

Détermination de propriétés de flots de données pour l'amélioration du temps d'exécution pire-cas

Candidat
Jordy RUIZ

Encadrant
Hugues CASSÉ

20 juin 2014

Sommaire

- 1 Introduction
- 2 Problématique et contexte
- 3 Solution
- 4 Ouvertures et conclusion

Plan

- 1 Introduction
- 2 Problématique et contexte
- 3 Solution
- 4 Ouvertures et conclusion

Introduction



Équipe TRACES

Plan

- 1 Introduction
- 2 Problématique et contexte
- 3 Solution
- 4 Ouvertures et conclusion

Estimation du pire temps d'exécution (WCET)

- But : surestimer le temps d'exécution d'une partie de programme
- Exemples
 - Le frein de voiture s'activera au pire 50ms après la commande
 - L'algorithme prendra une décision en moins d'1s
 - ...

Estimation du pire temps d'exécution (WCET)

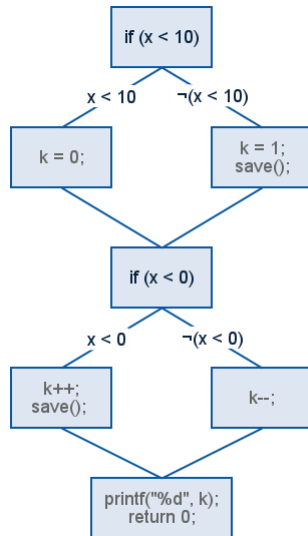
- But : surestimer le temps d'exécution d'une partie de programme
- Exemples
 - Le frein de voiture s'activera au pire 50ms après la commande
 - L'algorithme prendra une décision en moins d'1s
 - ...
- Systèmes temps-réel critiques : les mesures ne suffisent pas, il faut une **preuve** !

Estimation du pire temps d'exécution (WCET)

- But : surestimer le temps d'exécution d'une partie de programme
- Exemples
 - Le frein de voiture s'activera au pire 50ms après la commande
 - L'algorithme prendra une décision en moins d'1s
 - ...
- Systèmes temps-réel critiques : les mesures ne suffisent pas, il faut une **preuve** !
- Calcul du pire-temps : maximisation en ILP
 - $WCET = \max \sum x_i t_i$
+ contraintes matérielles + contraintes logicielles

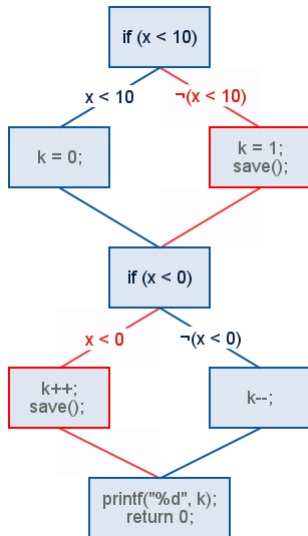
Recherche de chemins infaisables

- Graphe de flot de contrôle



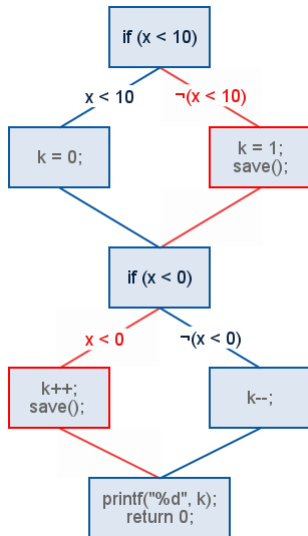
Recherche de chemins infaisables

- Graphe de flot de contrôle
- Chemins + SMT
 - $(x < 10) \wedge (x < 0)$
 - $(x < 10) \wedge \neg(x < 0)$
 - $\neg(x < 10) \wedge (x < 0) \models \perp$
 - $\neg(x < 10) \wedge \neg(x < 0)$



Recherche de chemins infaisables

- Graphe de flot de contrôle
- Chemins + SMT
 - $(x < 10) \wedge (x < 0)$
 - $(x < 10) \wedge \neg(x < 0)$
 - $\neg(x < 10) \wedge (x < 0) \models \perp$
 - $\neg(x < 10) \wedge \neg(x < 0)$
- Chemin infaisable
 \Rightarrow contrainte ILP
 $n_{(x < 0)} \leq n_{(x < 10)}$



Choix du solveur SMT

Notre choix de solveur s'est porté sur **CVC4** :

- Open-source, licence très libre



Choix du solveur SMT

Notre choix de solveur s'est porté sur **CVC4** :

- Open-source, licence très libre
- De très bons résultats à la SMT-COMP



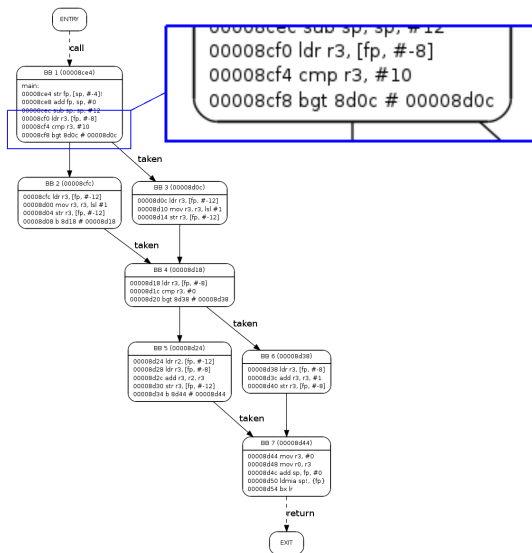
Choix du solveur SMT

Notre choix de solveur s'est porté sur **CVC4** :

- Open-source, licence très libre
- De très bons résultats à la SMT-COMP
- Une API C++ riche et bien documentée



Graphe en langage machine



Les instructions sémantiques d'OTAWA

```
ldr r0, [pc, #20]
@ seti ?15, 0x8310
@ seti t2, 0x14
@ add t1, ?15, t2
@ load ?0, t1, uint32

mov r1, #0
@ seti ?1, 0x0

mov r2, r1
@ set t1, ?1
@ set ?2, t1

bl 8574
@ seti t1, 0x8574
@ seti ?14, 0x8318
@ branch t1
```

Les variables d'OTAWA :

- les registres machine ?0, ?1...(16, 32... ou plus selon l'architecture)
- des variables temporaires t1, t2...
 - locales à une instruction machine (détruites à la fin)
 - aident à la traduction en instructions sémantiques

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : `BRANCH`, `TRAP`, `CONT`

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : `BRANCH`, `TRAP`, `CONT`
- d'invalidation : `SCRATCH`

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : `BRANCH`, `TRAP`, `CONT`
- d'invalidation : `SCRATCH`
- d'assignation de valeur : `SET`, `SETI`

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : BRANCH, TRAP, CONT
- d'invalidation : SCRATCH
- d'assignation de valeur : SET, SETI
- arithmétiques : ADD, SUB, MUL, DIV, MOD

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : BRANCH, TRAP, CONT
- d'invalidation : SCRATCH
- d'assignation de valeur : SET, SETI
- arithmétiques : ADD, SUB, MUL, DIV, MOD
- logiques : ~~NOT, AND, OR, XOR~~

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : BRANCH, TRAP, CONT
- d'invalidation : SCRATCH
- d'assignation de valeur : SET, SETI
- arithmétiques : ADD, SUB, MUL, DIV, MOD
- ~~logiques : NOT, AND, OR, XOR~~
- conditionnelles : CMP, IF

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : BRANCH, TRAP, CONT
- d'invalidation : SCRATCH
- d'assignation de valeur : SET, SETI
- arithmétiques : ADD, SUB, MUL, DIV, MOD
- ~~logiques : NOT, AND, OR, XOR~~
- conditionnelles : CMP, IF
- d'accès mémoire : LOAD, STORE

Les instructions sémantiques d'OTAWA

Des instructions...

- indicatrices du flot du programme : BRANCH, TRAP, CONT
- d'invalidation : SCRATCH
- d'assignation de valeur : SET, SETI
- arithmétiques : ADD, SUB, MUL, DIV, MOD
- ~~logiques : NOT, AND, OR, XOR~~
- conditionnelles : CMP, IF
- d'accès mémoire : LOAD, STORE

- ~~... et les équivalents *unsigned* : CMPU, MULU, DIVU, MODU~~

Plan

- 1 Introduction
- 2 Problématique et contexte
- 3 Solution**
- 4 Ouvertures et conclusion

Représentation des prédicats

```

15] + ?14 = [(t1 - 4)]
16] - ?4 = [(t1 - t2) - t2]
17] + ?4 = [(t1 - 4) - 4]
18] - ?13 - ((t1 - t2) - t2) = 8
19] + ?13 - ((t1 - 4) - 4) = 8
20] - t2 = 4
21] - ?14 = [t1 - 4]
22] - ?4 = [(t1 - 4) - 4]
23] - ?13 - ((t1 - 4) - 4) = 8
24] bx lr
25] branch ?14
26] Predicates generated: [?0 = 0]
27] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
28] EXIT block reached
29] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
30] SMT call: UNSAT
31] [Inf. path found: [1->3, 5->6] (bitcode=101)]
32] Current path identified as infeasible, stopping analysis
33] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
34] SMT call: SAT
35] Processing BB 2 (000082e8)
36] bl 8278
37] seti t1, 0x8278 (33400)
38] + t1 = 0x8278
39] seti ?14, 0x82ec (33516)
40] + ?14 = 0x82ec
41] branch t1
42] - t1 = 0x8278
43] Predicates generated: [?14 = 0x82ec]
44] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
45] SMT call: SAT
46] Processing BB 4 (000082ec)
47] b 82f4
48] seti t1, 0x82f4 (33524)
49] + t1 = 0x82f4
50] branch t1
51] - t1 = 0x82f4

```

```

161] load ?14, t1, shift1
162] - (?14 = 0x8318 | 9->10)
163] + ?14 = [t1]
164] add t1, t1, t2
165] [t1 - t2 / t1]
166] - ?14 = [t1]
167] + ?14 = [t1 - t2]
168] - ?4 = [t1 - t2]
169] + ?4 = [(t1 - t2) - t2]
170] - t3 - (t1 - t2) = 8
171] + t3 - ((t1 - t2) - t2) = 8
172] - t1 - t2 = ?13
173] + (t1 - t2) - t2 = ?13
174] set ?13, t3
175] - (t1 - t2) - t2 = ?13
176] + ?13 = t3
177] [?13 / t3]
178] - t3 - ((t1 - t2) - t2) = 8
179] + ?13 - ((t1 - t2) - t2) = 8
180] - ?13 = t3
181] [4 / t2]
182] - ?14 = [t1 - t2]
183] + ?14 = [t1 - 4]
184] - ?4 = [(t1 - t2) - t2]
185] + ?4 = [(t1 - 4) - 4]
186] - ?13 - ((t1 - t2) - t2) = 8
187] + ?13 - ((t1 - 4) - 4) = 8
188] - t2 = 4
189] - ?14 = [t1 - 4]
190] - ?4 = [(t1 - 4) - 4]
191] - ?13 - ((t1 - 4) - 4) = 8
192] bx lr
193] branch ?14
194] Predicates generated: [?0 = 0]
195] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
196] EXIT block reached
197] 1 infeasible path found:
198] - [1->3, 5->6]

```

```

15] + ?14 = [t1 - 4]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [t1 - 4]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
17] [Inf. path found: [1->3, 5->6] (bitcode=101)]
18] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
12] bl 8278
10] seti t1, 0x8278 (33400)
10] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
10] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
12] b 82f4
10] seti t1, 0x82f4 (33524)
10] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

16] add ?13, t2, ?13
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t1, t2
116] [t1 - t2 / t1]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]

```

```

15] + ?14 = [t1 - 4]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [t1 - 4]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
13] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
12] bl 8278
10] seti t1, 0x8278 (33400)
18] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
18] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
12] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4
    
```

```

16] add ?14, t2, #16
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t2, t2
116] [t1 - t2 / t1]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]
    
```

```

15] + ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [t1 - 4]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
14] Processing BB 2 (000082e8)
12] bl 8278
10] seti t1, 0x8278 (33400)
18] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
18] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
14] Processing BB 4 (000082ec)
12] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4
    
```

```

16] add ?13, t2, #10
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t1, t2
116] [(t1 - t2 / t1)]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]
    
```

```

15] + ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [t1 - 4]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch r14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
12] Processing BB 2 (000082e8)
12] bl 8278
16] seti t1, 0x8278 (33400)
18] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
18] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
12] Processing BB 4 (000082ec)
12] b 82f4
16] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4
    
```

```

16] load ?14, t2, r14
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t1, t2
116] [(t1 - t2 / t1)]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]
    
```

```

15] + ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
10] bx t1
10] branch ?14
10] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
17] bl 8278
10] seti t1, 0x8278 (33400)
10] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
10] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
17] bl 82f4
10] seti t1, 0x82f4 (33524)
10] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4
    
```

```

17] add ?14, t1, ?14
117] - (?14 = 0x8318 | 9->10)
180] + ?14 = [(t1)]
130] add t1, t1, t2
110] [(t1 - t2 / t1)]
145] - ?14 = [(t1)]
153] + ?14 = [(t1 - t2)]
145] - ?4 = [(t1 - t2)]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - ((t1 - t2) - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [(t1 - t2)]
105] + ?14 = [(t1 - 4)]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [(t1 - 4)]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx t1
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]
    
```



```

15] + ?14 = [(t1 - 4)]
16] - ?4 = [(t1 - t2) - t2]
17] + ?4 = [(t1 - 4) - 4]
18] - ?13 - ((t1 - t2) - t2) = 8
19] + ?13 - ((t1 - 4) - 4) = 8
20] - t2 = 4
21] - ?14 = [t1 - 4]
22] - ?4 = [(t1 - 4) - 4]
23] - ?13 - ((t1 - 4) - 4) = 8
24] bx lr
25] branch ?14
26] Predicates generated: [?0 = 0]
27] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
28] EXIT block reached
29] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
30] SMT call: UNSAT
31] [Inf. path found: [1->3, 5->6] (bitcode=101)]
32] Current path identified as infeasible, stopping analysis
33] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
34] SMT call: SAT
35] Processing BB 2 (000082e8)
36] bl 8278
37] seti t1, 0x8278 (33400)
38] + t1 = 0x8278
39] seti ?14, 0x82ec (33516)
40] + ?14 = 0x82ec
41] branch t1
42] - t1 = 0x8278
43] Predicates generated: [?14 = 0x82ec]
44] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
45] SMT call: SAT
46] Processing BB 4 (000082ec)
47] b 82f4
48] seti t1, 0x82f4 (33524)
49] + t1 = 0x82f4
50] branch t1
51] - t1 = 0x82f4

```

```

161] load ?14, t1, shift
162] - (?14 = 0x8318 | 9->10)
163] + ?14 = [t1]
164] add t1, t1, t2
165] [t1 - t2 / t1]
166] - ?14 = [t1]
167] + ?14 = [t1 - t2]
168] - ?4 = [t1 - t2]
169] + ?4 = [(t1 - t2) - t2]
170] - t3 - (t1 - t2) = 8
171] + t3 - ((t1 - t2) - t2) = 8
172] - t1 - t2 = ?13
173] + (t1 - t2) - t2 = ?13
174] set ?13, t3
175] - (t1 - t2) - t2 = ?13
176] + ?13 = t3
177] [?13 / t3]
178] - t3 - ((t1 - t2) - t2) = 8
179] + ?13 - ((t1 - t2) - t2) = 8
180] - ?13 = t3
181] [4 / t2]
182] - ?14 = [t1 - t2]
183] + ?14 = [t1 - 4]
184] - ?4 = [(t1 - t2) - t2]
185] + ?4 = [(t1 - 4) - 4]
186] - ?13 - ((t1 - t2) - t2) = 8
187] + ?13 - ((t1 - 4) - 4) = 8
188] - t2 = 4
189] - ?14 = [t1 - 4]
190] - ?4 = [(t1 - 4) - 4]
191] - ?13 - ((t1 - 4) - 4) = 8
192] bx lr
193] branch ?14
194] Predicates generated: [?0 = 0]
195] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
196] EXIT block reached
197] 1 infeasible path found:
198] - [1->3, 5->6]

```

```

15] + ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
12] bl 8278
10] seti t1, 0x8278 (33400)
14] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
14] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
12] b 82f4
10] seti t1, 0x82f4 (33524)
14] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

16] add ?14, t1, #10
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t1, t2
116] [(t1 - t2 / t1)]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [(t1 - 4)]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]

```

```

55] + ?14 = [t1 - 4]
54] - ?4 = [(t1 - t2) - t2]
55] + ?4 = [(t1 - 4) - 4]
54] - ?13 - ((t1 - t2) - t2) = 8
55] + ?13 - ((t1 - 4) - 4) = 8
50] - t2 = 4
54] - ?14 = [t1 - 4]
54] - ?4 = [(t1 - 4) - 4]
54] - ?13 - ((t1 - 4) - 4) = 8
52] bx lr
50] branch ?14
53] Predicates generated: [?0 = 0]
52] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
52] EXIT block reached
52] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
56] SMT call: UNSAT
53] [Inf. path found: [1->3, 5->6] (bitcode=101)]
52] Current path identified as infeasible, stopping analysis
52] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
56] SMT call: SAT
56] Processing BB 2 (000082e8)
52] bl 8278
50] seti t1, 0x8278 (33400)
58] + t1 = 0x8278
50] seti ?14, 0x82ec (33516)
58] + ?14 = 0x82ec
50] branch t1
50] - t1 = 0x8278
53] Predicates generated: [?14 = 0x82ec]
52] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
56] SMT call: SAT
56] Processing BB 4 (000082ec)
52] b 82f4
50] seti t1, 0x82f4 (33524)
58] + t1 = 0x82f4
50] branch t1
50] - t1 = 0x82f4
    
```

```

517] - (?14 = 0x8318 | 9->10)
588] + ?14 = [t1]
530] add t1, t1, t2
516] [t1 - t2 / t1]
545] - ?14 = [t1]
553] + ?14 = [t1 - t2]
545] - ?4 = [t1 - t2]
553] + ?4 = [(t1 - t2) - t2]
545] - t3 - (t1 - t2) = 8
553] + t3 - ((t1 - t2) - t2) = 8
545] - t1 - t2 = ?13
553] + (t1 - t2) - t2 = ?13
530] set ?13, t3
531] - (t1 - t2) - t2 = ?13
588] + ?13 = t3
500] [?13 / t3]
504] - t3 - ((t1 - t2) - t2) = 8
505] + ?13 - ((t1 - t2) - t2) = 8
560] - ?13 = t3
500] [4 / t2]
504] - ?14 = [t1 - t2]
505] + ?14 = [t1 - 4]
504] - ?4 = [(t1 - t2) - t2]
505] + ?4 = [(t1 - 4) - 4]
504] - ?13 - ((t1 - t2) - t2) = 8
505] + ?13 - ((t1 - 4) - 4) = 8
560] - t2 = 4
574] - ?14 = [t1 - 4]
574] - ?4 = [(t1 - 4) - 4]
574] - ?13 - ((t1 - 4) - 4) = 8
522] bx lr
530] branch ?14
503] Predicates generated: [?0 = 0]
502] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
552] EXIT block reached
529] 1 infeasible path found:
544] - [1->3, 5->6]
    
```

```

15] + ?14 = [t1 - 4]
16] - ?4 = [(t1 - t2) - t2]
17] + ?4 = [(t1 - 4) - 4]
18] - ?13 - ((t1 - t2) - t2) = 8
19] + ?13 - ((t1 - 4) - 4) = 8
20] - t2 = 4
21] - ?14 = [t1 - 4]
22] - ?4 = [(t1 - 4) - 4]
23] - ?13 - ((t1 - 4) - 4) = 8
24] bx lr
25] branch ?14
26] Predicates generated: [?0 = 0]
27] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
28] EXIT block reached
29] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
30] SMT call: UNSAT
31] [Inf. path found: [1->3, 5->6] (bitcode=101)]
32] Current path identified as infeasible, stopping analysis
33] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
34] SMT call: SAT
35] Processing BB 2 (000082e8)
36] bl 8278
37] seti t1, 0x8278 (33400)
38] + t1 = 0x8278
39] seti ?14, 0x82ec (33516)
40] + ?14 = 0x82ec
41] branch t1
42] - t1 = 0x8278
43] Predicates generated: [?14 = 0x82ec]
44] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
45] SMT call: SAT
46] Processing BB 4 (000082ec)
47] b 82f4
48] seti t1, 0x82f4 (33524)
49] + t1 = 0x82f4
50] branch t1
51] - t1 = 0x82f4

```

```

167] add ?14, t2, #16
168] - (?14 = 0x8318 | 9->10)
169] + ?14 = [t1]
170] add t1, t1, t2
171] [t1 - t2 / t1]
172] - ?14 = [t1]
173] + ?14 = [t1 - t2]
174] - ?4 = [t1 - t2]
175] + ?4 = [(t1 - t2) - t2]
176] - t3 - (t1 - t2) = 8
177] + t3 - ((t1 - t2) - t2) = 8
178] - t1 - t2 = ?13
179] + (t1 - t2) - t2 = ?13
180] set ?13, t3
181] - (t1 - t2) - t2 = ?13
182] + ?13 = t3
183] [?13 / t3]
184] - t3 - ((t1 - t2) - t2) = 8
185] + ?13 - ((t1 - t2) - t2) = 8
186] - ?13 = t3
187] [4 / t2]
188] - ?14 = [t1 - t2]
189] + ?14 = [t1 - 4]
190] - ?4 = [(t1 - t2) - t2]
191] + ?4 = [(t1 - 4) - 4]
192] - ?13 - ((t1 - t2) - t2) = 8
193] + ?13 - ((t1 - 4) - 4) = 8
194] - t2 = 4
195] - ?14 = [t1 - 4]
196] - ?4 = [(t1 - 4) - 4]
197] - ?13 - ((t1 - 4) - 4) = 8
198] bx lr
199] branch ?14
200] Predicates generated: [?0 = 0]
201] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
202] EXIT block reached
203] 1 infeasible path found:
204] - [1->3, 5->6]

```

```

15] + ?14 = [(t1 - 4)]
16] - ?4 = [(t1 - t2) - t2]
17] + ?4 = [(t1 - 4) - 4]
18] - ?13 - ((t1 - t2) - t2) = 8
19] + ?13 - ((t1 - 4) - 4) = 8
20] - t2 = 4
21] - ?14 = [t1 - 4]
22] - ?4 = [(t1 - 4) - 4]
23] - ?13 - ((t1 - 4) - 4) = 8
24] bx lr
25] branch ?14
26] Predicates generated: [?0 = 0]
27] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
28] EXIT block reached
29] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
30] SMT call: UNSAT
31] [Inf. path found: [1->3, 5->6] (bitcode=101)]
32] Current path identified as infeasible, stopping analysis
33] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
34] SMT call: SAT
35] Processing BB 2 (000082e8)
36] bl 8278
37] seti t1, 0x8278 (33400)
38] + t1 = 0x8278
39] seti ?14, 0x82ec (33516)
40] + ?14 = 0x82ec
41] branch t1
42] - t1 = 0x8278
43] Predicates generated: [?14 = 0x82ec]
44] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
45] SMT call: SAT
46] Processing BB 4 (000082ec)
47] b 82f4
48] seti t1, 0x82f4 (33524)
49] + t1 = 0x82f4
50] branch t1
51] - t1 = 0x82f4

```

```

161] load ?14, t1, 82f4
162] - (?14 = 0x8318 | 9->10)
163] + ?14 = [t1]
164] add t1, t1, t2
165] [t1 - t2 / t1]
166] - ?14 = [t1]
167] + ?14 = [t1 - t2]
168] - ?4 = [t1 - t2]
169] + ?4 = [(t1 - t2) - t2]
170] - t3 - (t1 - t2) = 8
171] + t3 - ((t1 - t2) - t2) = 8
172] - t1 - t2 = ?13
173] + (t1 - t2) - t2 = ?13
174] set ?13, t3
175] - (t1 - t2) - t2 = ?13
176] + ?13 = t3
177] [?13 / t3]
178] - t3 - ((t1 - t2) - t2) = 8
179] + ?13 - ((t1 - t2) - t2) = 8
180] - ?13 = t3
181] [4 / t2]
182] - ?14 = [t1 - t2]
183] + ?14 = [t1 - 4]
184] - ?4 = [(t1 - t2) - t2]
185] + ?4 = [(t1 - 4) - 4]
186] - ?13 - ((t1 - t2) - t2) = 8
187] + ?13 - ((t1 - 4) - 4) = 8
188] - t2 = 4
189] - ?14 = [t1 - 4]
190] - ?4 = [(t1 - 4) - 4]
191] - ?13 - ((t1 - 4) - 4) = 8
192] bx lr
193] branch ?14
194] Predicates generated: [?0 = 0]
195] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
196] EXIT block reached
197] 1 infeasible path found:
198] - [1->3, 5->6]

```

```

15] + ?14 = [t1 - 4]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [t1 - 4]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
12] bl 8278
10] seti t1, 0x8278 (33400)
18] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
18] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
12] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4
    
```

```

16] add ?14, t1, #14
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t1, t2
116] [t1 - t2 / t1]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]
    
```

```

15] + ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - t2) - t2]
15] + ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - t2) - t2) = 8
15] + ?13 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - ?14 = [(t1 - 4)]
14] - ?4 = [(t1 - 4) - 4]
14] - ?13 - ((t1 - 4) - 4) = 8
12] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
12] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
13] [Inf. path found: [1->3, 5->6] (bitcode=101)]
12] Current path identified as infeasible, stopping analysis
12] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
12] bl 8278
10] seti t1, 0x8278 (33400)
18] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
18] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
13] Predicates generated: [?14 = 0x82ec]
12] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
12] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4
    
```

```

16] add ?13, t2, #10
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
130] add t1, t1, t2
116] [(t1 - t2 / t1)]
145] - ?14 = [t1]
153] + ?14 = [t1 - t2]
145] - ?4 = [t1 - t2]
153] + ?4 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = ?13
153] + (t1 - t2) - t2 = ?13
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [?13 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - ?14 = [t1 - t2]
105] + ?14 = [t1 - 4]
104] - ?4 = [(t1 - t2) - t2]
105] + ?4 = [(t1 - 4) - 4]
104] - ?13 - ((t1 - t2) - t2) = 8
105] + ?13 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
122] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
129] 1 infeasible path found:
144] - [1->3, 5->6]
    
```

```

15] + ?14 = [(t1 - 4)]
16] - ?4 = [(t1 - t2) - t2]
17] + ?4 = [(t1 - 4) - 4]
18] - ?13 - ((t1 - t2) - t2) = 8
19] + ?13 - ((t1 - 4) - 4) = 8
20] - t2 = 4
21] - ?14 = [(t1 - 4)]
22] - ?4 = [(t1 - 4) - 4]
23] - ?13 - ((t1 - 4) - 4) = 8
24] bx lr
25] branch ?14
26] Predicates generated: [?0 = 0]
27] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
28] EXIT block reached
29] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
30] SMT call: UNSAT
31] [Inf. path found: [1->3, 5->6] (bitcode=101)]
32] Current path identified as infeasible, stopping analysis
33] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
34] SMT call: SAT
35] Processing BB 2 (000082e8)
36] bl 8278
37] seti t1, 0x8278 (33400)
38] + t1 = 0x8278
39] seti ?14, 0x82ec (33516)
40] + ?14 = 0x82ec
41] branch t1
42] - t1 = 0x8278
43] Predicates generated: [?14 = 0x82ec]
44] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
45] SMT call: SAT
46] Processing BB 4 (000082ec)
47] b 82f4
48] seti t1, 0x82f4 (33524)
49] + t1 = 0x82f4
50] branch t1
51] - t1 = 0x82f4

```

```

166] load ?14, t1, shift1
167] - (?14 = 0x8318 | 9->10)
168] + ?14 = [t1]
169] add t1, t1, t2
170] [(t1 - t2) / t1]
171] - ?14 = [t1]
172] + ?14 = [t1 - t2]
173] - ?4 = [(t1 - t2) - t2]
174] + ?4 = [(t1 - t2) - t2]
175] - t3 - ((t1 - t2) - t2) = 8
176] + t3 - ((t1 - t2) - t2) = 8
177] - t1 - t2 = ?13
178] + ((t1 - t2) - t2) = ?13
179] set ?13, t3
180] - ((t1 - t2) - t2) = ?13
181] + ?13 = t3
182] [?13 / t3]
183] - t3 - ((t1 - t2) - t2) = 8
184] + ?13 - ((t1 - t2) - t2) = 8
185] - ?13 = t3
186] [4 / t2]
187] - ?14 = [(t1 - t2)]
188] + ?14 = [(t1 - 4)]
189] - ?4 = [(t1 - t2) - t2]
190] + ?4 = [(t1 - 4) - 4]
191] - ?13 - ((t1 - t2) - t2) = 8
192] + ?13 - ((t1 - 4) - 4) = 8
193] - t2 = 4
194] - ?14 = [(t1 - 4)]
195] - ?4 = [(t1 - 4) - 4]
196] - ?13 - ((t1 - 4) - 4) = 8
197] bx lr
198] branch ?14
199] Predicates generated: [?0 = 0]
200] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
201] EXIT block reached
202] 1 infeasible path found:
203] - [1->3, 5->6]

```


Plan

- 1 Introduction
- 2 Problématique et contexte
- 3 Solution
- 4 Ouvertures et conclusion**

Extensions

- Thèse future dans la continuation du stage M2R, beaucoup d'extensions à faire :

Extensions

- Thèse future dans la continuation du stage M2R, beaucoup d'extensions à faire :
 - Traiter des programmes **avec boucles**
⇒ découpage du programme en partie sans boucles (ou avec boucles simples)



Extensions

- Thèse future dans la continuation du stage M2R, beaucoup d'extensions à faire :
 - Traiter des programmes **avec boucles**
⇒ découpage du programme en partie sans boucles (ou avec boucles simples)
 - Appels au solveur SMT plus intelligents



The image shows the CVC4 logo, which consists of the letters 'CVC' in a large, blue, stylized font with a 3D effect, and a red '4' to its right. In the background, there is a snippet of SMT-LIA code in a light gray font.

```
(and (or (and (= x0 y0) (=
y0 x1)) (and (= x0 z0)
x1 z0)) (or (and (= x1
y1) (= y1 z1) (and (= x2
y2) (and (= x2 z2) (= z2
x3))) (not (= x0 x3)))
```

Extensions

- Thèse future dans la continuation du stage M2R, beaucoup d'extensions à faire :
 - Traiter des programmes **avec boucles**
⇒ découpage du programme en partie sans boucles (ou avec boucles simples)
 - Appels au solveur SMT plus intelligents
 - Gérer les spécificités des types de données du langage machine

```
x = (unsigned int) y;
```

Extensions

- Thèse future dans la continuation du stage M2R, beaucoup d'extensions à faire :
 - Traiter des programmes **avec boucles**
⇒ découpage du programme en partie sans boucles (ou avec boucles simples)
 - Appels au solveur SMT plus intelligents
 - Gérer les spécificités des types de données du langage machine
 - Générer des contraintes ILP ne **suffit plus**
⇒ il faudrait faire de la **réécriture de graphe**.

Conclusion

- La recherche de chemins infaisables : un problème d'actualité

Conclusion

- La recherche de chemins infaisables : un problème d'actualité
- A l'heure actuelle, on traite déjà certaines classes de programme

Conclusion

- La recherche de chemins infaisables : un problème d'actualité
- A l'heure actuelle, on traite déjà certaines classes de programme
- Un travail qui trouve ses fondations dans l'interprétation abstraite

Conclusion

- La recherche de chemins infaisables : un problème d'actualité
- A l'heure actuelle, on traite déjà certaines classes de programme
- Un travail qui trouve ses fondations dans l'interprétation abstraite
- À poursuivre en thèse...

