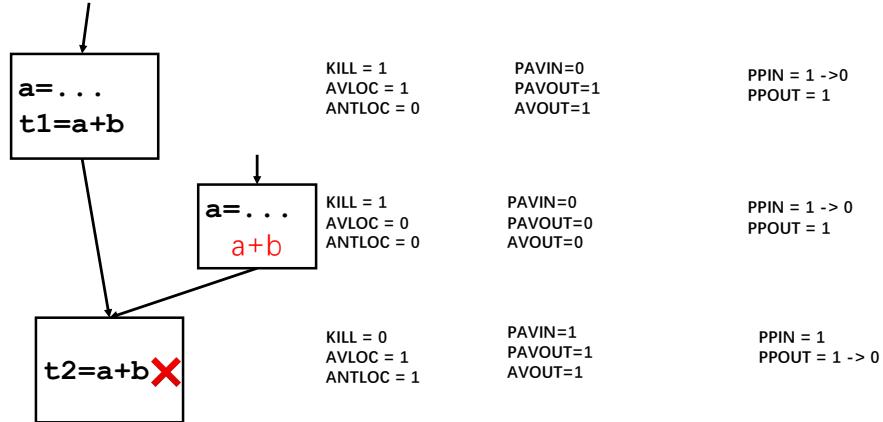


Figure 60: Example for PRE for $a+b$

12.3.1 Safety

It is safe to insert only if anticipated.

$$PPIN[i] \subseteq (PPOUT[i] - KILL[i]) \cup \text{ANTLOC}[i]$$

$$PPOUT[i] = \begin{cases} 0 & i = \text{entry} \\ \bigcap_{s \in \text{succ}(i)} PPIN[s] & \text{otherwise} \end{cases}$$

$$\text{INSERT} \subseteq PPOUT \subseteq \text{ANTOUT}$$

So it is safe.

12.4 Perform

On every path from an INSERT, there is a DELETE.

12.5 Limitations

12.6 A new way to think about partial redundancy

13 Lazy Code Motion

In 1979, Morel and Renvoise came up with an exciting new technique, the suppression of partial redundancies [1]. Their technique uniformly subsumed loop invariant code motion, common subexpression elimination, and the elimination of redundant computations. Probably, the most appealing facet of their technique was its structural purity: the transformation was solely based on data-flow analysis and did not require any specific knowledge on the control flow of the programs under investigation. On the other hand, their genuine proposal was conceptually complex. It involved an equation system of four highly interacting global properties while still suffering from three deficiencies. First, too few partial redundancies are removed. Intuitively, this was due to Morel’s and Renvoise’s design decision to insert code at the nodes of the underlying flow graph rather than at its edges, which unnecessarily restricted the possible computation points. Second, code was moved too far, which led to unnecessary register pressure. And third, the node placement was based on bidirectional data-flow equations which — from a conceptual point of view — are difficult to comprehend and — from a computational point of view — are more costly to compute.

As we started our work on lazy code motion, we were convinced that research efforts based on modifying the Morel/- Renvoise-style equations had led into a dead end. Partial redundancy elimination (PRE) is a beautiful technique with a simple underlying basic idea: expressions are hoisted to earlier program points increasing thereby their potential to make the original ones fully redundant, which can then be eliminated. We had the strong belief that it must be possible to construct a PRE-technique which is solely composed out of simple and well-understood components.

Decomposing the problem. A key idea to attack the problem was its **decomposition** based on a clean separation of concerns. We noticed that there are two optimization goals with a natural hierarchy: the primary is to reduce the number of computations to a minimum (computational optimality); the secondary to avoid unnecessary code movement to **minimize the lifetimes of temporaries and hence the register pressure (lifetime optimality)**. There is no a topological order for the bidirectional dataflow analysis, so this does complicate things.

Solving the problem. Fortunately, we already had an offthe-shelf solution for the first optimization goal. Investigating the relationship between model checking and data-flow analysis has led to a modal logic specification of a computationally optimal PRE following an as-early-as-possible code placement strategy [2]. We called the resulting transformation “Busy Code Motion (BCM),” as it hoists code as far as possible. Technically it required only two simple unidirectional data-flow analyses. This simplicity revealed the solution to our secondary goal, the avoidance of unnecessary code motion: the code only had to “sink back” from the BCM insertion points as far as computational optimality was preserved, which can be realized simply by adding another unidirectional data-flow analysis. The resulting transformation, which **solves the problem of unnecessary register pressure**, hoists code just far enough to ensure computationally optimal results, the reason for it being called “Lazy Code Motion (LCM).”

This successful way of playing with simple analysis components was later extended to also control/minimize code size [3]. Here, the natural trade-off between the optimization goals led to different solutions depending on the chosen priority between size and speed.

13.1 Big Picture

First calculates the “earliest” set of blocks for insertion, this maximizes redundancy elimination but may also result in long register lifetimes. Then it calculates the “latest” set of blocks for

insertion, this achieves the same amount of redundancy elimination as “earliest” but hopefully reduces register lifetimes.[4, 5]

13.2 PRE vs. LCM

The goal of PRE is that by **moving around** the places where an expression is evaluated and keeping the result in a temporary variable when necessary, we often can **reduce the number of evaluations** of this expression along many of the execution paths, **while not increasing that number along any path**. However, it is **not** possible to eliminate all redundant computations along every path, unless we are allowed to **change the control flow graph** by **creating new blocks** and **duplicating blocks**.

New blocks creation

It can be used to break “**critical edge**”, which is an edge leading from a node with more than one successor to a node with more than one predecessor.

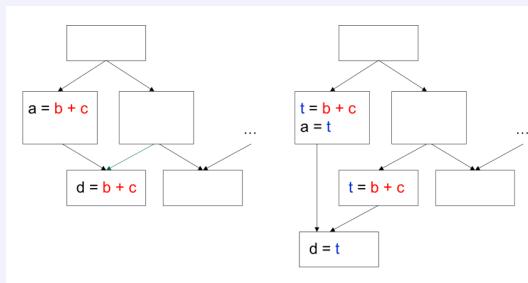


Figure 61: Example of new block creation

Block duplication

It can be used to isolate the path where redundancy is found.

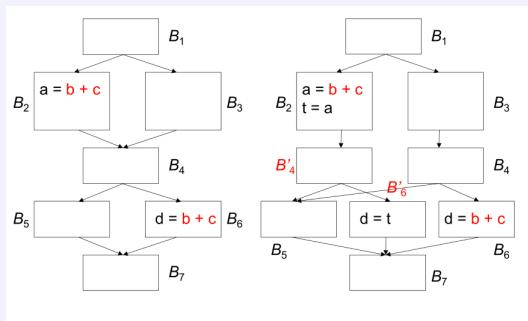


Figure 62: Example of block duplication

13.3 Preprocessing: Preparing the Flow Graph

First, we need to modify the flow graph. In order to ensure redundancy elimination power, we add a basic block for every edge that leads to a basic block with multiple predecessors. Also, in LCM, we restrict placement of instructions to the beginning of a basic block. Consider each statement as its own basic block to keep algorithm simple.

Full Redundancy: A Cut Set in a Graph

Full redundancy at p: expression $a+b$ redundant on all paths

- a cut set: nodes that separate entry from p (could have multiple cut sets).
- each node in a cut set contains a calculation of $a+b$.
- a, b not redefined.

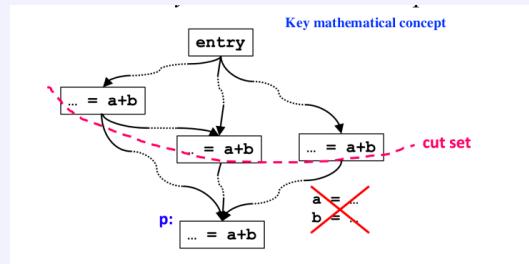


Figure 63: Full Redundancy

Partial Redundancy: Completing a Cut Set

Partial redundancy at p: redundant on some but not all paths

- Add operations to create a cut set containing $a+b$
- Note: Moving operations up can eliminate redundancy

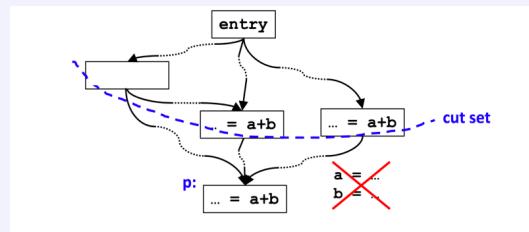


Figure 64: Partial Redundancy

13.4 Pass 1: Anticipated Expression

Direction	Backword
Domain	Set of expressions
Meet operator	\cap
Boundary	$IN[EXIT] = \phi$
Initialization for internal nodes	$IN[B] = \{all\ expressions\}$
Finitized ascending chain?	✓
Transferfunction	$f_b(x) = EUse_b \cup (x - EKill_b)$
Monotone&Distributive?	✓
$EUse_b$	set of expressions computed in B (EUuse, UEEEXP).
$EKill_b$	set of expressions any of whose operands are defined in B

13.5 Where to insert/move instructions?

13.5.1 Choice 1 : frontier of anticipation

What is the result if we insert $t = a + b$ at the frontier of anticipation ? i.e., those BBs for which $a + b$ is anticipated to the entry of BB, but not anticipated to the entry of its parents.?

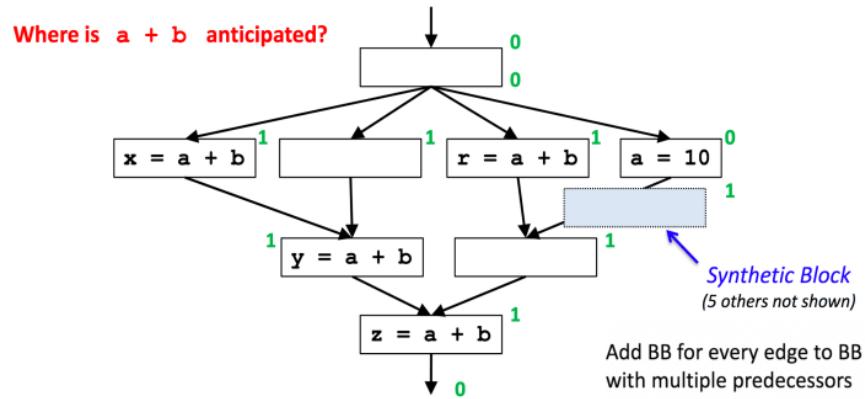


Figure 65: Frontier may be good for this example.

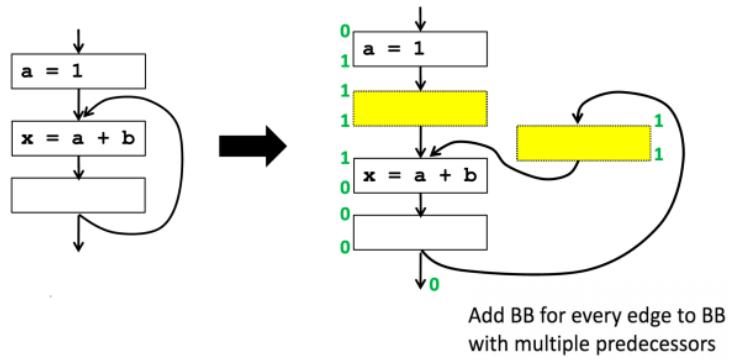


Figure 66: Frontier are colored in yellow. Frontier of anticipation may be not a good choice. For this example, if we insert $t = a + b$ at the frontier of anticipation, this doesn't eliminate redundancy within loop!

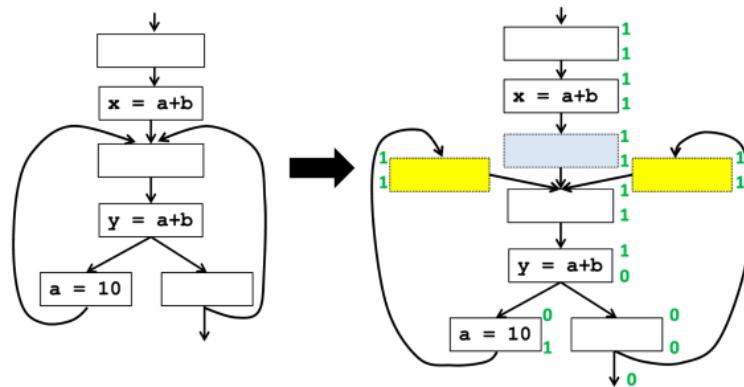


Figure 67: This example can also illustrate frontier is not our choice. In fact, we ideally like to insert " $a+b$ " in this case to the left BB.

How to find such anticipated frontier and exclude “those not needed blocks” discussed in previous loop examples? Our final solution: Place expression at “anticipated” but not “will be available” blocks

13.6 Pass 2: Place As Early As Possible

Name	Available Expressions
Direction	Forward
Transferfunction	$f_b(x) = (\text{Anticipated}[b].in \cup x) - EKill_b$
Domain	Set of expressions
Meet operator	\cap
Boundary	$OUT[Entry] = \phi$
Initialization for internal nodes	$OUT[B] = \{\text{all expressions}\}$

$$\text{earliest}[b] = \text{anticipated}[b] - \text{available}[b]$$

13.7 Pass 3: Lazy Code Motion

The values of expressions found to be redundant are usually held in registers until they are used. Computing a value as late as possible minimizes its lifetime: the duration between the time the value is defined and the time it is last used. Minimizing the lifetime of a value in turn minimizes the usage of a register.

postponable

An expression e is postponable at a program point p if

- all paths leading to p have seen earliest placement of e
- but not a subsequent use

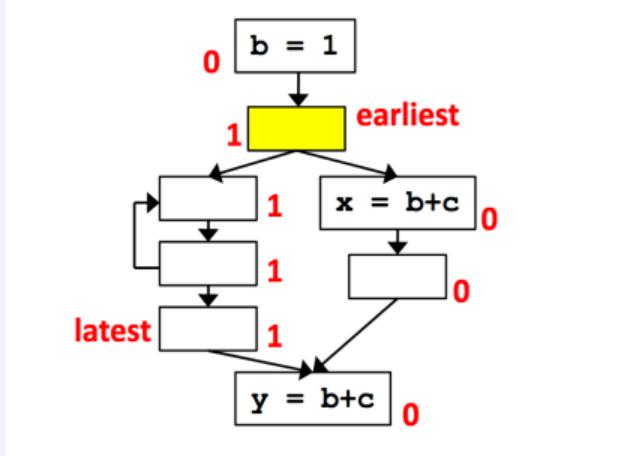


Figure 68: An example to illustrate Postponable Expressions.

Name	Postponable Expressions
Direction	Forward
Transferfunction	$f_b(x) = (\text{earliest}[b] \cap x) - \text{EUse}_b$
Domain	Set of expressions
Meet operator	\cap
Boundary	$\text{OUT}[\text{Entry}] = \phi$
Initialization for internal nodes	$\text{OUT}[B] = \{\text{all expressions}\}$

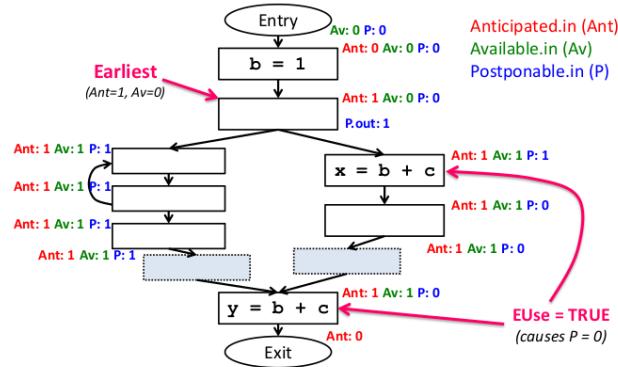


Figure 69: An example to illustrate Postponable.

```

latest[b] = (earliest[b] ∪ postponable.in[b]) ∩
(EUuseb ∪ ¬(∩s ∈ succ[b](earliest[s] ∪ postponable.in[s])))
• OK to place expression: earliest or postponable
• Need to place at b if either
  – used in b, or
  – not OK to place in one of its successors

```

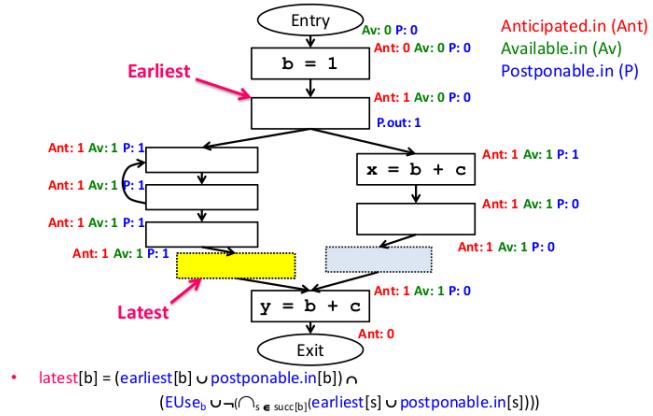


Figure 70: An example to illustrate “Latest”.

13.8 Pass 4: Cleaning Up

Name	Used Expressions
Direction	Backward
Transferfunction	$f_b(x) = (\text{EUse}[b] \cap x) - \text{latest}[b]$
Domain	Set of expressions
Meet operator	\cup
Boundary	$\text{in}[\text{exit}] = \phi$
Initialization for internal nodes	$\text{in}[b] = \phi$

For all basic blocks b , if $(x+y) \in (\text{latest}[b] \cap \text{used.out}[b])$, at beginning of b : add new $t = x+y$, then replace every original $x+y$ by t .

14 A Variation of Knoop, Ruthing, and Steffen's Lazy Code Motion

14.1 Where to Insert?

We want to insert the new computation where it is not partially available there.

Anticipable(Very Busy) Expression

An expression e is anticipable at a program point p if e will be computed along every path from p to p_{end} , and no variable in e is redefined until its computation. It is safe to move an expression to a basic block where that expression is anticipable. By "safe" we mean "performance safe", i.e., no extra computation will be performed. Notice that if an expression e is computed at a basic block where it is both available and anticipable, then that computation is clearly redundant.

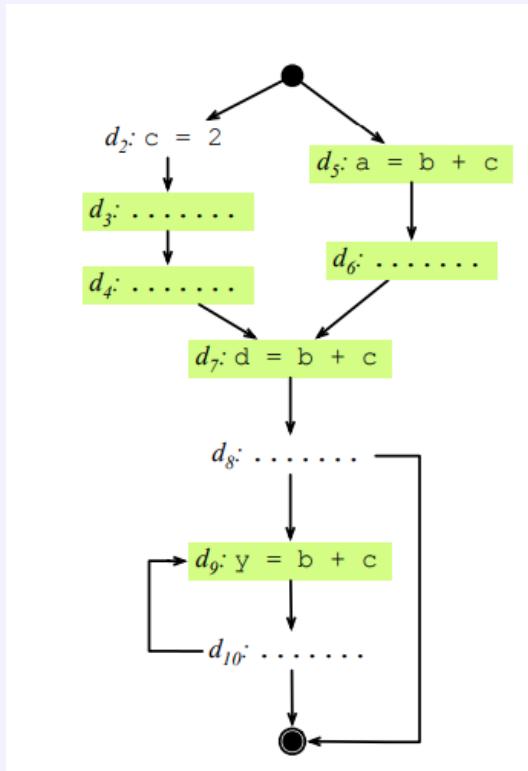


Figure 71: For $b+c$, the green blocks are anticipable points.

The key to partial redundancy elimination is deciding where to add computations of an expression to change partial redundancies into full redundancies (which may then be optimized away). There are now two steps that we must perform:

- First, we find the earliest places in which we can move the computation of an expression without adding unnecessary computations to the CFG. This step is like pushing the computation of the expressions up.
- Second, we try to move these computations down, closer to the places where they are necessary, without adding redundancies to the CFG. This phase is like pulling these computations down the CFG. So that we can, for instance, reduce register pressure.

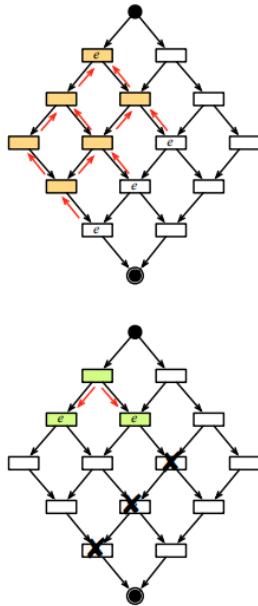


Figure 72: Pushing up, Pulling down.

14.1.1 Earliest Placement

We must now find the earliest possible places where we can compute the target expressions. Earliest in the sense that p_1 comes before p_2 if p_1 precedes p_2 in any topological ordering of the CFG.

$$\text{EARLIEST}(i, j) = \text{IN}_{\text{ANTICIPABLE}}(j) \cap \overline{\text{OUT}_{\text{AVAILABLE}}(i)} \cap (\text{KILL}(i) \cup \overline{\text{OUT}_{\text{ANTICIPABLE}}(i)})$$

For the **Fisrt** part, We can move an expression e to an edge ij only if e is anticipable at the entrance of j . If the expression is available at the beginning of the edge, then we should not move it there. But the **Second** part, If an expression is anticipable at i , then we should not move it to ij , because we can move it to before i . On the other hand, if i kills the expression, then it cannot be computed before i .

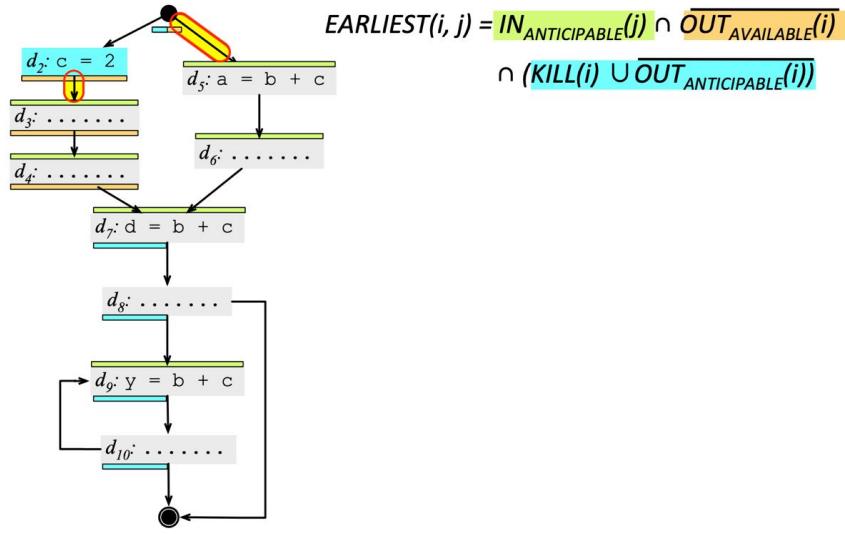


Figure 73: An example for calculating EARLIEST.

14.1.2 Latest Placement

$$\begin{aligned} \text{IN}_{\text{LATER}}(j) &= \cap_{i \in \text{pred}(j)} \text{LATER}(i, j) \\ \text{LATER}(i, j) &= \text{EARLIEST}(i, j) \cup \left(\text{IN}_{\text{LATER}}(i) \cap \overline{\text{EXPR}(i)} \right). \end{aligned}$$

$\text{LATER}(i, j)$ is true if we can move the computation of the expression down the edge ij . An expression e is in $\text{EXPR}(i)$ if e is computed at i . This predicate is also computed for edges, although we have IN_{LATER} being computed for nodes.

For $\text{LATER}(i, j)$: If $\text{EARLIEST}(i, j)$ is true, then $\text{LATER}(i, j)$ is also true, as we can move the computation of e to edge ij without causing redundant computations. If $\text{IN}_{\text{LATER}}(i, j)$ is true, and the expression is not used at i , then $\text{LATER}(i, j)$ is true. If the expression is used at i , then there is no point in computing it at ij , because it will be recomputed at i anyway.

For $\text{IN}_{\text{LATER}}(i, j)$, it is a condition that we propagate down. If all the predecessors of a node j accept the expression as nonredundant, then we can compute the expression down on j .

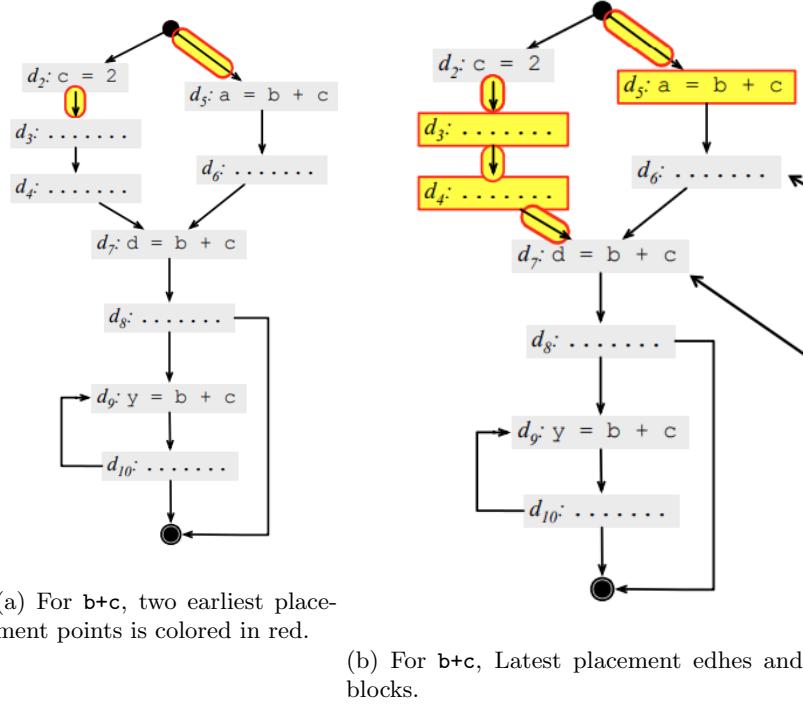


Figure 74: A more complex example of strength reduction.

14.1.3 Where to Insert Computations?

We insert the new computations at the latest possible place. That is

$$INSERT(i, j) = LATER(i, j) \cap \overline{IN_{LATER}(j)}$$

There are different insertion points, depending on the structure of the CFG, if $x \in INSERT(i, j)$:

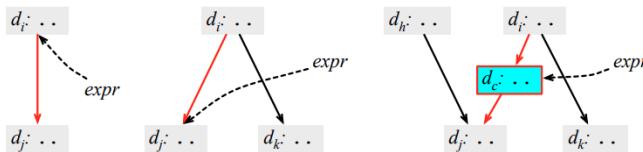


Figure 75: Different insertion points

14.2 Modify CFG

Rename all computation of the expression.

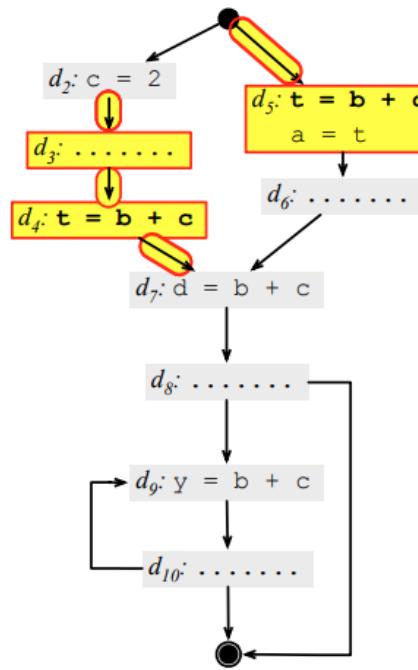


Figure 76: For $b+c$, the result of applying modifying CFG.

14.3 Which Computations to Remove?

We remove computations that are already covered by the latest points, and that we cannot use later on.

$$DELETE(i) = \text{EXPR}(i) \cap \text{IN}_{\text{LATER}}(i)$$

For **First** part, of course, the expression must be used in the block, otherwise we would have nothing to delete. For **second** part, The expression may not be a computation that is necessary later on.

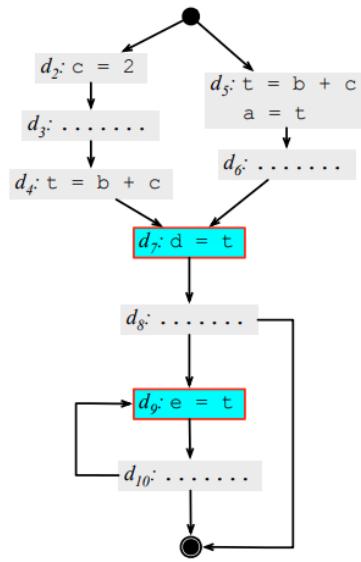


Figure 77: For $b+c$, the result of applying redundancy $b+c$

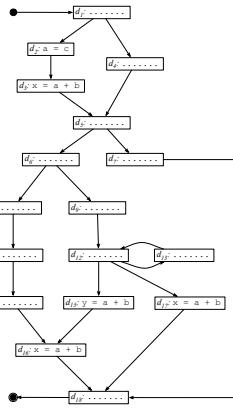
14.4 A fully explained example



An Example to Conquer them All

- The original formulation of Lazy Code Motion was published in a paper by Knoop *et al.*¹⁰.
 - The authors used a complex example to illustrate all the phases of their algorithm.
 - Many papers are build around examples.
 - That is a good strategy to convey ideas to readers.

◊: Lazy Code Motion, PLDI (1992)

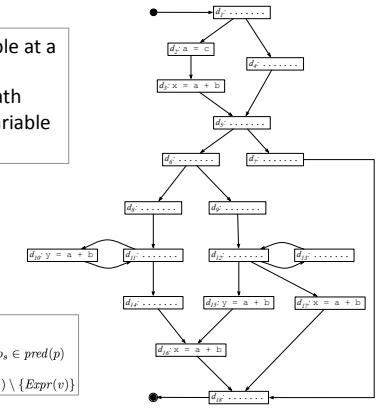


Available Expressions

An expression e is available at a program point p if e is computed along every path from p_{start} to p , and no variable in e is redefined until p .

What is the OUT set of available expressions in the example?

$$\begin{aligned} IN(p) &= \cap OUT(p_s), p_s \in pred(p) \\ OUT(p) &= (IN(p) \cup \{E\}) \setminus \{Expr(v)\} \end{aligned}$$

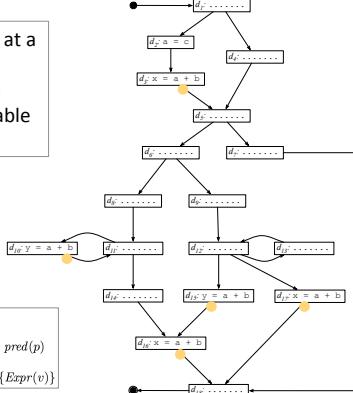


Available Expressions

An expression e is available at a program point p if e is computed along every path from p_{start} to p , and no variable in e is redefined until p .

$n; v \equiv E$

$$\begin{aligned} IN(p) &= \bigcap OUT(p_s), p_s \in pred(p) \\ OUT(p) &= (IN(p) \cup \{E\}) \setminus \{Expr(v)\} \end{aligned}$$

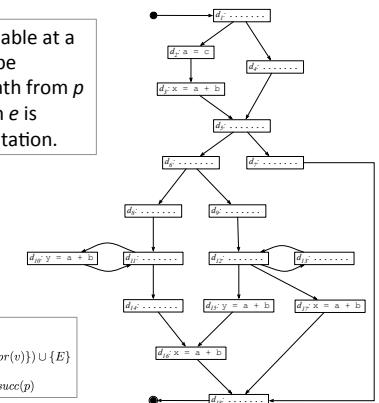


Anticipable Expressions

An expression e is anticipable at a program point p if e will be computed along every path from p to p_{end} , and no variable in e is redefined until its computation.

What is the IN set of anticipable expressions in the example?

$$\begin{aligned} p : v = E \\ IN(p) &= (OUT(p) \setminus \{Expr(v)\}) \cup \{E\} \\ OUT(p) &= \bigcap_{v \in p} IN(p_v), p_v \in succ(p) \end{aligned}$$



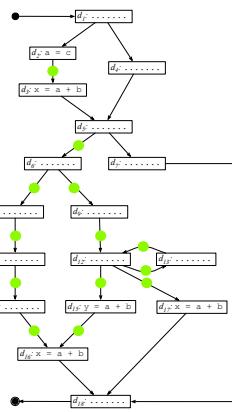
Anticipable Expressions

An expression e is anticipable at a program point p if e will be computed along every path from p to p_{end} , and no variable in e is redefined until its computation.

What is the IN set of anticipable expressions in the example?

$p : v = E$

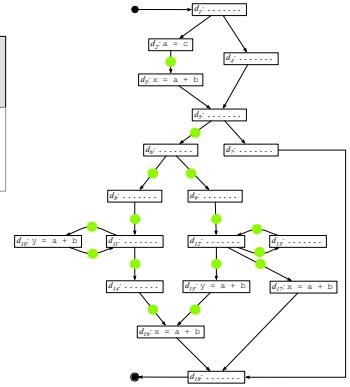
$$\begin{aligned} IN(p) &= (OUT(p) \setminus \{Expr(v)\}) \cup \{E\} \\ OUT(p) &= \cap IN(p_s), p_s \in succ(p) \end{aligned}$$



$$EARLIEST(i, j) = IN_{ANTICIPABLE}(j) \cap OUT_{AVAILABLE}(i) \cap (KILL(i) \cup OUT_{ANTICIPABLE}(i))$$

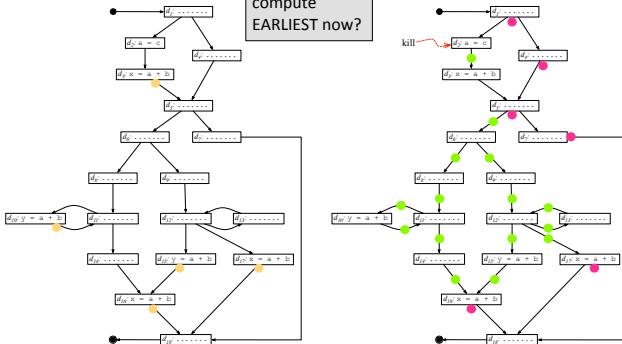
What is $KILL(i) \cup OUT_{ANTICIPABLE}(i)$ in our running example?

This figure shows the IN sets of anticipability analysis.



$$EARLIEST(i, j) = IN_{ANTICIPABLE}(j) \cap OUT_{AVAILABLE}(i) \cap (KILL(i) \cup OUT_{ANTICIPABLE}(i))$$

Can you compute EARLIEST now?



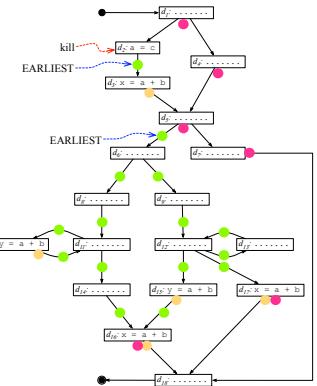
$$EARLIEST(i, j) = IN_{ANTICIPABLE}(j) \cap OUT_{AVAILABLE}(i) \cap (KILL(i) \cup OUT_{ANTICIPABLE}(i))$$

We have two EARLIEST edges in this CFG.

● Anticipable at IN(j)

● Not anticipable at OUT(i)

● Available at OUT(i)

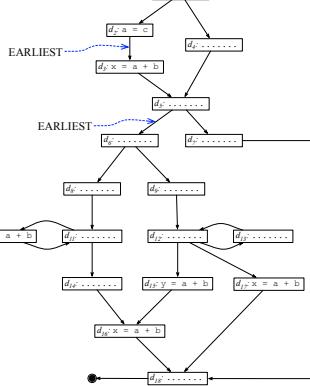


Latest

$$IN_{LATER}(j) = \cap_{i \in pred(j)} LATER(i, j)$$

$$LATER(i, j) = EARLIEST(i, j) \cup (IN_{LATER}(i) \cap EXPR(i))$$

The goal now is to compute the latest IN sets, and the latest edges. Can you do it?



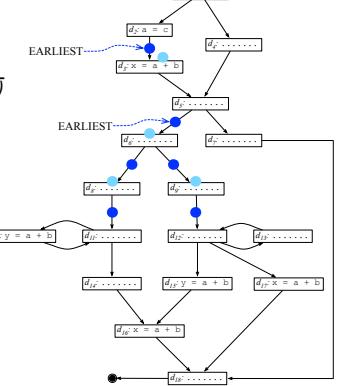
Latest

$$IN_{LATER}(j) = \cap_{i \in pred(j)} LATER(i, j)$$

$$LATER(i, j) = EARLIEST(i, j) \cup (IN_{LATER}(i) \cap EXPR(i))$$

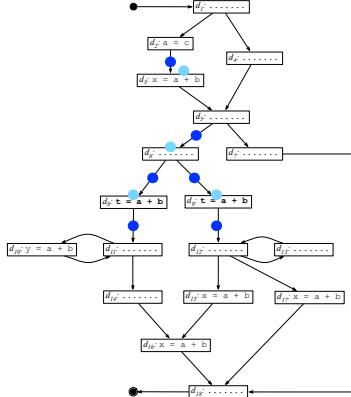
The LATEST edges are marked with the dark blue circles.

The LATEST IN sets are marked with the light blue circles.



$$INSERT(i, j) = LATER(i, j) \cap \overline{IN_{LATER}(j)}$$

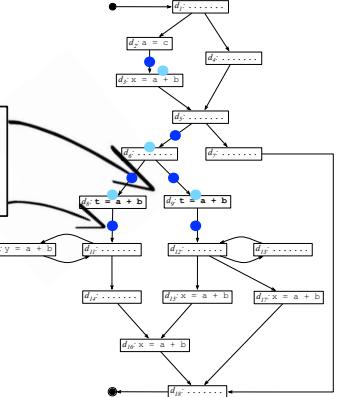
We must now find the sites where we can insert new computations of $a + b$. Can you compute $INSERT(i, j)$?



$$INSERT(i, j) = LATER(i, j) \cap \overline{IN_{LATER}(j)}$$

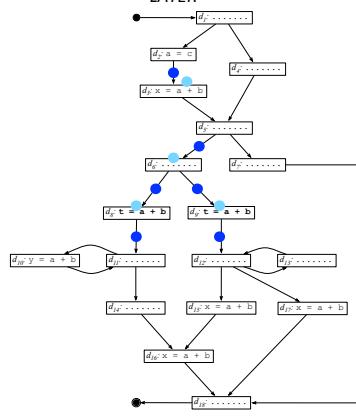
In this example, we only have two sites to insert new computations.

Do you remember why we insert the computation of $a + b$ at d_8 , instead of d_{11} ?



$$DELETE(i) = EXPR(i) \cap \overline{IN_{LATER}(i)}$$

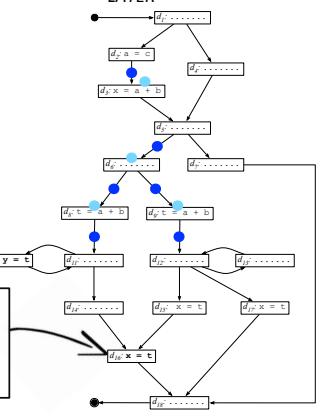
We must now delete redundant computations that exist at program points p. Can you determine $DELETE(p)$?



$$DELETE(i) = EXPR(i) \cap \overline{IN_{LATER}(i)}$$

Is it clear why all the other computations of $a + b$ must be kept unchanged?

In this example, there are four expressions that we can replace with a temporary.



15 Region-Based Analysis

The iterative data-flow analysis algorithm we have discussed so far is just one approach to solving data-flow problems. Here we discuss another approach called region-based analysis[6]. Recall that in the iterative-analysis approach, we create transfer functions for basic blocks, then find the fixedpoint solution by repeated passes over the blocks. Instead of creating transfer functions just for individual blocks, a region-based analysis finds transfer functions that summarize the execution of progressively larger regions of the program. Ultimately, transfer functions for entire procedures are constructed and then applied, to get the desired data-flow values directly.

While a data-flow framework using an iterative algorithm is specified by a semilattice of data-flow values and a family of transfer functions closed under composition, region-based analysis requires more elements. A region-based framework includes both a semilattice of data-flow values and a semilattice of transfer functions that must possess a meet operator, a composition operator, and a closure operator.

A region-based analysis is particularly useful for data-flow problems where paths that have cycles may change the data-flow values. The closure operator allows the effect of a loop to be summarized more effectively than does iterative analysis. The technique is also useful for interprocedural analysis, where transfer functions associated with a procedure call may be treated like the transfer functions associated with basic blocks.

15.1 Motivating Example

Consider the example in 78, we want to know how many bits needed to store the return value for a fpga device. We can pessimistically solve for the worst case. But we can also try to be more precise to calculate for each call site. It would be nice if instead of having to go back and iteratively solve a problem, for each different value of x .

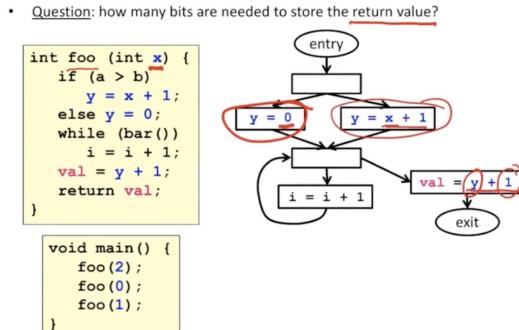


Figure 78: Motivating Example for region-based analysis

The idea behind region-based analysis is that we want to create a transfer function for the entire procedure.

15.2 Algorithm

Region

A region in a flow graph is a set of nodes with a header that dominates all other nodes in a region.

In Iterative Analysis, Transfer function F_B summarize effect from beginning to end of basic block B.

In Region-Based Analysis, Transfer function $F_{R,B}$ summarize effect from beginning of region R to end of basic block B. Recursively construct a larger region R from smaller regions construct $F_{R,B}$ from transfer functions for smaller regions until the program is one region. Let P be the region for the entire program, and v be initial value at entry node, $\text{out}[B] = F_{R,B}(v)$, $\text{in}[B] = \cap_{B'} \text{out}[B']$ where B' is a predecessor of B

We will use Reaching definitions as our transfer function to illustrate Region-Based Analysis.

15.2.1 Operations on Transfer Functions

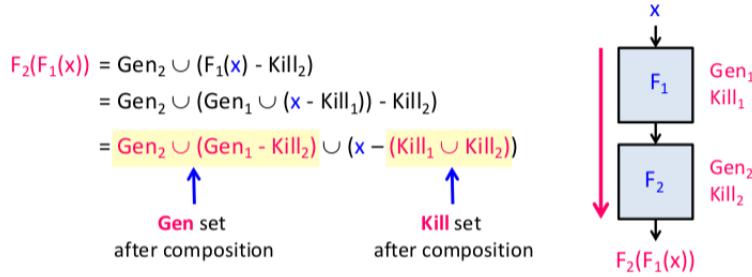
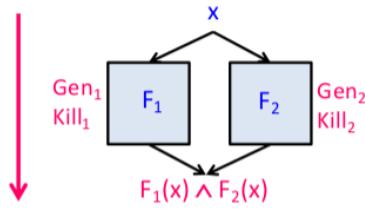


Figure 79: Operations on Transfer Functions: Composition

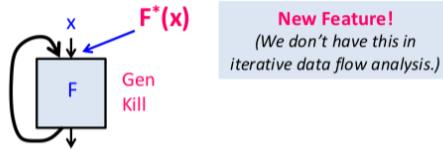


(Recall that for Reaching Definitions, $\wedge = \cup$.)

$$\begin{aligned}
 F_1(x) \wedge F_2(x) &= Gen_1 \cup (x - Kill_1) \cup Gen_2 \cup (x - Kill_2) \\
 &= (Gen_1 \cup Gen_2) \cup (x - (Kill_1 \cap Kill_2))
 \end{aligned}$$

↑ ↑
Gen set after \wedge **Kill** set after \wedge

Figure 80: Operations on Transfer Functions: Meet



What is the value at the **input of the block**?

- *including* the possible effects of the **back edge**
→ it may iterate 0, 1, 2, ..., ∞ number of times

$$\begin{aligned}
 F^*(x) &= \Lambda_{\{n \geq 0\}} F^n(x) \\
 &= x \wedge F(x) \wedge F(F(x)) \wedge \dots \quad \text{For Reaching Definitions} \\
 &= x \cup (Gen \cup (x - Kill)) \cup (Gen \cup ((Gen \cup (x - Kill)) - Kill)) \cup \dots \\
 &= Gen \cup (x - \emptyset)
 \end{aligned}$$

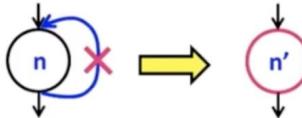
↑ ↑
Gen set **Kill** set (after closure)

Figure 81: Operations on Transfer Functions: Closure

15.2.2 Structure of Nested Regions (An Example)

T1-T2 rule (Hecht & Ullman)

- T1: Remove a loop
If n is a node with a loop, i.e. an edge $n \rightarrow n$, delete that edge



- T2: Remove a vertex
If there is a node n that has a unique predecessor, m , then m may consume n by deleting n and making all successors of n be successors of m .

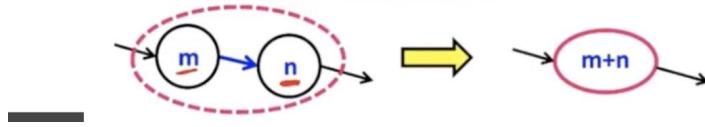
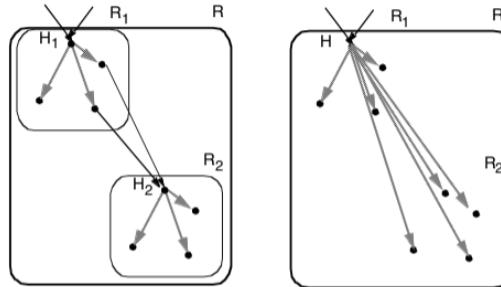


Figure 82

15.2.3 Transfer Functions for T2 Rule



- Transfer function
 $F_{R,B}$: summarizes the effect from beginning of R to end of B
 $F_{R,in(H2)}$: summarizes the effect from beginning of R to beginning of H_2
- Unchanged for blocks B in region R_1 ($F_{R,B} = F_{R1,B}$)
 - $F_{R,in(H2)} = \Delta_p F_{R,p}$ where p is a predecessor of H_2
 - For blocks B in region R_2 : $F_{R,B} = F_{R2,B} \cdot F_{R,in(H2)}$

Figure 83

15.2.4 Transfer Functions for T1 Rule

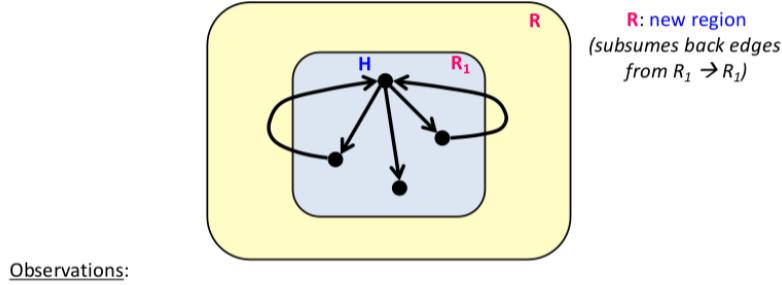


Figure 84

15.2.5 Example: Reaching Definitions

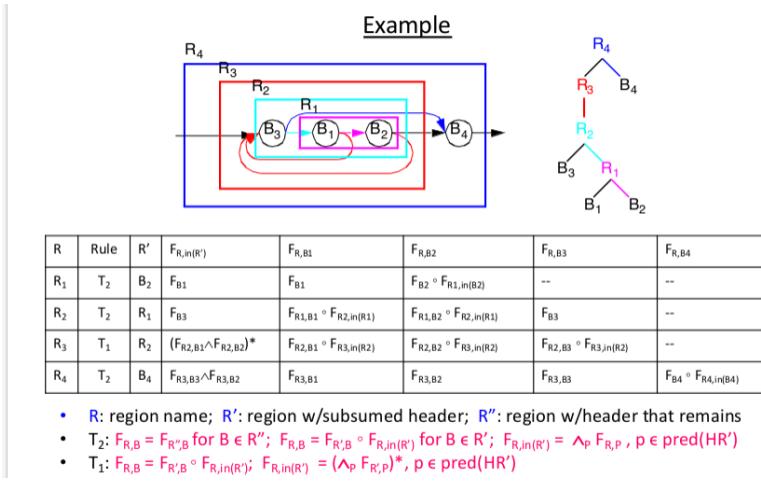


Figure 85

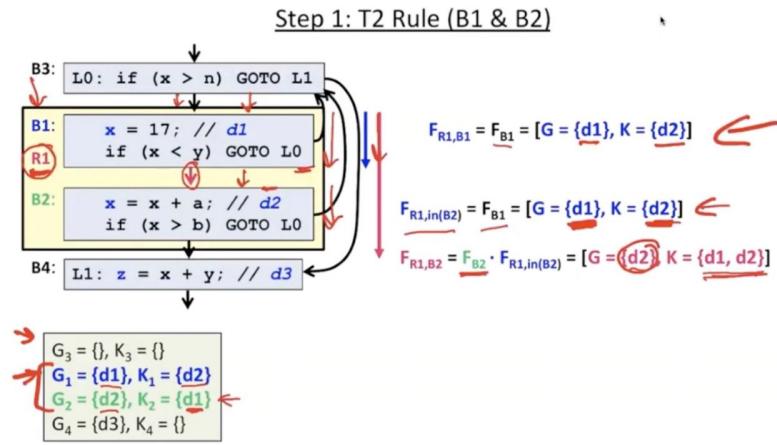


Figure 86

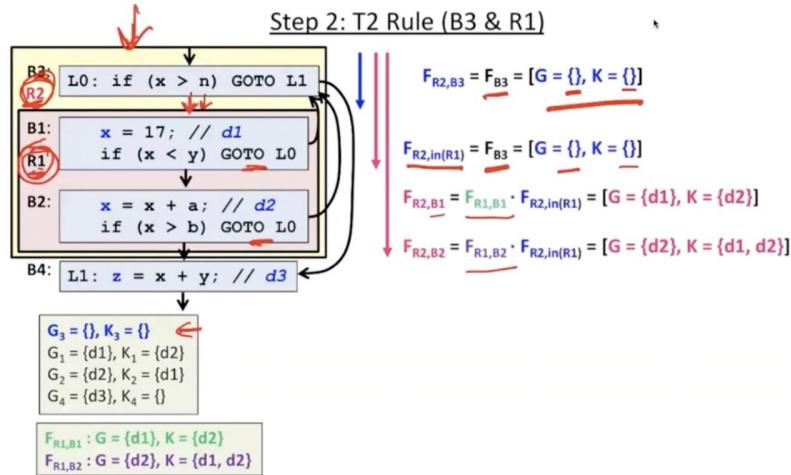


Figure 87

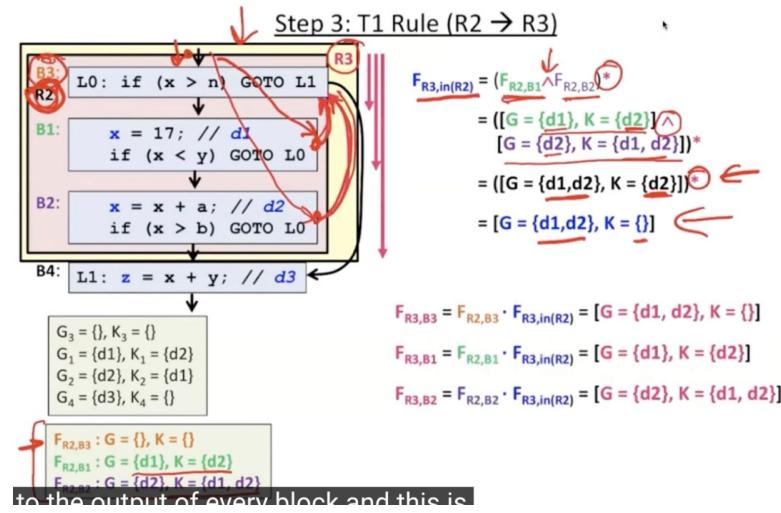


Figure 88

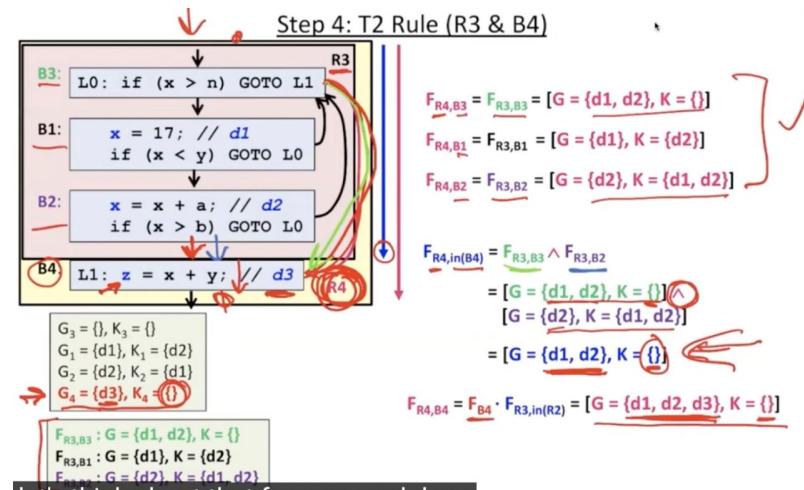


Figure 89

16 Pointer Analysis

Pointer analysis is a compile-time technique that helps identify relationships between pointer variables and the memory locations that they point to during program execution. Pointers are powerful programming constructs and allow complex memory manipulation during program execution through techniques such as pointer arithmetic and dynamic memory allocation. Pointer relationships can thus be complex and difficult to analyze at compile time. On the other hand, however, they provide the benefit of simplifying various other compile time analyses such as constant propagation, alias analysis in C programs that allow extensive use of pointers.^[7]

Potential applications of pointer analysis for multithreaded programs include: the development of sophisticated software engineering tools such as race detectors, memory leak detectors, wild pointer detectors and program slicers; memory system optimizations such as prefetching and moving computation to remote data; automatic batching of long latency file system operations; support parallelism in different levels: instruction-level parallelism and thread-level parallelism ; and to provide information required to apply traditional compiler optimizations such as constant propagation, common subexpression elimination, register allocation, code motion and induction variable elimination to multithreaded programs.^[8]

Aliases

Two variables are aliases if they reference the same memory location.

The Pointer Alias Analysis Problem

Decide for every pair of pointers at every program point: do they point to the same memory location?

16.1 Background

A pointer alias analysis attempts to determine when two pointer expressions refer to the same storage location. A points-to analysis , or similarly, an analysis based on a compact representation , attempts to determine what storage locations a pointer can point to. This information can then be used to determine the aliases in the program. Alias information is central to determining what memory locations are modified or referenced.

There are several dimensions that affect the cost/precision trade-offs of interprocedural pointer analyses. How a pointer analysis addresses each of these dimensions helps to categorize the analysis. An empirical comparison with a difference in more than one dimension can limit the usefulness of the comparison. Some of the dimensions are

Flow-sensitivity: Is control-flow information of a procedure used during the analysis? By not considering control-flow information, and therefore computing a conservative summary, flow-insensitive analyses compute one solution for either the whole program or for each method, whereas a flow-sensitive analysis computes a solution for each program point. Flow-insensitive analyses thus can be more efficient, but less precise than a flow-sensitive analysis. Flow-insensitive analyses are either equality-based, which treat assignments as bidirectional and typically use a union-find data structure, or subset-based, which treat an assignment as a unidirectional flow of values.

Context-sensitivity: Is calling context considered when analyzing a function or can values flow from one call through the function and return to another caller?

Heap modeling: Are objects named by allocation site, or is a more sophisticated shape analysis performed?

Aggregate modeling: Are elements of aggregates distinguished or collapsed into one object?

Whole program: Does an analysis require the whole program or can a sound solution be obtained by analyzing only components of a program?

Alias representation: Is an explicit alias representation [51, 64] or a points-to/compact representation used?

16.2 Flow-Sensitivity

Flow-sensitive pointer analysis respects a program's control flow and computes a separate solution for each program point, in contrast to a flow-insensitive analysis, which ignores statement ordering and computes a single solution that is conservatively correct for all program points.

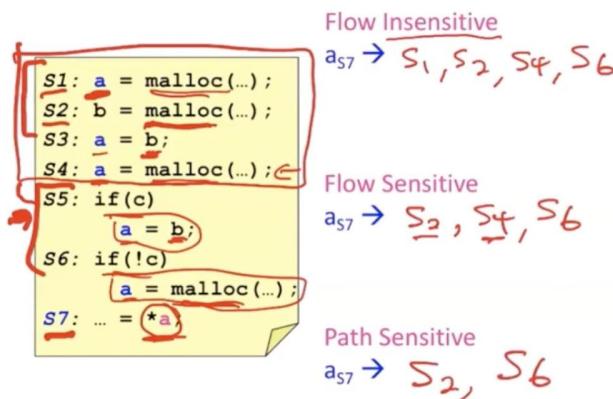


Figure 90: Flow-sensitive vs. flow-insensitive analysis

16.3 Context-sensitive

Context sensitivity has a most significant impact on analysis precision due to separate treatment for each method in the program. In practice, each time analysis considers new method call it creates a new structure that represents unique method scope in the memory. It treats all read/write operations inside this method in scope of this context and makes this information available later for its processing.

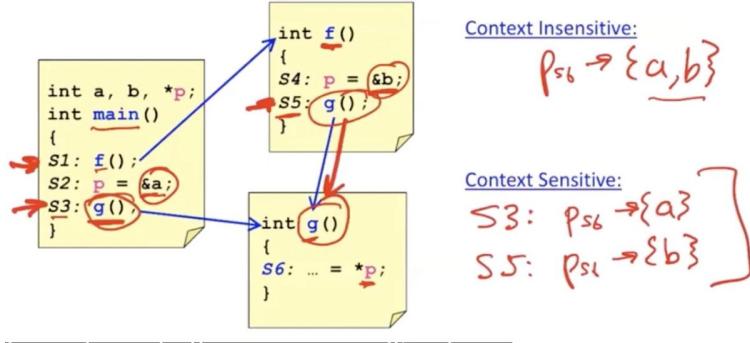


Figure 91: Context-sensitive vs. Context-insensitive analysis

16.4 Modeling Aggregates

A key implementation detail is whether aggregate components are distinguished or summarized into one object. C/C++’s weak typing makes this difficult to address correctly. Thus, most published work does not distinguish aggregates. However, this difficulty does not exist in a strongly-typed language like Java, and therefore, components should be distinguished in such languages. Most recent work has chosen to distinguish components. Unfortunately, few researchers have studied the impact of this decision.

16.5 Andersen’s Points-To Analysis

[9] Two common kinds of pointer analysis are alias analysis and points-to analysis. Alias analysis computes sets S holding pairs of variables p, q , where p and q may (or must) point to the same location. Points-to analysis, as described above, computes a relation $\text{points-to}(p, q)$, where p may (or must) point to the location of the variable q . We will focus primarily on points-to analysis, beginning with a simple but useful approach originally proposed by Andersen (PhD thesis: “Program Analysis and Specialization for the C Programming Language”). Our initial setting will be C programs. We are interested in analyzing instructions that are relevant to pointers in the program. Ignoring for the moment memory allocation and arrays, we can decompose all pointer operations into four types: taking the address of a variable, copying a pointer from one variable to another, assigning through a pointer, and dereferencing a pointer:

$$\begin{array}{l}
 I ::= \dots \\
 | \quad p := \&x \\
 | \quad p := q \\
 | \quad *p := q \\
 | \quad p := *q
 \end{array}$$

Andersen’s points-to analysis is a context-insensitive interprocedural analysis. It is also a flow-insensitive analysis, that is an analysis that does not consider program statement order. Context and

flow-insensitivity are used to improve the performance of the analysis, as precise pointer analysis can be notoriously expensive in practice.

We will formulate Andersen's analysis by generating set constraints which can later be processed by a set constraint solver using a number of technologies. Constraint generation for each statement works as given in the following set of rules. Because the analysis is flow-insensitive, we do not care what order the instructions in the program come in; we simply generate a set of constraints and solve them.

$$\frac{}{\llbracket p := \&x \rrbracket \hookrightarrow l_x \in p} \text{address-of}$$

$$\frac{}{\llbracket p := q \rrbracket \hookrightarrow p \supseteq q} \text{copy}$$

$$\frac{}{\llbracket *p := q \rrbracket \hookrightarrow *p \supseteq q} \text{assign}$$

$$\frac{}{\llbracket p := *q \rrbracket \hookrightarrow p \supseteq *q} \text{dereference}$$

The constraints generated are all set constraints. The first rule states that a constant location l_x , representing the address of x , is in the set of locations pointed to by p . The second rule states that the set of locations pointed to by p must be a superset of those pointed to by q . The last two rules state the same, but take into account that one or the other pointer is dereferenced.

A number of specialized set constraint solvers exist and constraints in the form above can be translated into the input for these. The dereference operation (the $*$ in $*p \subseteq q$) is not standard in set constraints, but it can be encoded—see Fahndrich's Ph.D. thesis for an example of how “to encode Andersen's points-to analysis for the BANE constraint solving engine. We will treat constraint-solving abstractly using the following constraint propagation rules:

$$\frac{p \supseteq q \quad l_x \in q}{l_x \in p} \text{copy}$$

$$\frac{*p \supseteq q \quad l_r \in p \quad l_x \in q}{l_x \in r} \text{assign}$$

$$\frac{p \supseteq *q \quad l_r \in q \quad l_x \in r}{l_x \in p} \text{dereference}$$

Figure 92

We can also apply Andersen's analysis to programs with dynamic memory allocation, such as:

```

1 : q := malloc1()
2 : p := malloc2()
3 : p := q
4 : r := &p
5 : s := malloc3()
6 : *r := s
7 : t := &s
8 : u := *t

```

Figure 93

In this example, the analysis is run the same way, but we treat the memory cell allocated at each malloc or new statement as an abstract location labeled by the location n of the allocation point. We can use the rules:

$\overline{\llbracket p := \text{malloc}_n() \rrbracket} \hookrightarrow l_n \in p$ *malloc*

Figure 94

We must be careful because a malloc statement can be executed more than once, and each time it executes, a new memory cell is allocated. Unless we have some other means of proving that the malloc executes only once, we must assume that if some variable p only points to one abstract malloc'd location l_n , that is still may-alias information (i.e. p points to only one of the many actual cells allocated at the given program location) and not must-alias information.

Analyzing the efficiency of Andersen's algorithm, we can see that all constraints can be generated in a linear $O(n)$ pass over the program. The solution size is $O(n^2)$ because each of the $O(n)$ variables defined in the program could potentially point to $O(n)$ other variables.

We can derive the execution time from a theorem by David McAllester published in SAS'99. There are $O(n)$ flow constraints generated of the form $p \subseteq q$, $*p \subseteq q$, or $p \subseteq *q$. How many times could a constraint propagation rule fire for each flow constraint? For a $p \subseteq q$ constraint, the rule may fire at most $O(n)$ times, because there are at most $O(n)$ premises of the proper form $l_x \in p$. However, a constraint of the form $p \subseteq *q$ could cause $O(n^2)$ rule firings, because there are $O(n)$ premises each of the form $l_x \in p$ and $l_r \in q$. With $O(n)$ constraints of the form $p \subseteq *q$ and $O(n^2)$ firings for each, we have $O(n^3)$ constraint firings overall. A similar analysis applies for $*p \subseteq q$ constraints. McAllester's theorem states that the analysis with $O(n^3)$ rule firings can be implemented in $O(n^3)$ time. Thus we have derived that Andersen's algorithm is cubic in the size of the program, in the worst case.

16.5.1 Field-Sensitive Analysis

What happens when we have a pointer to a struct in C, or an object in an object-oriented language? In this case, we would like the pointer analysis to tell us what each field in the struct or object points to. A simple solution is to be field-insensitive, treating all fields in a struct as equivalent. Thus if p points to a struct with two fields f and g , and we assign:

$$\begin{aligned} 1 : & \quad p.f := \&x \\ 2 : & \quad p.g := \&y \end{aligned}$$

Figure 95

A field-insensitive analysis would tell us (imprecisely) that $p.f$ could point to y . In order to be more precise, we can track the contents each field of each abstract location separately. In the discussion below, we assume a setting in which we cannot take the address of a field; this assumption is true for Java but not for C. We can define a new kind of constraints for fields:

$$\frac{}{\llbracket p := q.f \rrbracket \hookrightarrow p \supseteq q.f} \text{field-read}$$

$$\frac{}{\llbracket p.f := q \rrbracket \hookrightarrow p.f \supseteq q} \text{field-assign}$$

Figure 96

Now assume that objects (e.g. in Java) are represented by abstract locations l . We can process field constraints with the following rules:

$$\frac{p \supseteq q.f \quad l_q \in q \quad l_f \in l_q.f}{l_f \in p} \text{field-read}$$

$$\frac{p.f \supseteq q \quad l_p \in p \quad l_q \in q}{l_q \in l_p.f} \text{field-assign}$$

Figure 97

If we run this analysis on the code above, we find that it can distinguish that $p.f$ points to x and $p.g$ points to y .

16.6 Steensgaard's Points-To Analysis

For large programs, a cubic algorithm is too inefficient. Steensgaard proposed an pointer analysis algorithm that operates in near-linear time, supporting essentially unlimited scalability in practice. The first challenge in designing a near-linear time points-to analysis is to represent the results in linear space. This is nontrivial because over the course of program execution, any given pointer p could potentially point to the location of any other variable or pointer q . Representing all of these pointers explicitly will inherently take $O(n^2)$ space. The solution Steensgaard found is based on using constant space for each variable in the program. His analysis associates each variable p with an abstract location named after the variable. Then, it tracks a single points-to relation between that abstract location p and another one q , to which it may point. Now, it is possible that in some

real program p may point to both q and some other variable r. In this situation, Steensgaard's algorithm unifies the abstract locations for q and r, creating a single abstract location representing both of them. Now we can track the fact that p may point to either variable using a single points-to relationship.

For example, consider the program below:

```

1 :  p := &x
2 :  r := &p
3 :  q := &y
4 :  s := &q
5 :  r := s

```

Figure 98

Andersen's points-to analysis would produce the following graph:

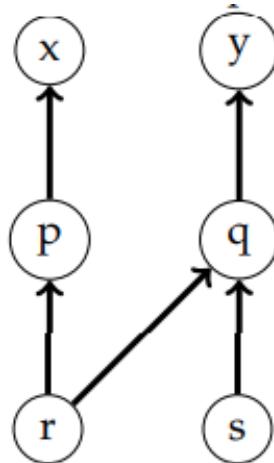


Figure 99

But in Steensgaard's setting, when we discover that r could point both to q and to p, we must merge q and p into a single node:

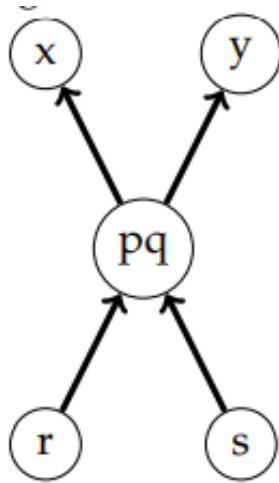


Figure 100

Notice that we have lost precision: by merging the nodes for p and q our graph now implies that s could point to p, which is not the case in the actual program. But we are not done. Now pq has two outgoing arrows, so we must merge nodes x and y. The final graph produced by Steensgaard's algorithm is therefore:

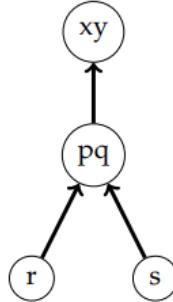


Figure 101

To define Steensgaard's analysis more precisely, we will study a simplified version of that ignores function pointers. It can be specified as follows:

$$\begin{aligned}
 \overline{[p := q]} &\hookrightarrow \overline{\text{join}(*p, *q)} \quad \text{copy} \\
 \overline{[p := \&x]} &\hookrightarrow \overline{\text{join}(*p, x)} \quad \text{address-of} \\
 \overline{[p := *q]} &\hookrightarrow \overline{\text{join}(*p, **q)} \quad \text{dereference} \\
 \overline{[*p := q]} &\hookrightarrow \overline{\text{join}(**p, *q)} \quad \text{assign}
 \end{aligned}$$

Figure 102

With each abstract location p , we associate the abstract location that p points to, denoted $*p$. Abstract locations are implemented as a union-find data structure so that we can merge two abstract locations efficiently. In the rules above, we implicitly invoke find on an abstract location before calling join on it, or before looking up the location it points to.

The join operation essentially implements a union operation on the abstract locations. However, since we are tracking what each abstract location points to, we must update this information also. The algorithm to do so is as follows:

```

join(e1, e2)
  if (e1 == e2)
    return
  e1next = *e1
  e2next = *e2
  unify(e1, e2)
  join(e1next, e2next)

```

Figure 103

Once again, we implicitly invoke find on an abstract location before comparing it for equality, looking up the abstract location it points to, or calling join recursively.

As an optimization, Steensgaard does not perform the join if the right hand side is not a pointer. For example, if we have an assignment $p := q$ and q has not been assigned any pointer value so far in the analysis, we ignore the assignment. If later we find that q may hold a pointer, we must revisit the assignment to get a sound result.

Steensgaard illustrated his algorithm using the following program:

```

1 : a := &x
2 : b := &y
3 : if p then
4 :   y := &z
5 : else
6 :   y := &x
7 : c := &y

```

Figure 104

His analysis produces the following graph for this program:

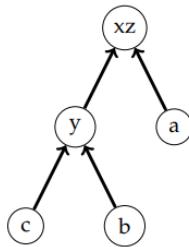


Figure 105

Rayside illustrates a situation in which Andersen must do more work than Steensgaard:

```

1 : q := &x
2 : q := &y
3 : p := q
4 : q := &z

```

Figure 106

After processing the first three statements, Steensgaard's algorithm will have unified variables x and y, with p and q both pointing to the unified node. In contrast, Andersen's algorithm will have both p and q pointing to both x and y. When the fourth statement is processed, Steensgaard's algorithm does only a constant amount of work, merging z in with the already-merged xy node. On the other hand, Andersen's algorithm must not just create a points-to relation from q to z, but must also propagate that relationship to p. It is this additional propagation step that results in the significant performance difference between these algorithms.

Analyzing Steensgaard's pointer analysis for efficiency, we observe that each of n statements in the program is processed once. The processing is linear, except for find operations on the unionfind data structure (which may take amortized time $O(\alpha(n))$ each) and the join operations. We note that in the join algorithm, the short-circuit test will fail at most $O(n)$ times—at most once for each variable in the program. Each time the short-circuit fails, two abstract locations are unified, at cost $O(\alpha(n))$. The unification assures the short-circuit will not fail again for one of these two variables. Because we have at most $O(n)$ operations and the amortized cost of each operation is at most $O(\alpha(n))$, the overall running time of the algorithm is near linear: $O(n * \alpha(n))$. Space consumption is linear, as no space is used beyond that used to represent abstract locations for all the variables in the program text.

Based on this asymptotic efficiency, Steensgaard's algorithm was run on a 1 million line program (Microsoft Word) in 1996; this was an order of magnitude greater scalability than other pointer analyses known at the time. Steensgaard's pointer analysis is field-insensitive; making it field-sensitive would mean that it is no longer linear.

16.7 Adding Context Sensitivity to Andersen's Algorithm

We can define a version of Andersen's points-to algorithm that is context-sensitive. In the following approach, we analyze each function separately for each calling point. The analysis keeps track of the current context, the calling point n of the current procedure. In the constraints, we track separate values for each variable x_n according to the calling context n of the procedure defining it, and we track separate values for each memory location l_n^k according to the calling context n active when that location was allocated at new instruction k . The rules are as follows:

$$\begin{array}{c}
\frac{n \vdash p := \mathbf{new}_k A \quad \text{new}}{l_n^k \in p_n} \\
\frac{n \vdash p := q \quad l_n \in q_n \quad \text{copy}}{l_n \in p_n} \\
\frac{n \vdash x.f := y \quad l_x \in x_n \quad l_y \in y_n}{l_y \in l_x.f} \quad \text{field-read} \\
\frac{n \vdash x := y.f \quad l_y \in y_n \quad l_z \in l_y.f}{l_z \in x_n} \quad \text{field-assign} \\
\frac{n \vdash f_k(y) \quad l_y \in y_n \quad \boxed{f(z) = e} \in \text{Program}}{l_y \in z_k \quad k \vdash e} \quad \text{call}
\end{array}$$

Figure 107

To illustrate this analysis, imagine we have the following code:

```

interface A { void g(); }
class B implements A { void g() { ... } }
class C implements A { void g() { ... } }
class D {
    A f(A a1) { return a1; }
}

// in main()
D d1 = new D();
if (...) {
    A x = d1.f(new B());
    x.g() // which g is called?
} else
    A y = d1.f(new C());
    y.g() // which g is called?

```

Figure 108

The analysis produces the following aliasing graph:

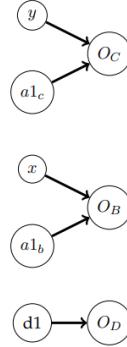


Figure 109

In this example, tracking two separate versions of the variable `a1` is sufficient to distinguish the objects of type B and C as they are passed through method `f`, meaning that the analysis can accurately track which version of `g` is called in each program location.

Call-string context sensitivity has its limits, however. Consider the following example, adapted from notes by Ryder:

```

interface X { void g(); }
class Y implements X { void g() { ... } }
class Z implements X { void g() { ... } }
class A {
    X x;
    void setX(X v) { helper(v); }
    void helper(X vh) { x = vh; }
    X getX() { return x; }
}
// in main()
A a1 = new A(); // allocates Oa1
A a2 = new A(); // allocates Oa2
a1.setX(new Y()); // allocates OY
a2.setX(new Z()); // allocates OZ
X x1 = a1.getX();
X x2 = a2.getX();
x1.g(); // which g() is called?
x2.g(); // which g() is called?
  
```

Figure 110

If we analyze this example with a 1-CFA style call-string sensitive pointer analysis, we get the following analysis results:

Context	Variable	Location	Notes
•	a1	Oa1	
•	a2	Oa2	
Y	this	Oa1	
Y	v	OY	
h	this	Oa1	
h	vh	OY	
Oa1	x	OY	
Z	this	Oa2	
Z	v	OZ	
h	this	Oa1,Oa2	updated
h	vh	OY,OZ	updated
Oa1	x	OY,OZ	updated
Oa2	x	OY,OZ	
•	x1	OY,OZ	
•	x1	OY,OZ	

Figure 111

Essentially, because of the helper method, one function call's worth of context sensitivity is insufficient to distinguish the calls to setX and helper for the objects Oa1 and Oa2. We could fix this by increasing context sensitivity, e.g. by going to a 2-CFA analysis that tracks call strings of length two. This has a very high cost in practice, however; 2-CFA does not scale well to large object-oriented programs.

A better solution comes from the insight that in the above example, call-strings are really tracking the wrong kind of context. What we need to do is distinguish between Oa1 and Oa2. In other words, the call chain does not matter so much; we want to be sensitive to the receiver object.

An alternative approach based on this idea is called object-sensitive analysis. It uses for the context not the call site, but rather the receiver object. In this case, we index everything not by a calling point n but instead by a receiver object l. The rules are as follows:

$$\begin{array}{c}
 \frac{l \vdash p := \mathbf{new}_k A}{l^k \in p_l} \text{ new} \\
 \frac{l \vdash p := q \quad l_l \in q_l}{l_l \in p_l} \text{ copy} \\
 \frac{l \vdash x.f := y \quad l_x \in x_l \quad l_y \in y_l}{l_y \in l_{x.f}} \text{ field-read} \\
 \frac{l \vdash x := y.f \quad l_y \in y_l \quad l_z \in l_{y.f}}{l_z \in x_l} \text{ field-assign} \\
 \frac{l \vdash x.f(y) \quad l_x \in x_l \quad l_y \in y_l \quad \llbracket f(z) = e \rrbracket \in \text{Program}}{l_x \in \mathbf{thisi}_{l_x} \quad l_y \in z_{l_x} \quad l_x \vdash e} \text{ call}
 \end{array}$$

Figure 112

Now if we reanalyze the example above, we get:

Context	Variable	Location
•	a1	Oa1
•	a2	Oa2
Oa1	v	OY
Oa1	vh	OY
Oa1	x	OY
Oa2	v	OZ
Oa2	vh	OZ
Oa2	x	OZ
•	x1	OY
•	x1	OZ

Figure 113

In practice, object-sensitive analysis appears to be the best approach to context sensitivity in the pointer or call-graph construction analysis of object-oriented programs. Intuitively, it seems that organizing a program around objects makes the objects themselves the most interesting thing to analyze.

The state of the art implementation technique for points-to analysis of object-oriented programs was presented by Bravenboer and Smaragdakis in OOPSLA 2009. Their approach generates declarative Datalog code to represent the input program, and a datalog evaluation engine solves what are essentially declarative constraints to get the analysis result.

In an more recent POPL 2011 paper analyzing object-sensitivity, Smaragdakis, Bravenboer, and Lhotak demonstrate that it is more effective than call-string sensitivity. They also propose a ‘ technique known as type-sensitive analysis which tracks only the type of the receiver (and, for depths ≥ 2 , the type of the object that created the reciever, etc.), and show that type-sensitive analysis is nearly as precise as object-sensitive analysis and much more scalable.

17 Profile Guided Optimizations

17.1 Efficient Path Profiling

17.2 Improved Basic Block Reordering

Improved Basic Block Reordering [10] is published by Andy Newell and Sergey Pupyrev from Facebook.

Given a directed control flow graph comprising of basic blocks and frequencies of jumps between the blocks, find an ordering of the blocks such that the number of fall-through jumps is maximized. This is the maximum directed TRAVELING SALESMAN PROBLEM (TSP). Solving TSP alone is not sufficient for constructing a good ordering of basic blocks. It is easy to find examples of control flow graphs with multiple different orderings that are all optimal with respect to the TSP objective. Consider for example a control flow graph in Figure 114 in which the maximum number of fall-through branches is achieved with two orderings that utilize a different number of I-cache lines in a typical execution. For these cases, an algorithm needs to take into consideration non-fall-through branches to choose the best ordering. However, maximizing the number of fall-through jumps is not always preferred from the performance point of view. Consider a control flow graph with seven basic blocks in Figure 115. It is not hard to verify that the ordering with the maximum number of fall-through branches is one containing two concatenated chains, $B_0 \rightarrow B_1 \rightarrow B_3 \rightarrow B_4$ and $B_5 \rightarrow B_6 \rightarrow B_2$ (upper-right in Figure 115). Observe that for this placement, the hot part of the function occupies three 64-byte cache lines. Arguably a better ordering is the lower-right in Figure 115, which uses only two cache lines for the five hot blocks, B_0, B_1, B_2, B_3, B_4 , at the cost of breaking the lightly weighted branch $B_6 \rightarrow B_2$.

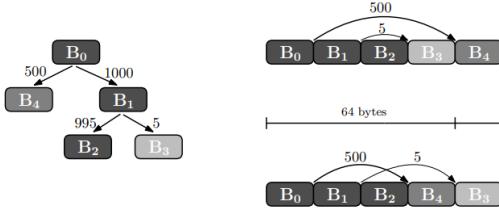


Figure 114: Two orderings of basic blocks with the same TSP score (1995) resulting in different I-cache utilization. All blocks have the same size of 16 bytes and colored according to their hotness in the profile.

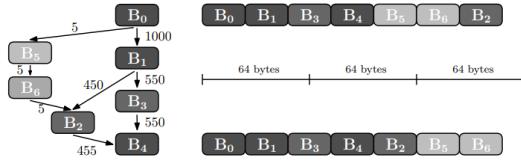


Figure 115: A control flow graph with jump frequencies (left) and two possible orderings of basic blocks (right). All blocks have the same size (in bytes) and colored according to their hotness in the profile. An optimal TSPbased layout (upper right) utilizes three cache lines for the hot code, while an arguably better layout (lower right) can be built with a new EXTTSP model.

17.2.1 Contribution

The contributions of the paper are the following.

- Identify an opportunity for improvement over the classical approach for basic block reordering, initiated by Pettis and Hansen [11]. Then they extend the model and suggest a new optimization problem with the objective closely related to the performance of a binary.
- Develop a new practical algorithm for basic block reordering. The algorithm relies on a greedy technique for solving the optimization problem.
- Propose a Mixed Integer Programming formulation for the aforementioned optimization problem, which is capable of finding optimal solutions on small functions

17.2.2 New ideas

In their study, they consider the following features.

- The length of a jump impacts the performance of instruction caches. Longer jumps are more likely to result in a cache miss than shorter ones. In particular, a jump with the length shorter than 64 bytes has a chance to remain within the same cache line.
- The direction of a branch plays a role for branch predicting. A branch $s \rightarrow t$ is called forward if $s < t$, that is, block s precedes block t in the ordering; otherwise, the branch is called backward.
- The branches can be classified into unconditional (if the out-degree is one) and conditional (if the out-degree is two). A special kind of branches is between consecutive blocks in the ordering that are called fall-through; in this case, a jump instruction is not needed.
- They introduce a new score that estimates the quality of a basic block ordering taking into account the branch characteristics. In the most generic form, the new function, called EXTENDED TSP (EXTTSP), is expressed as follows:

$$\text{ExtTSP} = \sum_{(s,t)} w(s,t) \times K_{s,t} \times h_{s,t}(\text{len}(s,t))$$

where the sum is taken over all branches in the control flow graph. Here $w(s, t)$ is the frequency of branch $s \rightarrow t$ and $0 \leq K_{s,t} \leq 1$ is a weight coefficient modeling the relative importance of the branch for optimization. We distinguish six types of branches arising in code: conditional and unconditional versions of fall-through, forward, and backward branches. Thus, we introduce six coefficients for EXTTSP. The lengths of the jumps are accounted in the last term of the expression, which increases the importance of short jumps. A non-negative function $h_{s,t}(len(s, t))$ is defined by value of 1 for zero-length jumps, value of 0 for jumps exceeding a prescribed length, and it monotonically decreases between the two values. To be consistent with the objective of TSP, the EXTTSP score needs to be maximized for the best performance. Notice that EXTTSP is a generalization of TSP, as the latter can be modeled by setting $K_{s,t} = 1, h(len(s, t)) = 1$ for fall-through branches and $K_{s,t} = 0$ otherwise.

They use machine learning methods to find parameters for EXTTSP that have the highest correlation with the performance of a binary in the experiment.

$$\text{ExtTSP} = \sum_{(s,t)} w(s, t) \times \begin{cases} 1 & \text{if } len(s, t) = 0, \\ 0.1 \cdot \left(1 - \frac{len(s, t)}{1024}\right) & \text{if } 0 < len(s, t) \leq 1024 \\ & \text{and } s < t, \\ 0.1 \cdot \left(1 - \frac{len(s, t)}{640}\right) & \text{if } 0 < len(s, t) \leq 640 \\ & \text{and } t < s, \\ 0 & \text{otherwise.} \end{cases}$$

. Intuitively, EXTTSP resembles the traditional TSP model, as the number of fall-through branches is the dominant factor. The main difference is that EXTTSP rewards longer jumps. The impact of such jumps is significantly lower and it linearly decreases with the length of a jump. Next we summarize our high-level observations regarding the new score function.

17.2.3 Algorithm

Algorithm 14 Basic Block Reordering

Input: control flow graph $G = (V, E, w)$, the entry point $v^* \in V$
Output: ordering of basic blocks ($v^* = B_1, B_2, \dots, B_{|v|}$)

```

function REORDERBASICBLOCKS
    for  $v \in V$  do
         $Chains \leftarrow Chains \cup (v)$ 
    end for
    while  $|Chains| > 1$  do                                 $\triangleright$  chain merging
        for  $c_i, c_j \in Chains$  do
             $gain[c_i, c_j] \leftarrow ComputeMergeGain(c_i, c_j)$ 
        end for
         $src, dst \leftarrow \arg \max_{i,j} gain[c_i, c_j]$            $\triangleright$  find best pair of chains
         $Chains \leftarrow Chains \cup Merge(src, dst) \setminus \{src, dst\};$        $\triangleright$  merge the pair and update chains
    end while
    return ordering given by the remaining chain;
end function

function COMPUTEMERGE_GAIN( $src, dst$ )
    for  $i = 1$  to  $blocks(src)$  do                       $\triangleright$  try all ways to split chain src
         $s_1 \leftarrow src[1 : i]$                              $\triangleright$  break the chain at index i
         $s_2 \leftarrow src[i + 1 : blocks(src)]$ 
         $score_i \leftarrow \max \begin{cases} ExtTSP(s_1, s_2, dst) & \text{if } v^* \notin dst \\ ExtTSP(s_1, dst, s_2) & \text{if } v^* \notin dst \\ ExtTSP(s_2, s_1, dst) & \text{if } v^* \notin s_1, dst \\ ExtTSP(s_2, dst, s_1) & \text{if } v^* \notin s_1, dst \\ ExtTSP(dst, s_1, s_2) & \text{if } v^* \notin src \\ ExtTSP(dst, s_2, s_1) & \text{if } v^* \notin src \end{cases}$            $\triangleright$  try all valid ways to concatenate
    end for
    return  $\max_i score_i - ExtTSP(src) - ExtTSP(dst)$   $\triangleright$  the gain of merging chains src and dst
end function

```

References

- [1] Etienne Morel and Claude Renvoise. “Global optimization by suppression of partial redundancies”. In: *Communications of the ACM* 22.2 (1979), pp. 96–103.
- [2] Bernhard Steffen. “Data flow analysis as model checking”. In: *International Symposium on Theoretical Aspects of Computer Software*. Springer. 1991, pp. 346–364.
- [3] Oliver Rüthing, Jens Knoop, and Bernhard Steffen. “Sparse code motion”. In: *Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*. 2000, pp. 170–183.

- [4] *293S_08_PRE_LCM*. https://sites.cs.ucsb.edu/~yufeiding/cs293s/slides/293S_08_PRE_LCM.pdf. (Accessed on 11/27/2022).
- [5] *Microsoft PowerPoint - L12-Lazy-Code-Motion*. <https://www.cs.cmu.edu/afs/cs/academic/class/15745-s16/www/lectures/L12-Lazy-Code-Motion.pdf>. (Accessed on 11/27/2022).
- [6] *Microsoft PowerPoint - L12-Interval-Analysis*. <http://www.cs.cmu.edu/afs/cs/academic/class/15745-s13/public/lectures/L12-Interval-Analysis-1up.pdf>. (Accessed on 11/27/2022).
- [7] *Points-to Analysis*. <https://engineering.purdue.edu/Cetus/Documentation/manual/ch07s05.html>. (Accessed on 11/30/2022).
- [8] Radu Rugina and Martin C Rinard. “Pointer analysis for structured parallel programs”. In: *ACM Transactions on Programming Languages and Systems (TOPLAS)* 25.1 (2003), pp. 70–116.
- [9] *notes07-pointers.pdf*. <http://www.cs.cmu.edu/~clegoues/courses/15-8190-16sp/notes/notes07-pointers.pdf>. (Accessed on 12/04/2022).
- [10] Andy Newell and Sergey Pupyrev. “Improved basic block reordering”. In: *IEEE Transactions on Computers* 69.12 (2020), pp. 1784–1794.
- [11] Karl Pettis and Robert C Hansen. “Profile guided code positioning”. In: *Proceedings of the ACM SIGPLAN 1990 conference on Programming language design and implementation*. 1990, pp. 16–27.