02913
Advanced Analysis Techniques
January 2012

Flemming Nielson
Hanne Riis Nielson
Nikolaj Bjørner
Information about 02913

• Please see the following page for the plans: http://www2.imm.dtu.dk/courses/02913/

• Please see the following page for formalities: http://www.kurser.dtu.dk/02913.aspx?menulanguage=en-GB

• the time schedule for Monday and Tuesday
  – morning: 9.00 onwards,
  – lunch,
  – afternoon: 15.00 – 16.30.
Attendees to 02913

1. Carroline Ramli <cdpu@imm.dtu.dk>
2. Jose Nuno Carvalho Quaresma <jncq@imm.dtu.dk>
3. Michal Terepeta <mtte@imm.dtu.dk>
4. Phan Anh Dung <padu@imm.dtu.dk>
5. Piotr Filipiuk <pifi@imm.dtu.dk>
6. Fabrizio Biondi <fbio@itu.dk>
7. Kasper Svendsen <kasv@itu.dk>
8. Gian Perrone <gdpe@itu.dk>
9. Lei Song <leis@itu.dk>
10. Tijs Slaats <tslaats@itu.dk>
11. Han Yue <s111374@student.dtu.dk>
12. Roberto Vigo <rvig@imm.dtu.dk>
13. Nataliya Skrypnyuk <nsk@imm.dtu.dk>
14. Flemming Nielson <nielson@imm.dtu.dk>
15. Hanne Riis Nielson <riis@imm.dtu.dk>
16. Ximeng Li <s100998@student.dtu.dk>
17. Christian W. Probst <probst@imm.dtu.dk>
18. Lijun Zhang <lizh@imm.dtu.dk>
19. Sebastian Mödersheim <samo@imm.dtu.dk>
20. Ender Yuksel <ey@imm.dtu.dk>
02913

Introduction to SAT

Monday 2nd January 2012

Flemming Nielson
Literature

Propositional Logic

- variables
- literals
- operators
- conjunctive normal form
- (disjunctive normal form)
- (conversion / blow-up)
Boolean Satisfiability (SAT)

• constructive version:
  – find all assignments (rare)
  – find some assignment or indicate failure

• existential version (decidability version):
  – does there exist an assignment

• how do they relate?
Translation to SAT

• 4 colorability to SAT
  – Figure 1

Figure 1. Encoding of graph coloring.

Encoding

\[ \neg((c_{10} \land c_{20}) \lor (\neg c_{10} \land \neg c_{20})) \land ((c_{11} \land c_{21}) \lor (\neg c_{11} \land \neg c_{21})) \land \]
\[ \neg((c_{10} \land c_{30}) \lor (\neg c_{10} \land \neg c_{30})) \land ((c_{11} \land c_{31}) \lor (\neg c_{11} \land \neg c_{31})) \land \]
\[ \neg((c_{30} \land c_{20}) \lor (\neg c_{30} \land \neg c_{20})) \land ((c_{31} \land c_{21}) \lor (\neg c_{31} \land \neg c_{21})) \]

Solution

\[ c_{10} = 0 \land c_{11} = 0 \land c_{20} = 0 \land c_{21} = 1 \land c_{30} = 1 \land c_{31} = 0 \]

– o10=o20 iff (o10\land o20) \lor (\neg o10\lor \neg o20)
Translation to SAT

• digital circuits
  – fairly direct

• temporal logic
  – bounded reachability only

• is translation always the way to go?
Solving SAT

- the decidability version is NP-complete
- in practice better than “expected” exponential
Solving SAT

- input CNF
- apply Systematic Search
- use DPLL to speed it up
  - Davis, Putnam, Logemann, Loveland
- many improvements
DPLL: basic algorithm

- flowchart (notes)
DPLL: subroutines

• branch
  – nondeterministic choose “new” variable and give it a value

• implication
  – find all implications from the assignment and the CNF

• backtrack
  – in case of conflict go back to closest branch and reconsider (fail if no such branch)
DPLL: worked example

- Figure 2

![Figure 2. Search space of a formula.](image)

\[ \neg x_1 \lor \neg x_2 \land (\neg x_1 \lor x_2 \lor \neg x_3) \land (\neg x_1 \lor x_3 \lor \neg x_4) \land (x_1 \lor x_4) \]

(Figure 2. Search space of a formula.)

- DPLL:
  - worked example

  - **Figure 2**

- **DPLL approach**
  - Decision
  - Unit

- **DPLL:** worked example
  - **Figure 2**
DPLL: improvement

• non-chronological backtracking using
• conflict driven learning (notes)
DPLL: worked example

- Figure 3
Industrial Impact

- hardware verification
- software verification
- configuration management
- ...
Beyond SAT

• SMT
  – Satisfaction Modulo Theories
  – SAT with the variables being queries to a specific theory (where conjunctions of queries can be decided)
  – examples:
    • uninterpreted function symbols with equality
    • linear (integer / real) arithmetic
    • datastructures like arrays and lists

• The topic of Tuesday
SAT: questions for today

• Explain how to convert formula to CNF
  ① basic algorithm, exponential blow up
  ② extra variables, linear blow up (p.78)

• Explain some improvements on DPLL
  ③ two-literal watching (p.80)
  ④ random restart (p.80)
  ⑤ clause and variable elimination (p.80)
  ⑥ DPLL and OBDD (p.80)
  ⑦ discrete optimization, local search (p.81)