

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

Candidat
Jordy RUIZ

Encadrant
Hugues CASSE

23 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)

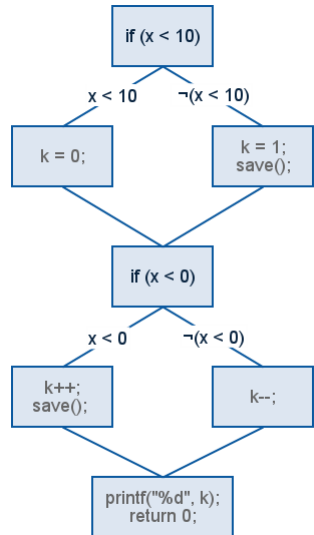
- But : surestimer le temps d'exécution d'une partie de programme
- Exemples
 - Le frein de voiture s'activera au pire 50ms après la commande
 - L'algorithme prendra une décision en moins d'1s
 - ...
- Systèmes temps-réel critiques : les mesures ne suffisent pas, il faut une **preuve** !

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

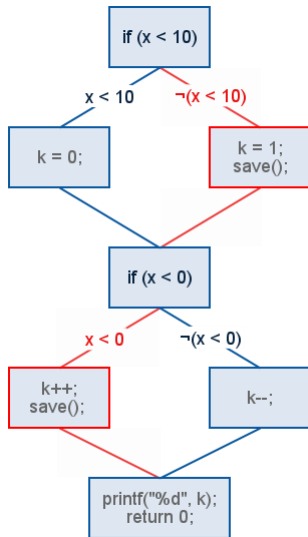
Recherche de chemins infaisables

- Graphe de flot de contrôle



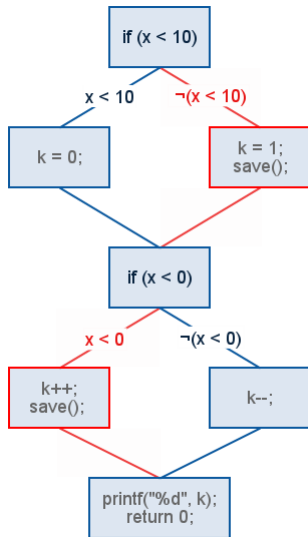
Recherche de chemins infaisables

- 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
 $n_{(x < 0)} \leq n_{(x < 10)}$



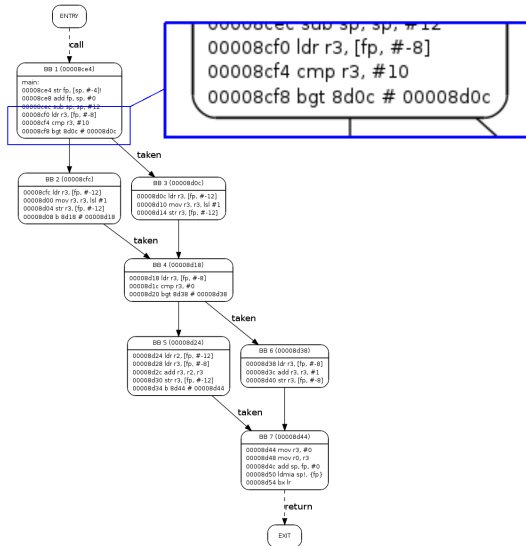
Choix du solveur SMT

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

- Open-source, licence très libre
- 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

- Une trentaine d'instructions sémantiques
- On fait de l'analyse abstraite : on met à \top quand on ne sait pas gérer
 - \implies instruction SCRATCH
 - \implies Il s'agit de toujours rester **correct**

Plan

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

Représentation des prédicats

- **Prédicat** : Expression \times Comparateur \times Expression
- **Expression** :
 - Constante($k \in \mathbb{Z}$)
 - Variable($id \in \mathbb{Z}$)
 - Memoire($addr \in \mathbb{Z}$)
 - ExprArithmétique
- **ExprArithmétique** : Expression \times Operateur \times Expression

```

171] + ?14 = [t1 - 4]
174] - ?4 = [(t1 - t2) - t2]
175] + ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - 4) - 4) = 8
176] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
176] branch ?14
173] Predicates generated: [?0 = 0]
172] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
172] EXIT block reached
172] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
176] SMT call: UNSAT
173] [Inf. path found: [1->3, 5->6] (bitcode=101)]
172] Current path identified as infeasible, stopping analysis
172] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
176] SMT call: SAT
176] Processing BB 2 (000082e8)
22] bl 8278
176] seti t1, 0x8278 (33400)
178] + t1 = 0x8278
176] seti ?14, 0x82ec (33516)
178] + ?14 = 0x82ec
176] branch t1
176] - t1 = 0x8278
173] Predicates generated: [?14 = 0x82ec]
172] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
176] SMT call: SAT
176] Processing BB 4 (000082ec)
22] b 82f4
176] seti t1, 0x82f4 (33524)
178] + t1 = 0x82f4
176] branch t1
176] - t1 = 0x82f4

```

```

176] load ?14, t1, imm0
177] - (?14 = 0x8318 | 9->10)
178] + ?14 = [t1]
176] add t1, t1, t2
176] [t1 - t2 / t1]
174] - ?14 = [t1]
175] + ?14 = [t1 - t2]
174] - ?4 = [t1 - t2]
175] + ?4 = [(t1 - t2) - t2]
174] - t3 - (t1 - t2) = 8
175] + t3 - ((t1 - t2) - t2) = 8
174] - t1 - t2 = ?13
175] + (t1 - t2) - t2 = ?13
173] set ?13, t3
173] - (t1 - t2) - t2 = ?13
178] + ?13 = t3
176] [?13 / t3]
174] - t3 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - t2) - t2) = 8
176] - ?13 = t3
176] [4 / t2]
174] - ?14 = [t1 - t2]
175] + ?14 = [t1 - 4]
174] - ?4 = [(t1 - t2) - t2]
175] + ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - 4) - 4) = 8
176] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
176] branch ?14
173] Predicates generated: [?0 = 0]
172] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
172] EXIT block reached
29] 1 infeasible path found:
44] - [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
22] 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
16] [Inf. path found: [1->3, 5->6] (bitcode=101)]
16] 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)
22] 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)
22] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

15] + ?14 = [t1 - 4]
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]

```

```

171] + ?14 = [(t1 - 4)
184] - ?4 = [(t1 - t2) - t2]
195] + ?4 = [(t1 - 4) - 4]
204] - ?13 - ((t1 - t2) - t2) = 8
205] + ?13 - ((t1 - 4) - 4) = 8
209] - t2 = 4
214] - ?14 = [t1 - 4]
214] - ?4 = [(t1 - 4) - 4]
214] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
201] branch ?14
203] Predicates generated: [?0 = 0]
202] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
202] EXIT block reached
202] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
206] SMT call: UNSAT
203] [Inf. path found: [1->3, 5->6] (bitcode=101)]
202] Current path identified as infeasible, stopping analysis
202] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
206] SMT call: SAT
206] Processing BB 2 (000082e8)
22] bl 8278
209] seti t1, 0x8278 (33400)
208] + t1 = 0x8278
210] seti ?14, 0x82ec (33516)
208] + ?14 = 0x82ec
209] branch t1
209] - t1 = 0x8278
203] Predicates generated: [?14 = 0x82ec]
202] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
206] SMT call: SAT
206] Processing BB 4 (000082ec)
22] b 82f4
209] seti t1, 0x82f4 (33524)
208] + t1 = 0x82f4
209] branch t1
209] - t1 = 0x82f4

```

```

199] load ?14, t1, imm0
117] - (?14 = 0x8318 | 9->10)
188] + ?14 = [t1]
190] 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
22] bx lr
130] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
29] 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
22] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
12] EXIT block reached
14] 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)
22] 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)
22] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

15] add ?14, t1, #16
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
22] 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
10] Processing BB 2 (000082e8)
22] b 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
12] Processing BB 4 (000082ec)
22] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

15] load ?14, t1, 4116
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
11] 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
11] 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

```

```

15] load ?14, t1, imm0
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
12] 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
21] bx lr
20] branch ?14
22] Predicates generated: [?0 = 0]
22] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
22] EXIT block reached
22] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
26] SMT call: UNSAT
28] [Inf. path found: [1->3, 5->6] (bitcode=101)]
22] Current path identified as infeasible, stopping analysis
22] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
26] SMT call: SAT
26] Processing BB 2 (000082e8)
27] bl 8278
20] seti t1, 0x8278 (33400)
21] + t1 = 0x8278
20] seti ?14, 0x82ec (33516)
21] + ?14 = 0x82ec
20] branch t1
21] - t1 = 0x8278
23] Predicates generated: [?14 = 0x82ec]
22] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
26] SMT call: SAT
26] Processing BB 4 (000082ec)
27] b 82f4
20] seti t1, 0x82f4 (33524)
21] + t1 = 0x82f4
20] branch t1
21] - t1 = 0x82f4

```

```

15] load ?14, t1, 0x82ec
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
22] bx lr
230] branch ?14
103] Predicates generated: [?0 = 0]
102] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
152] EXIT block reached
229] 1 infeasible path found:
244] - [1->3, 5->6]

```



```

171] + ?14 = [t1 - 4]
174] - ?4 = [(t1 - t2) - t2]
175] + ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - 4) - 4) = 8
176] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
176] branch ?14
173] Predicates generated: [?0 = 0]
172] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
172] EXIT block reached
172] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
176] SMT call: UNSAT
173] [Inf. path found: [1->3, 5->6] (bitcode=101)]
172] Current path identified as infeasible, stopping analysis
172] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
176] SMT call: SAT
176] Processing BB 2 (000082e8)
22] bl 8278
176] seti t1, 0x8278 (33400)
178] + t1 = 0x8278
176] seti ?14, 0x82ec (33516)
178] + ?14 = 0x82ec
176] branch t1
176] - t1 = 0x8278
173] Predicates generated: [?14 = 0x82ec]
172] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
176] SMT call: SAT
176] Processing BB 4 (000082ec)
22] b 82f4
176] seti t1, 0x82f4 (33524)
178] + t1 = 0x82f4
176] branch t1
176] - t1 = 0x82f4

```

```

176] load ?14, t1, imm0
177] - (?14 = 0x8318 | 9->10)
178] + ?14 = [t1]
176] add t1, t1, t2
176] [(t1 - t2 / t1]
174] - ?14 = [t1]
175] + ?14 = [t1 - t2]
174] - ?4 = [t1 - t2]
175] + ?4 = [(t1 - t2) - t2]
174] - t3 - (t1 - t2) = 8
175] + t3 - ((t1 - t2) - t2) = 8
174] - t1 - t2 = ?13
175] + (t1 - t2) - t2 = ?13
176] set ?13, t3
173] - (t1 - t2) - t2 = ?13
178] + ?13 = t3
176] [?13 / t3]
174] - t3 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - t2) - t2) = 8
176] - ?13 = t3
176] [4 / t2]
174] - ?14 = [t1 - t2]
175] + ?14 = [t1 - 4]
174] - ?4 = [(t1 - t2) - t2]
175] + ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - 4) - 4) = 8
176] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
176] branch ?14
173] Predicates generated: [?0 = 0]
172] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
172] EXIT block reached
29] 1 infeasible path found:
44] - [1->3, 5->6]

```

```

15] + 714 = [t1 - 4]
14] - 74 = [(t1 - t2) - t2]
15] + 74 = [(t1 - 4) - 4]
14] - 713 - ((t1 - t2) - t2) = 8
15] + 713 - ((t1 - 4) - 4) = 8
10] - t2 = 4
14] - 714 = [t1 - 4]
14] - 74 = [(t1 - 4) - 4]
14] - 713 - ((t1 - 4) - 4) = 8
22] 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)
22] bl 8278
10] seti t1, 0x8278 (33400)
14] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
14] + 714 = 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)
22] b 82f4
10] seti t1, 0x82f4 (33524)
14] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

15] load ?14, t1, imm0
117] - (?14 = 0x8318 | 9->10)
188] + 714 = [t1]
130] add t1, t1, t2
116] [t1 - t2 / t1]
145] - 714 = [t1]
153] + 714 = [t1 - t2]
145] - 74 = [t1 - t2]
153] + 74 = [(t1 - t2) - t2]
145] - t3 - (t1 - t2) = 8
153] + t3 - ((t1 - t2) - t2) = 8
145] - t1 - t2 = 713
153] + (t1 - t2) - t2 = 713
130] set ?13, t3
131] - (t1 - t2) - t2 = ?13
188] + ?13 = t3
100] [713 / t3]
104] - t3 - ((t1 - t2) - t2) = 8
105] + 713 - ((t1 - t2) - t2) = 8
160] - ?13 = t3
100] [4 / t2]
104] - 714 = [t1 - t2]
105] + 714 = [t1 - 4]
104] - 74 = [(t1 - t2) - t2]
105] + 74 = [(t1 - 4) - 4]
104] - 713 - ((t1 - t2) - t2) = 8
105] + 713 - ((t1 - 4) - 4) = 8
160] - t2 = 4
174] - 714 = [t1 - 4]
174] - 74 = [(t1 - 4) - 4]
174] - 713 - ((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
22] bx lr
10] branch ?14
10] Predicates generated: [?0 = 0]
10] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
10] EXIT block reached
10] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
10] SMT call: UNSAT
10] [Inf. path found: [1->3, 5->6] (bitcode=101)]
10] Current path identified as infeasible, stopping analysis
10] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
10] SMT call: SAT
10] Processing BB 2 (000082e8)
10] bl 8278
10] seti t1, 0x8278 (33400)
10] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
10] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
10] Predicates generated: [?14 = 0x82ec]
10] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
10] SMT call: SAT
10] Processing BB 4 (000082ec)
10] b 82f4
10] seti t1, 0x82f4 (33524)
10] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

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)
102] 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

```

```

15] load ?14, t1, 4116
16] - (?14 = 0x8318 | 9->10)
17] + ?14 = [t1]
18] add t1, t1, t2
19] [(t1 - t2 / t1]
20] - ?14 = [t1]
21] + ?14 = [t1 - t2]
22] - ?4 = [t1 - t2]
23] + ?4 = [(t1 - t2) - t2]
24] - t3 - (t1 - t2) = 8
25] + t3 - ((t1 - t2) - t2) = 8
26] - t1 - t2 = ?13
27] + (t1 - t2) - t2 = ?13
28] set ?13, t3
29] - (t1 - t2) - t2 = ?13
30] + ?13 = t3
31] [?13 / t3]
32] - t3 - ((t1 - t2) - t2) = 8
33] + ?13 - ((t1 - t2) - t2) = 8
34] - ?13 = t3
35] [4 / t2]
36] - ?14 = [t1 - t2]
37] + ?14 = [t1 - 4]
38] - ?4 = [(t1 - t2) - t2]
39] + ?4 = [(t1 - 4) - 4]
40] - ?13 - ((t1 - t2) - t2) = 8
41] + ?13 - ((t1 - 4) - 4) = 8
42] - t2 = 4
43] - ?14 = [t1 - 4]
44] - ?4 = [(t1 - 4) - 4]
45] - ?13 - ((t1 - 4) - 4) = 8
46] bx lr
47] branch ?14
48] Predicates generated: [?0 = 0]
49] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
50] EXIT block reached
51] 1 infeasible path found:
52] - [1->3, 5->6]

```

```

171] + ?14 = [t1 - 4]
174] - ?4 = [(t1 - t2) - t2]
175] + ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - 4) - 4) = 8
176] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
176] branch ?14
173] Predicates generated: [?0 = 0]
172] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
172] EXIT block reached
172] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
176] SMT call: UNSAT
173] [Inf. path found: [1->3, 5->6] (bitcode=101)]
172] Current path identified as infeasible, stopping analysis
172] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
176] SMT call: SAT
176] Processing BB 2 (000082e8)
22] bl 8278
176] seti t1, 0x8278 (33400)
178] + t1 = 0x8278
176] seti ?14, 0x82ec (33516)
178] + ?14 = 0x82ec
176] branch t1
176] - t1 = 0x8278
173] Predicates generated: [?14 = 0x82ec]
172] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
176] SMT call: SAT
176] Processing BB 4 (000082ec)
22] b 82f4
176] seti t1, 0x82f4 (33524)
178] + t1 = 0x82f4
176] branch t1
176] - t1 = 0x82f4

```

```

176] load ?14, t1, imm0
177] - (?14 = 0x8318 | 9->10)
178] + ?14 = [t1]
176] add t1, t1, t2
176] [(t1 - t2 / t1]
174] - ?14 = [t1]
175] + ?14 = [t1 - t2]
174] - ?4 = [t1 - t2]
175] + ?4 = [(t1 - t2) - t2]
174] - t3 - ((t1 - t2) - t2) = 8
175] + t3 - ((t1 - t2) - t2) = 8
174] - t1 - t2 = ?13
175] + (t1 - t2) - t2 = ?13
176] set ?13, t3
173] - (t1 - t2) - t2 = ?13
178] + ?13 = t3
176] [?13 / t3]
174] - t3 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - t2) - t2) = 8
176] - ?13 = t3
176] [4 / t2]
174] - ?14 = [t1 - t2]
175] + ?14 = [t1 - 4]
174] - ?4 = [(t1 - t2) - t2]
175] + ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - t2) - t2) = 8
175] + ?13 - ((t1 - 4) - 4) = 8
176] - t2 = 4
174] - ?14 = [t1 - 4]
174] - ?4 = [(t1 - 4) - 4]
174] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
176] branch ?14
173] Predicates generated: [?0 = 0]
172] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
172] EXIT block reached
29] 1 infeasible path found:
44] - [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
22] bx lr
10] branch ?14
18] Predicates generated: [?0 = 0]
22] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
22] EXIT block reached
22] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
16] SMT call: UNSAT
18] [Inf. path found: [1->3, 5->6] (bitcode=101)]
22] Current path identified as infeasible, stopping analysis
22] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
16] SMT call: SAT
16] Processing BB 2 (000082e8)
22] bl 8278
10] seti t1, 0x8278 (33400)
18] + t1 = 0x8278
10] seti ?14, 0x82ec (33516)
18] + ?14 = 0x82ec
10] branch t1
10] - t1 = 0x8278
18] Predicates generated: [?14 = 0x82ec]
22] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
16] SMT call: SAT
16] Processing BB 4 (000082ec)
22] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

10] load ?14, t1, imm0
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
22] 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)
14] 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)
14] SMT call: SAT
16] Processing BB 2 (000082e8)
22] 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)
14] SMT call: SAT
16] Processing BB 4 (000082ec)
22] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

15] add ?14, t1, #16
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
22] bx lr
10] branch ?14
13] Predicates generated: [?0 = 0]
12] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
22] 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)
22] 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)
22] b 82f4
10] seti t1, 0x82f4 (33524)
18] + t1 = 0x82f4
10] branch t1
10] - t1 = 0x82f4

```

```

15] load ?14, t1, imm0
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]

```



```

171] + ?14 = [(t1 - 4)
184] - ?4 = [(t1 - t2) - t2]
195] + ?4 = [(t1 - 4) - 4]
204] - ?13 - ((t1 - t2) - t2) = 8
205] + ?13 - ((t1 - 4) - 4) = 8
209] - t2 = 4
214] - ?14 = [t1 - 4]
214] - ?4 = [(t1 - 4) - 4]
214] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
20] branch ?14
203] Predicates generated: [?0 = 0]
202] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
202] EXIT block reached
202] Processing Edge: BB 5 (000082f4) -> BB 6 (000082fc) (not taken)
206] SMT call: UNSAT
203] [Inf. path found: [1->3, 5->6] (bitcode=101)]
202] Current path identified as infeasible, stopping analysis
202] Processing Edge: BB 1 (000082d8) -> BB 2 (000082e8) (not taken)
206] SMT call: SAT
206] Processing BB 2 (000082e8)
22] bl 8278
20] seti t1, 0x8278 (33400)
208] + t1 = 0x8278
210] seti ?14, 0x82ec (33516)
208] + ?14 = 0x82ec
20] branch t1
209] - t1 = 0x8278
203] Predicates generated: [?14 = 0x82ec]
202] Processing Edge: BB 2 (000082e8) -> BB 4 (000082ec) (not taken)
206] SMT call: SAT
206] Processing BB 4 (000082ec)
22] b 82f4
20] seti t1, 0x82f4 (33524)
208] + t1 = 0x82f4
20] branch t1
209] - t1 = 0x82f4

```

```

200] load ?14, t1, imm0
217] - (?14 = 0x8318 | 9->10)
208] + ?14 = [t1]
230] add t1, t1, t2
216] [(t1 - t2 / t1]
245] - ?14 = [t1]
253] + ?14 = [t1 - t2]
245] - ?4 = [t1 - t2]
253] + ?4 = [(t1 - t2) - t2]
245] - t3 - ((t1 - t2) - t2) = 8
253] + t3 - ((t1 - t2) - t2) = 8
245] - t1 - t2 = ?13
253] + (t1 - t2) - t2 = ?13
230] set ?13, t3
231] - (t1 - t2) - t2 = ?13
208] + ?13 = t3
200] [?13 / t3]
204] - t3 - ((t1 - t2) - t2) = 8
205] + ?13 - ((t1 - t2) - t2) = 8
260] - ?13 = t3
200] [4 / t2]
204] - ?14 = [t1 - t2]
205] + ?14 = [t1 - 4]
204] - ?4 = [(t1 - t2) - t2]
205] + ?4 = [(t1 - 4) - 4]
204] - ?13 - ((t1 - t2) - t2) = 8
205] + ?13 - ((t1 - 4) - 4) = 8
260] - t2 = 4
214] - ?14 = [t1 - 4]
214] - ?4 = [(t1 - 4) - 4]
214] - ?13 - ((t1 - 4) - 4) = 8
22] bx lr
230] branch ?14
203] Predicates generated: [?0 = 0]
202] Processing Edge: BB 10 (00008318) -> EXIT (virtual)
202] EXIT block reached
229] 1 infeasible path found:
244] - [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



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...

