C32SAT: Checking C Expressions

Robert Brummayer and Armin Biere

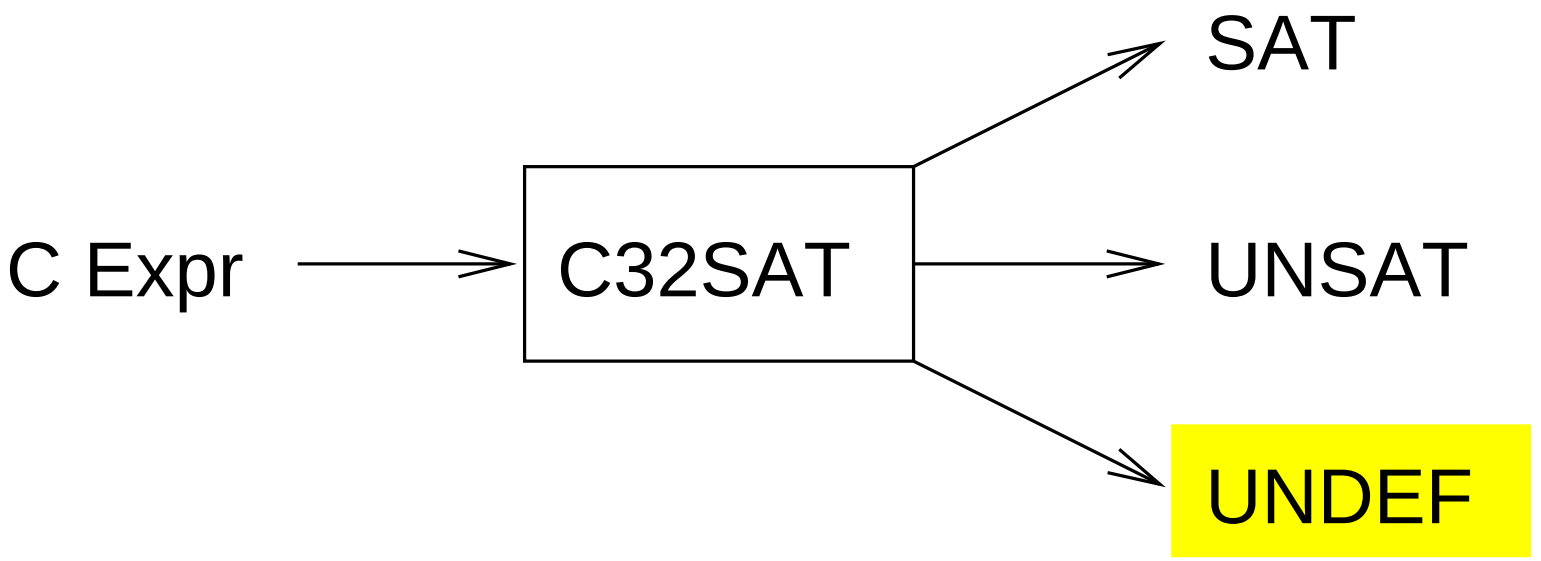
Institute for Formal Models and Verification
Johannes Kepler University Linz, Austria

CAV'07

Berlin

Session X: Constraints and Decisions
July 6, 2007

R. Brummayer, FMV, JKU Linz



Undefinedness in C

R. Brummayer, FMV, JKU Linz

- Undefined behavior upon
  - Overflow
  - Division by zero
  - Shift by a negative integer
  - Shift by an integer $\geq$ bit width
  - ...
- Semantics depend on the compiler
- Portability and security issues

Addition Overflow

R. Brummayer, FMV, JKU Linz

$$x + y$$

0	1	1	1	1	1	1	1	$= 127$

$+$

0	0	0	0	0	0	0	1	$= 1$

$=$

1	0	0	0	0	0	0	0	$= -128$

Division Overflow

R. Brummayer, FMV, JKU Linz

```
y != 0 && x / y
```

Division Overflow

R. Brummayer, FMV, JKU Linz

```
y != 0 && x / y
```

1	0	0	0	0	0	0	0	$= -128$

$/$

1	1	1	1	1	1	1	1	$= -1$

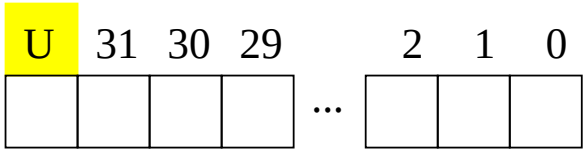
$=$

1	0	0	0	0	0	0	0	$= -128$

Internal insights

R. Brummayer, FMV, JKU Linz

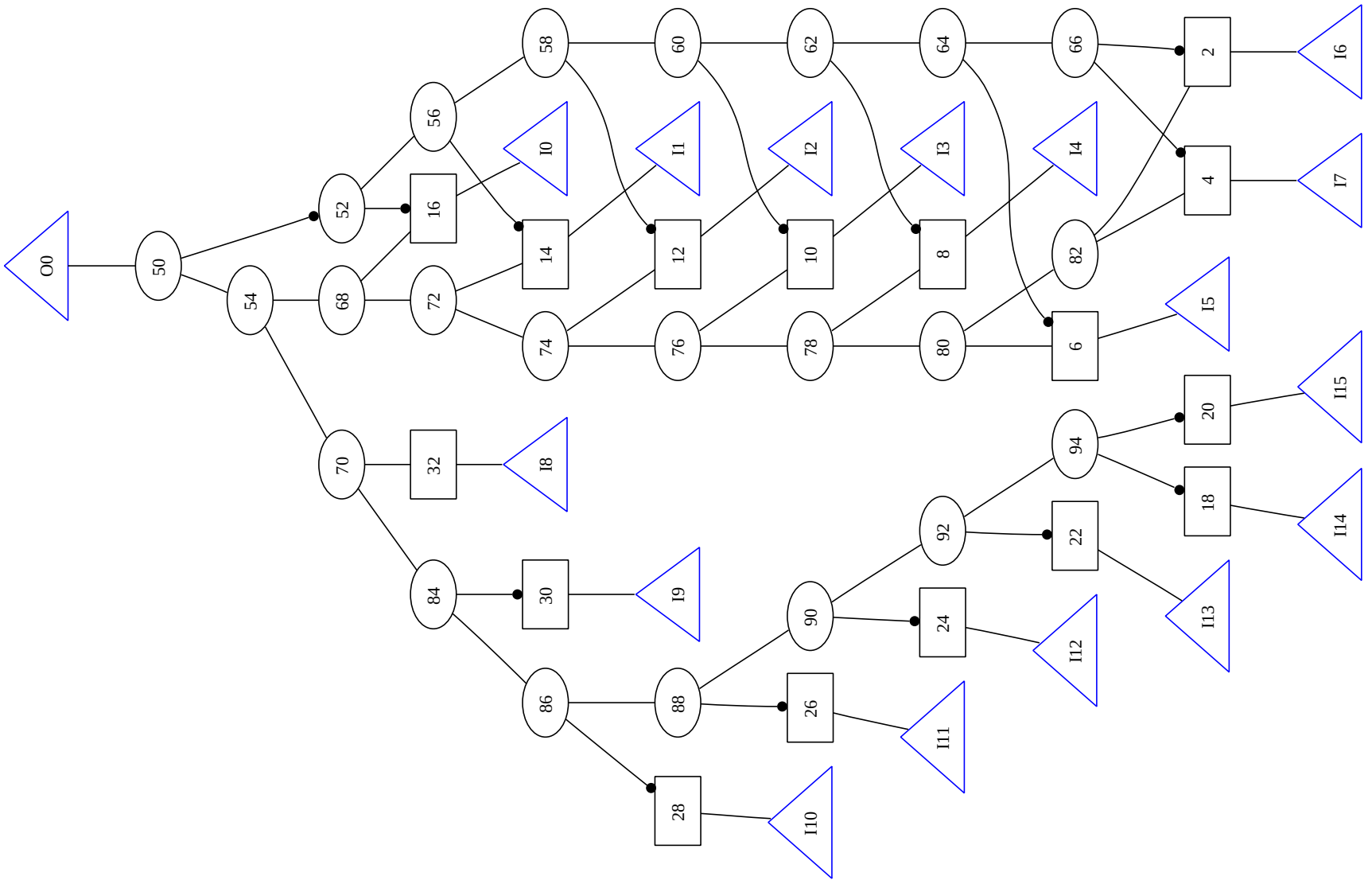
- Internal representation by vectors of And-Inverter Graphs (AIGs)
- Functional instead of relational representation
- One additional AIG per AIG vector represents “undefinedness”



- Expr. is undefined if some sub-expr. is undefined (except short circuit)
- Bit blasting to SAT solver (PicoSAT)

Division Overflow AIG (AIGER Format, 8 bits)

R. Brummayer, FMV, JKU Linz



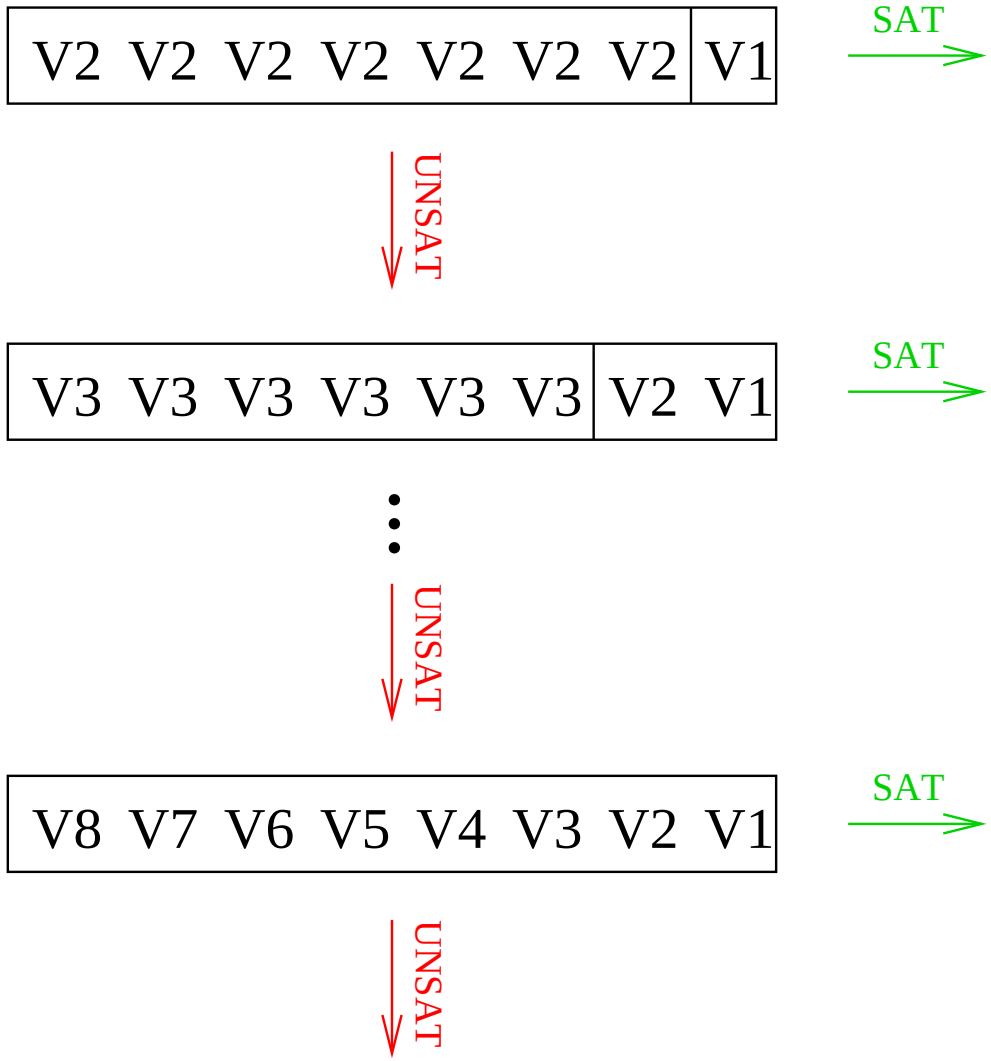
Optimization techniques

R. Brummayer, FMV, JKU Linz

- Boolean range analysis
  - Check if only boolean operators are applied to variable
- Local two-level AIG rewriting [BrummayerBiere, MEMICS'06]
  - Guaranteed to be globally size decreasing
- Under-approximation [Bryant et al., TACAS'07]
  - Restrict number of AIGs for encoding
  - If UA formula is SAT, then also original formula is SAT
  - If UA formula is UNSAT, then refine approximation

Under-approximation

R. Brummayer, FMV, JKU Linz



Conclusion

R. Brummayer, FMV, JKU Linz

- Checking “undefinedness” (ISO/IEC C99)
- Functional representation
- Optimizations
- Future work
  - Pointers
  - Over-approximation
  - Incremental API