

Opaque Predicates Detection by Abstract Interpretation

Mila Dalla Preda and Roberto Giacobazzi

University of Verona, Italy

Matias Madou* and Koen De Bosschere

Ghent University, Belgium



Motivation

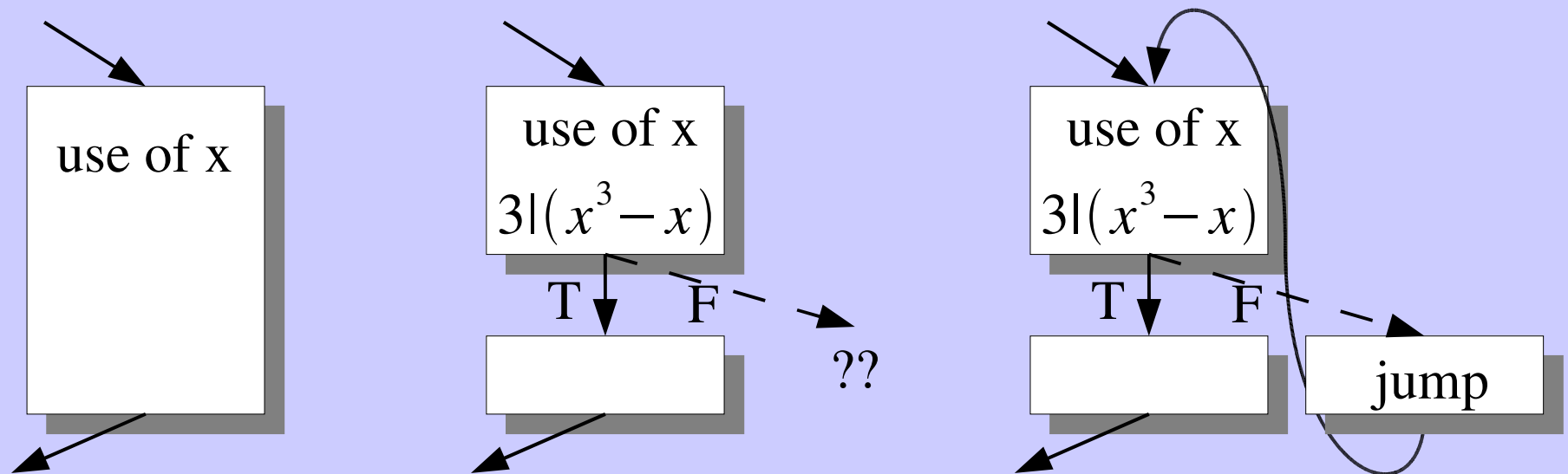
- Opaque predicates are used to protect software (code obfuscation and software watermarking)
- Goal: describe a group of avoidable opaque predicates. They are easy to break!

Contributions

- Three approaches to detect opaque predicates
 - based on dynamic information
 - based on static/dynamic information
 - based on formal program semantics and semantics approximation by abstract interpretation
- By use of abstract interpretation: $\forall x \in \mathbb{Z} : n \mid f(x)$
(f returns a multiple of n)
are easy to break

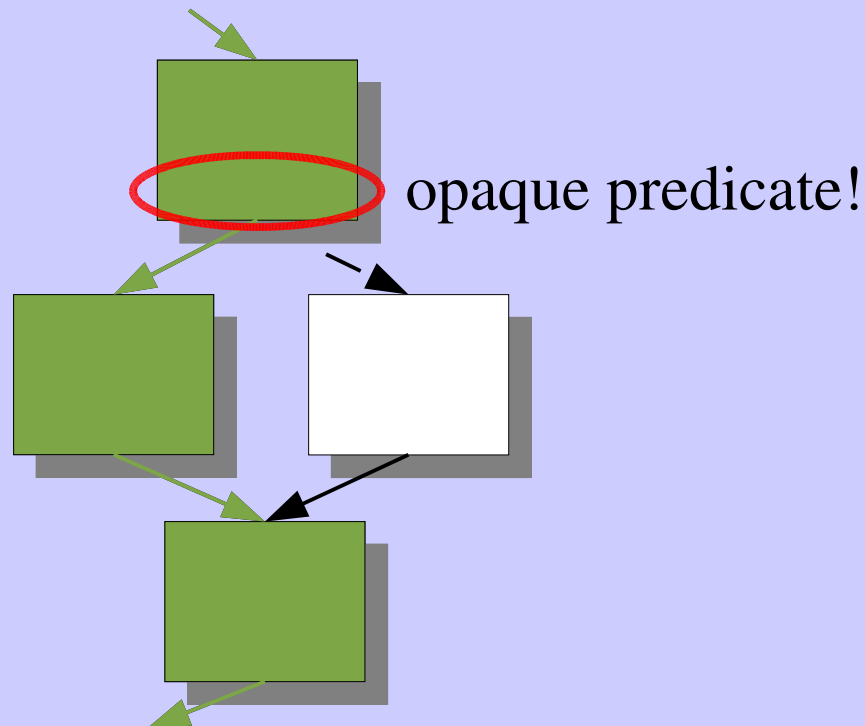
Opaque Predicates

- Def: A predicate is opaque if its value is known a priori to a program transformation, while it is difficult for an attacker to deduce it.
- Goal: Introducing fake paths
- Example: $\forall x \in \mathbb{Z} : 3 \mid (x^3 - x)$



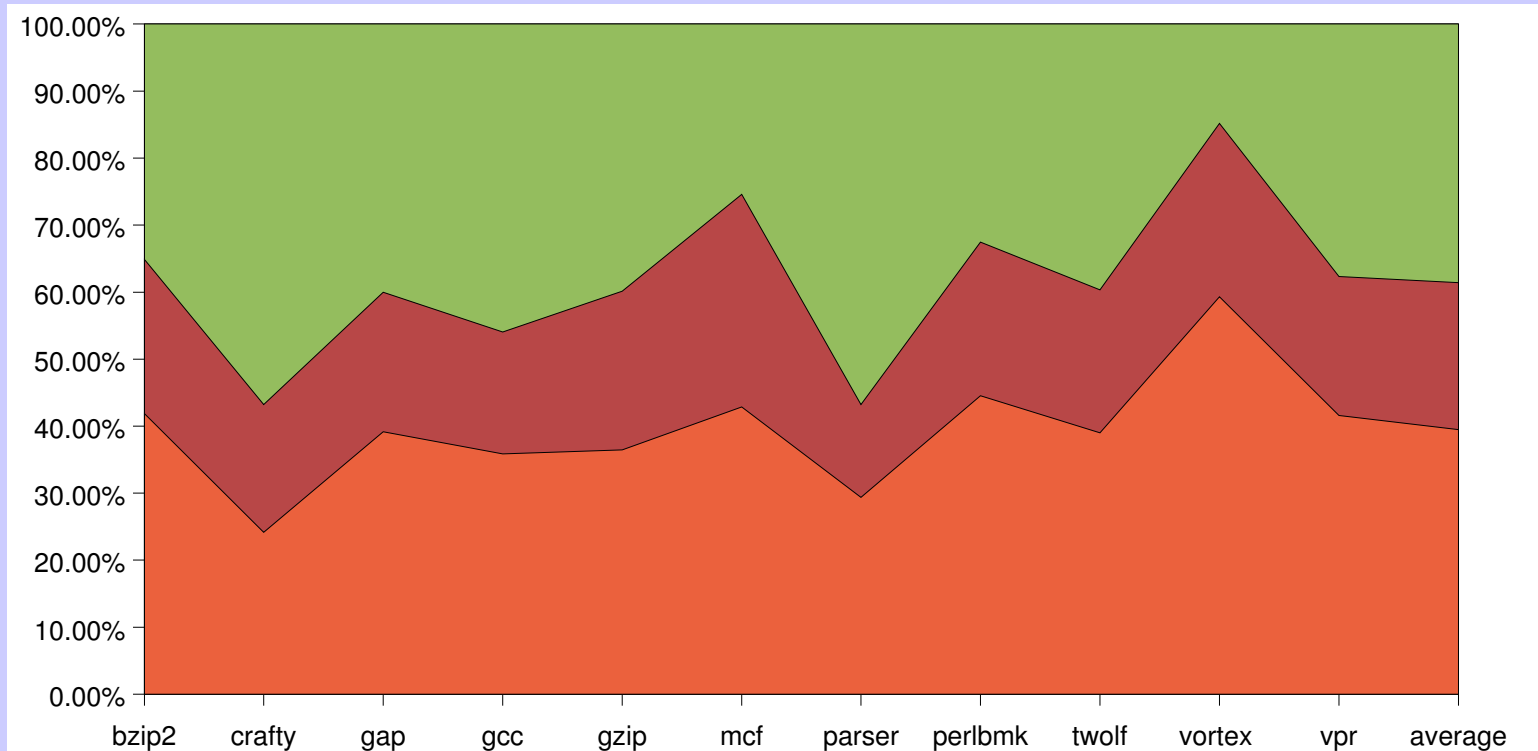
(1) Dynamic Attack

- Use only dynamic information



Problem: Attacker has a limited number of different inputs \Rightarrow false negatives

(1) Dynamic Attack: Results



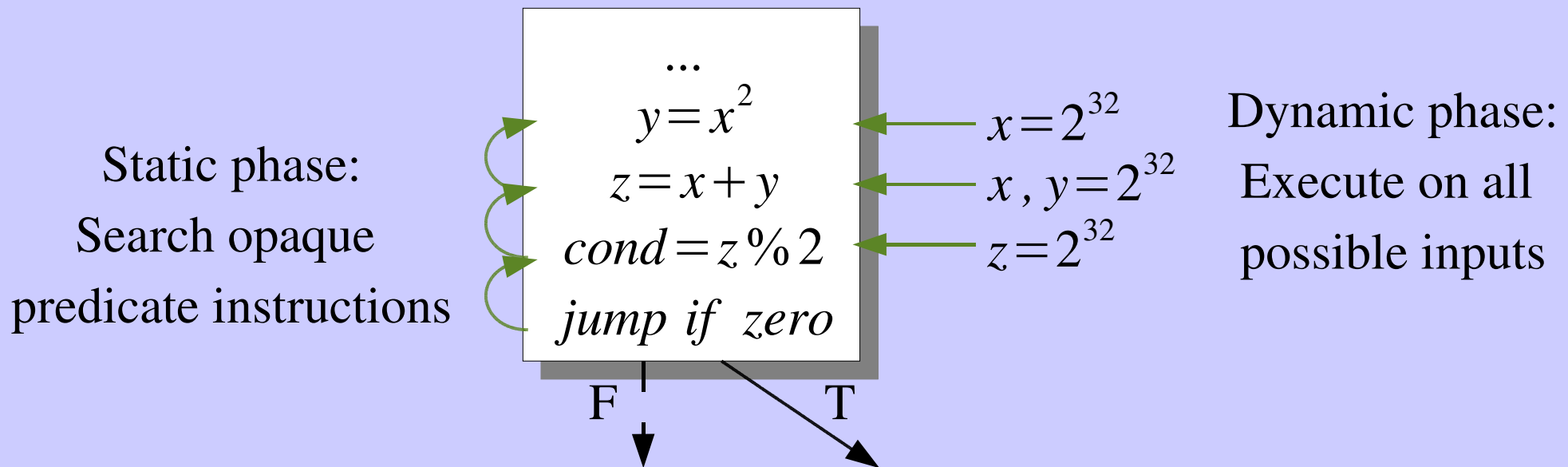
■ % both ways ■ % both jump ■ % both fallthrough

Conclusion: too imprecise

(2) Brute Force Attack

- Static/Dynamic brute force attack on assembly code
- Example: $\forall x \in \mathbb{Z} : 2 \mid (x^2 + x)$

Into elementary functions: $x + y$ and x^2



(2) Brute Force Attack: Results

- Test-case: $2 | (x + x)$
- 16-bit x86 environment: 3 instructions
- 1.6GHz Pentium M Processor
- Static phase by hand;
only dynamic phase; 2^{16} inputs: 8.83 seconds
- Conclusion: precise; but time consuming

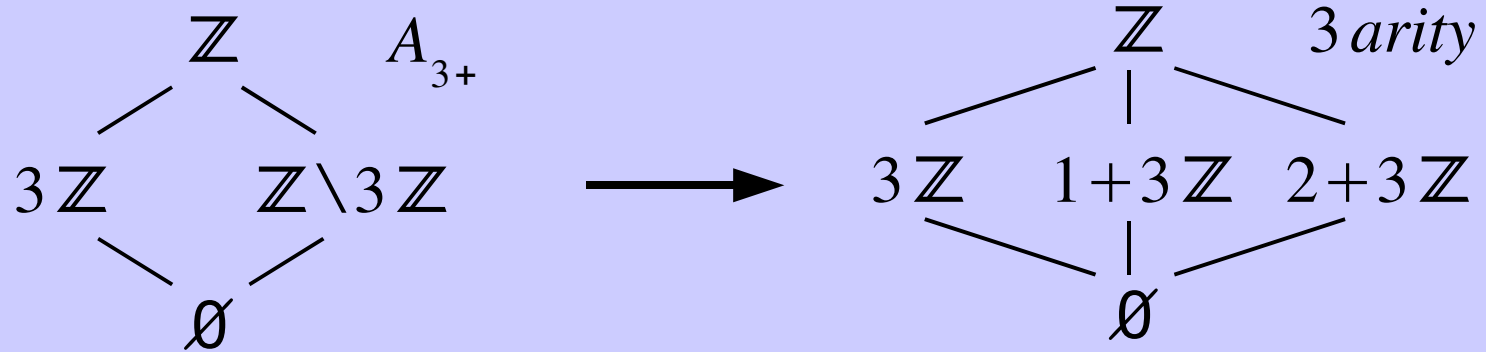
(3) Abstract Interpretation

- Concentrate on a specific group: $\forall x \in \mathbb{Z} : n \mid f(x)$
- Simple examples: $\forall x \in \mathbb{Z} : 2 \mid (x^2 + x)$ and $\forall x \in \mathbb{Z} : 3 \mid (x^3 - x)$
- Complex example: $\forall x \in \mathbb{Z}^+ : 24 \mid (2 \cdot 7^x + 3 \cdot 4^x - 5)$
- Abstract domains: $Sign = \{ \mathbb{Z}, \mathbb{Z}_{\geq 0}, \mathbb{Z}_{\leq 0}, 0, \emptyset \}$
 $Parity = \{ \mathbb{Z}, even, odd, \emptyset \}$
- Goal: Find the correct abstract domain that breaks a given opaque predicate

(3) Abstract Interpretation: Theory

- Find an abstract domain which breaks: $\forall x \in \mathbb{Z} : 3 \mid (x^3 - x)$

- Start:



- Into elementary functions: $f(x) = x^3 - x = h(g_1(x), g_2(x))$

$$h(x, y) = x - y$$

$$g_1(x) = x^3, g_2(x) = x$$

$$F^\#(3\mathbb{Z}) = 3\mathbb{Z}$$

$$F^\#(\mathbb{Z} \setminus 3\mathbb{Z}) = \mathbb{Z} \leftarrow F(x) = \{y^3 - z \mid y, z \in X\}$$

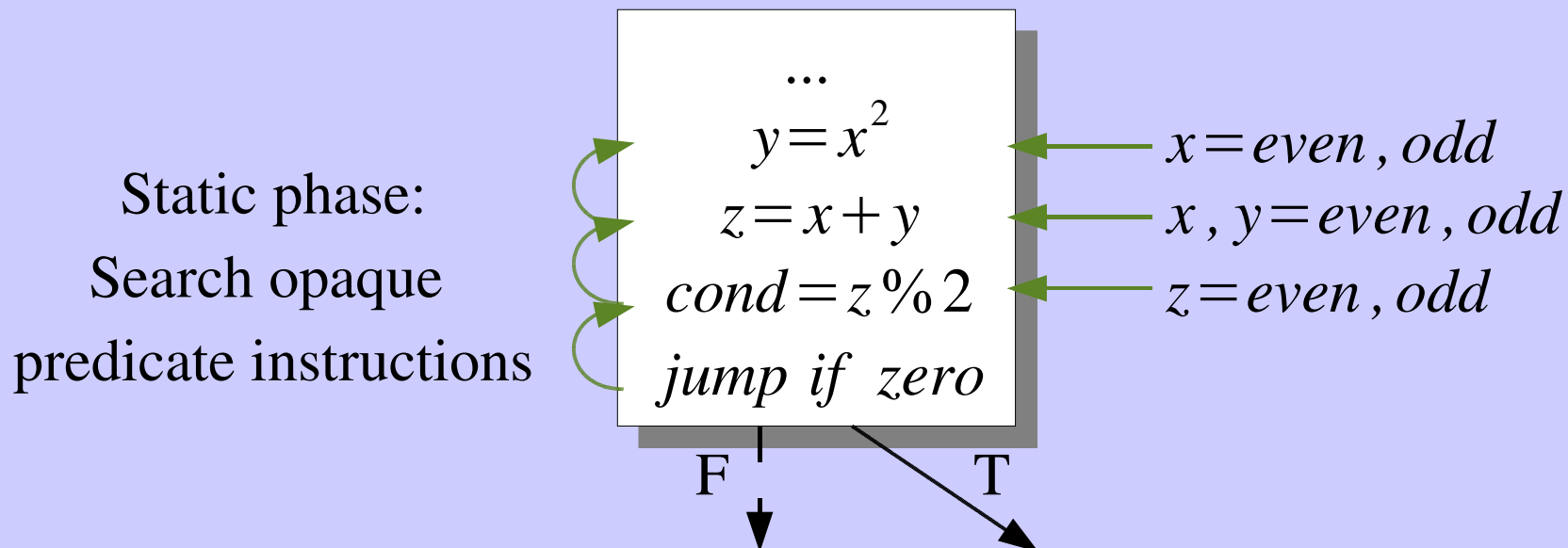
$AT_{A_{3+}}^{F^\#}$ is sound but not complete

(3) Abstract Interpretation: Practice

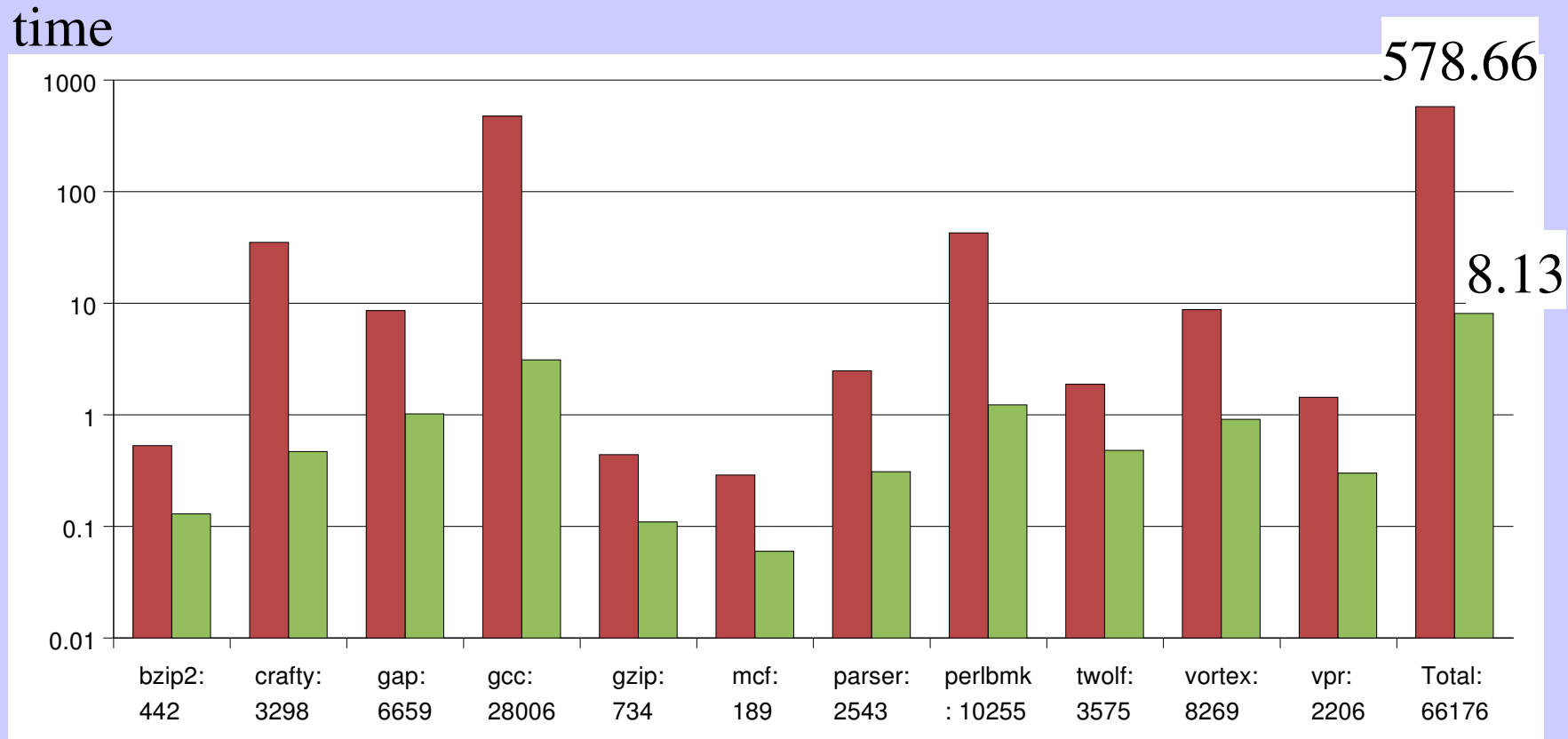
- Loco: x86 obfuscator/deobfuscator
- Implementation: $Parity = \{ \mathbb{Z}, even, odd, \emptyset \}$
- SPECInt 2000 benchmarks obfuscated with:
 $\forall x \in \mathbb{Z} : 2 \mid (x^2 + x)$ and $\forall x \in \mathbb{Z} : 2 \mid (x + x)$
- Problem: What is the start of the opaque predicate??

(3) Abstract Interpretation: Practice

- Similar to the static part of the Brute Force Attack: Going back into the code
- Example: $\forall x \in \mathbb{Z} : 2 \mid (x^2 + x)$
- Domain: $Parity = \{ \mathbb{Z}, even, odd, \emptyset \}$



(3) Abstract Interpretation: Results



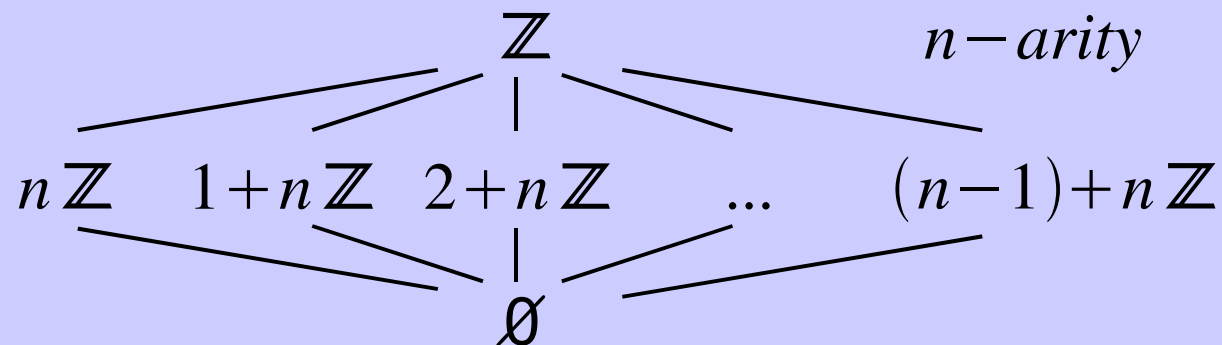
■ time to obfuscate ■ time to defobfuscate

Recall: brute force attack; 8.83 sec to deobfuscate one 16-bit opaque predicate

Designing domains

- Completeness domain refinement

$$\forall x \in \mathbb{Z} : n \mid f(x)$$



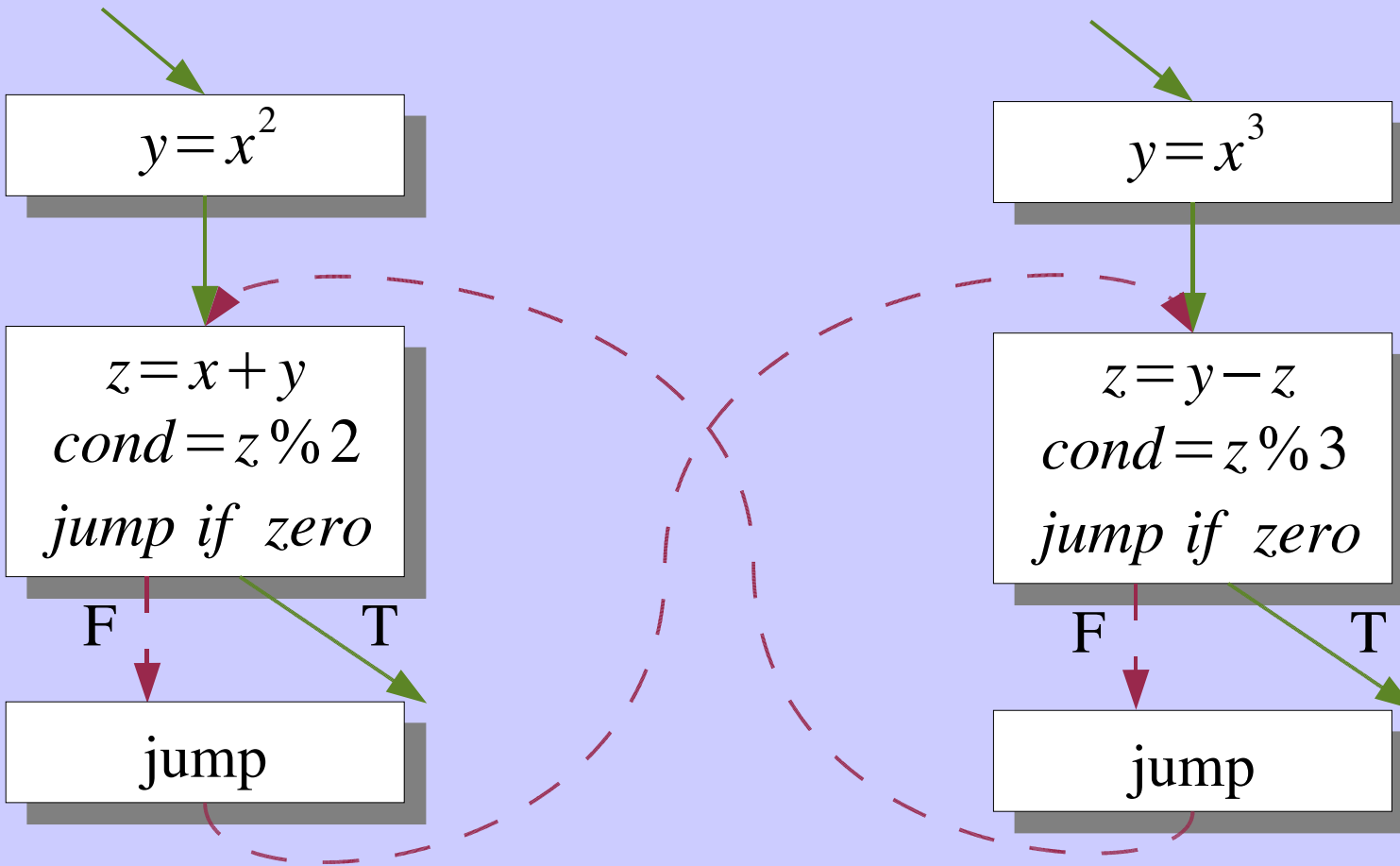
Future Work: Abstract Interpretation

- Apply abstract Interpretation on other opaque predicates
- Simple example: $\forall x \in \mathbb{Z} : x^2 \geq 0$
- Abstract domain: $Sign = \{ \mathbb{Z}, \mathbb{Z}_{\geq 0}, \mathbb{Z}_{\leq 0}, 0, \emptyset \}$
- Other: Is it possible to break $\forall x, y \in \mathbb{Z} : 7y^2 - 1 \neq x^2$ by use of abstract interpretation??

Future Work: Interaction, theory

$$\forall x \in \mathbb{Z} : 2 \mid (x^2 + x)$$

$$\forall x \in \mathbb{Z} : 3 \mid (x^3 - x)$$



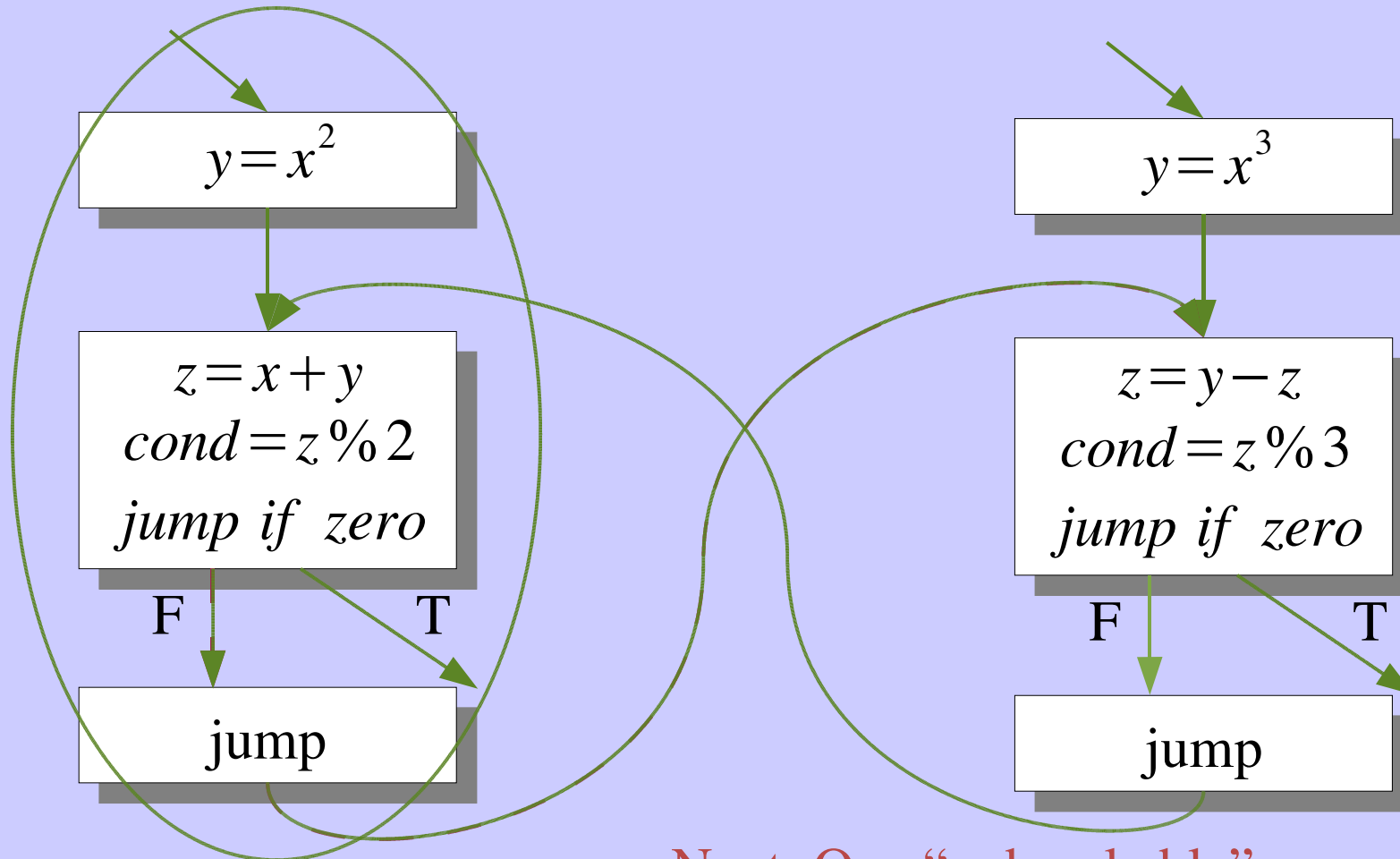
$$2 \text{ arity} = \{ \mathbb{Z}, 1 + 2\mathbb{Z}, 2\mathbb{Z}, \emptyset \}$$

$$3 \text{ arity} = \{ \mathbb{Z}, 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}, \emptyset \}$$

Future Work: Interaction, practice

$$\forall x \in \mathbb{Z} : 2 \mid (x^2 + x)$$

$$\forall x \in \mathbb{Z} : 3 \mid (x^3 - x)$$



$$2\text{arity} = \{ \mathbb{Z}, 1 + 2\mathbb{Z}, 2\mathbb{Z}, \emptyset \}$$

Next: One “unbreakable” opaque predicate protects all “weak” opaque predicates

Questions?

Presentation: <http://www.madou.net>