ITMO UNIVERSITY

Сириус
Образовательный центр

Алгоритмические основы SAT-решателей

Даниил Чивилихин

18 августа 2020

Летняя школа «Дискретные методы синтеза и верификации для киберфизических систем»

17-21 августа 2020 г.

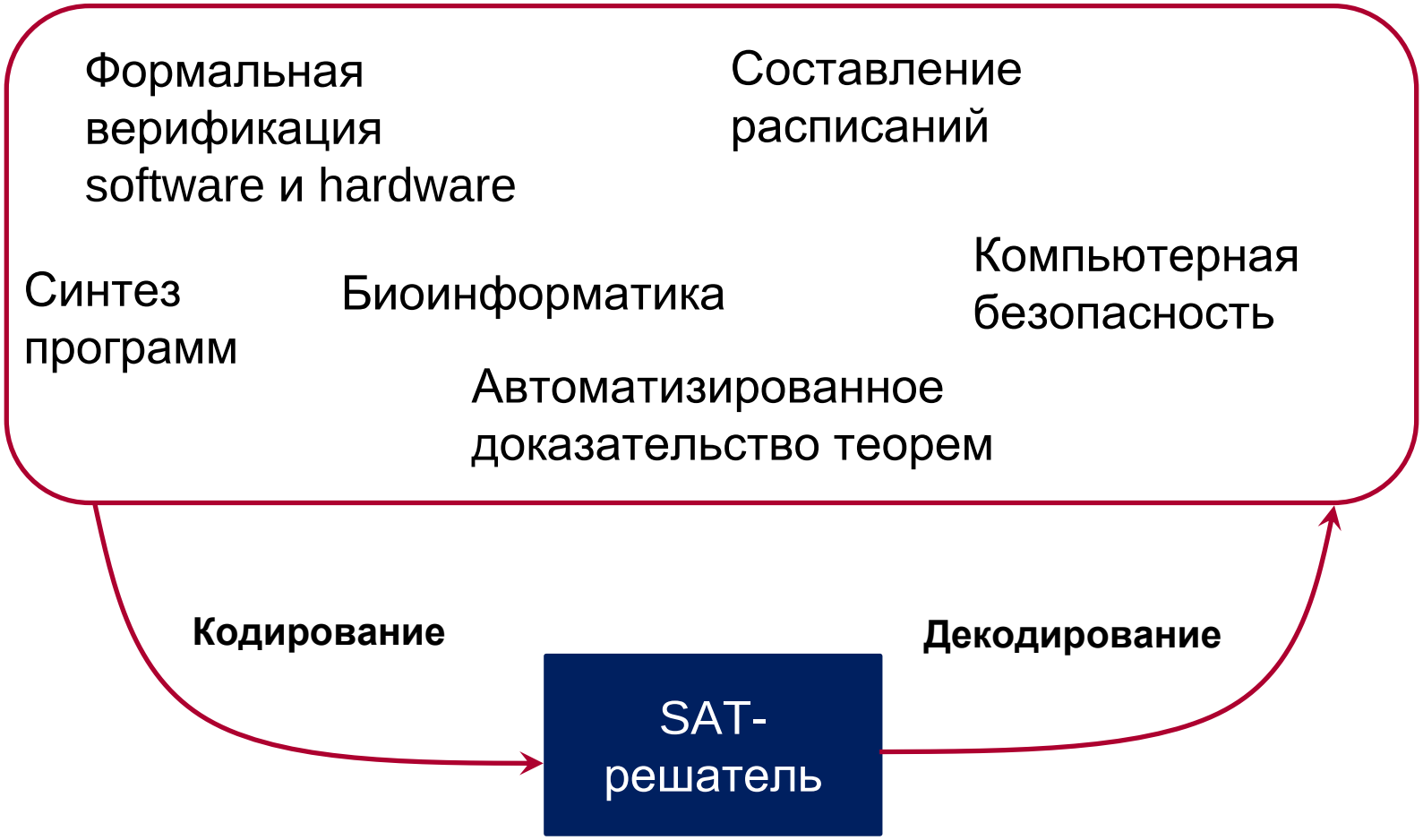
О себе

- ФМЛ № 239 – 2007
- Университет ИТМО – бакалавр, 2011
- Университет ИТМО – магистр, 2013
- Университет ИТМО – к.т.н., 2015
- С 2015 занимаюсь SAT и верификацией
- Со-руководитель лаборатории «Дискретная оптимизация и формальные методы» ИТМО
- Международный научный центр «Компьютерные технологии»

План лекции

Решение задач путем сведения к SAT
Пропозициональная логика
SAT-решатели
Правило распространения единичного дизъюнкта
Алгоритм DPLL
Алгоритм CDCL
Эвристики
Минимизация конфликтных дизъюнктов

Области применения SAT-решателей



Решение задач с помощью сведения к SAT

- Хотим решить задачу из класса X ($x \in X$)
- Функция сведения $f: X \to SAT$
- «Кормим» f(x) SAT-решателю, вуаля!

+ один раз написали сведение, пользуемся прогрессом SAT-решателей

Но об этом – в следующей лекции.

Императивное решение vs сведение к SAT

Императивное решение

Как (конструктивно) построить решение?

Сведение к SAT

Какими свойствами должно обладать решение?

Пропозициональная логика: дресс-код

- Логические переменные: галстук и рубашка
- Логические связки: ¬, ∧, ∨
- Литералы: галстук, ¬галстук, рубашка, ¬рубашка

Три условия / дизъюнкта

1. Невежливо не носить ни галстука, ни рубашки

$$(\text{галстук} \vee \text{рубашка})$$

2. Не стоит носить галстук без рубашки

$$(\text{галстук} \rightarrow \text{рубашка}) \equiv (\neg\text{галстук} \vee \text{рубашка})$$

1. Носить галстук вместе с рубашкой – уже слишком

$$\neg(\text{галстук} \wedge \text{рубашка}) \equiv (\neg\text{галстук} \vee \neg\text{рубашка})$$

Формула $(\text{галстук} \vee \text{рубашка}) \wedge (\neg\text{галстук} \vee \text{рубашка}) \wedge (\neg\text{галстук} \vee \neg\text{рубашка})$ разрешима?

Булева формула

Булевы переменные –значения из {0, 1}.

Литералы для x – x, $\neg x$

Булева формула – переменные и логические связки, например ∧ (И) ,∨ (ИЛИ) ,¬ (НЕ).

Произвольная формула

$$(x \wedge y) \rightarrow (z \vee (a \wedge b))$$

Дизъюнкт – дизъюнкция литералов

$$(x \vee \neg y \vee z)$$

Конъюнктивная нормальная форма (КНФ)

Конъюнкция дизъюнктов

$$(x \vee y \vee z) \wedge (\neg x \vee y) \wedge (y \vee \neg z)$$

По произвольной формуле *F* можно построить КНФ, выполнимую тогда и только тогда, когда выполнима *F* (преобразования Цейтина)

[Цейтин Г.С. О сложности вывода в исчислении высказываний. Зап. научн. семинаров ЛОМИ. Т.8. 1968. С. 234-259.]

SAT-решатели (SAT solvers)

Вход: булева формула в КНФ

Выход: UNSAT / SAT + выполняющий набор

Вход: $(x_1 \vee x_2) \wedge (x_2 \vee \neg x_3) \wedge (\neg x_1)$

SAT: $(x_1 \vee x_2) \wedge (x_2 \vee \neg x_3) \wedge (\neg x_1)$

$$x_1 = 0, x_2 = 1, x_3 = 1$$

Вход: $(x_1 \vee x_2) \wedge (x_2 \vee \neg x_3) \wedge (\neg x_1) \wedge (x_1 \vee \neg x_2)$

UNSAT

SAT-решатели (SAT solvers)

- Полные vs. неполные SAT-решатели

- Основаны на
  - правиле распространения единичного дизъюнкта
  - алгоритмах DPLL и CDCL
  - и множестве различных эвристик

Правило распространения единичного дизъюнкта (Unit propagation rule)

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge (\neg x_1)$$

Правило распространения единичного дизъюнкта (Unit propagation rule)

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge (\neg x_1)$$

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge (\neg x_1)$$

Правило распространения единичного дизъюнкта (Unit propagation rule)

$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge (\neg x_1)$

$(\sout{x_1} \vee x_2 \vee x_3) \wedge (\sout{x_1} \vee x_3) \wedge \sout{(\neg x_1 \vee x_4 \vee \neg x_5)} \wedge (\neg x_1)$

$(\quad x_2 \vee x_3) \wedge (\quad x_3) \wedge \qquad\qquad (\neg x_1)$

Правило распространения единичного дизъюнкта (Unit propagation rule)

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge (\neg x_1)$$

$$(\sout{x_1} \vee x_2 \vee x_3) \wedge (\sout{x_1} \vee x_3) \wedge \sout{(\neg x_1 \vee x_4 \vee \neg x_5)} \wedge (\neg x_1)$$

$$\sout{(\quad x_2 \vee x_3)} \wedge (\quad x_3) \wedge \qquad (\neg x_1)$$

Правило распространения единичного дизъюнкта (Unit propagation rule)

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge (\neg x_1)$$

$$(\cancel{x_1} \vee x_2 \vee x_3) \wedge (\cancel{x_1} \vee x_3) \wedge \cancel{(\neg x_1 \vee x_4 \vee \neg x_5)} \wedge (\neg x_1)$$

$$\cancel{(x_2 \vee x_3)} \wedge (x_3) \wedge (\neg x_1)$$

$$(x_3) \wedge (\neg x_1)$$

SAT!

Правило распространения единичного дизъюнкта (Unit propagation rule)

Пусть формула содержит единичный дизъюнкт с литералом l.

1. Удалить все дизъюнкты, содержащие l, кроме l.
2. Удалить из всех дизъюнктов литерал $\neg l$.

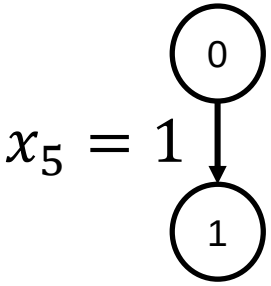
Полученная формула эквивалентна исходной.

Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

0

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

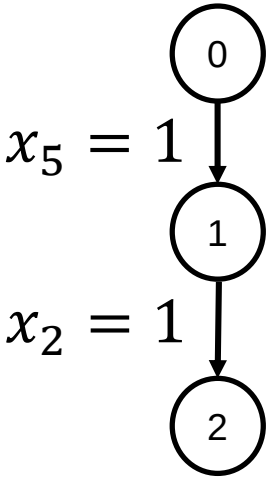
Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)



$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

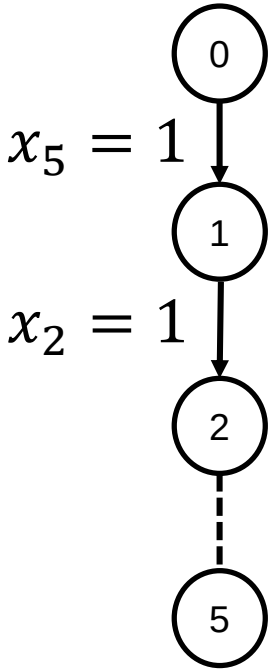
Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



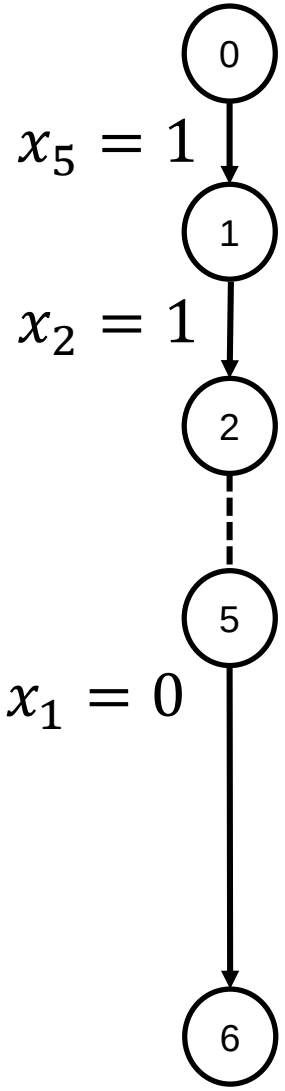
Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



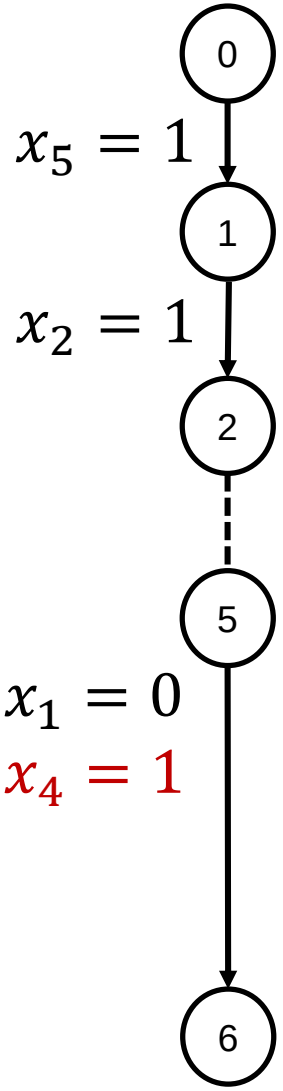
Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

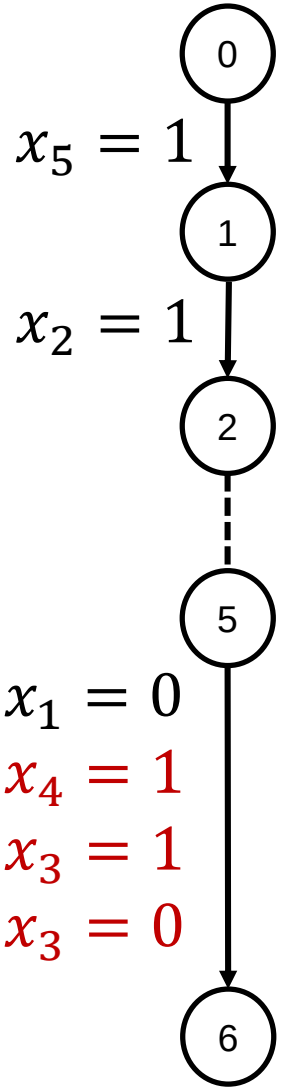
$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

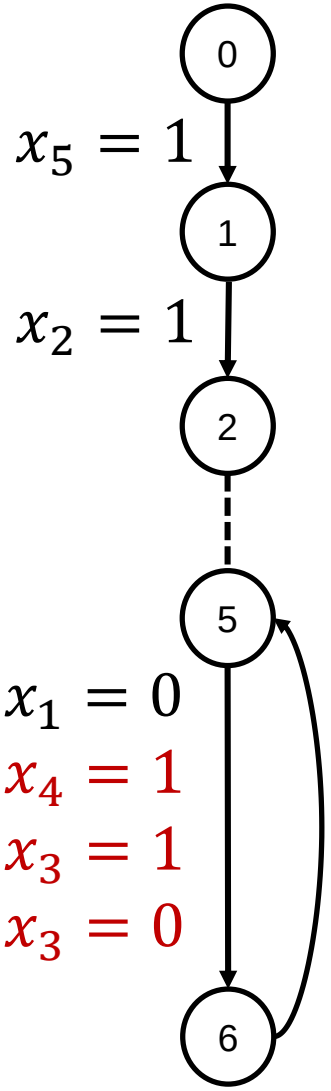
$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

Конфликт!



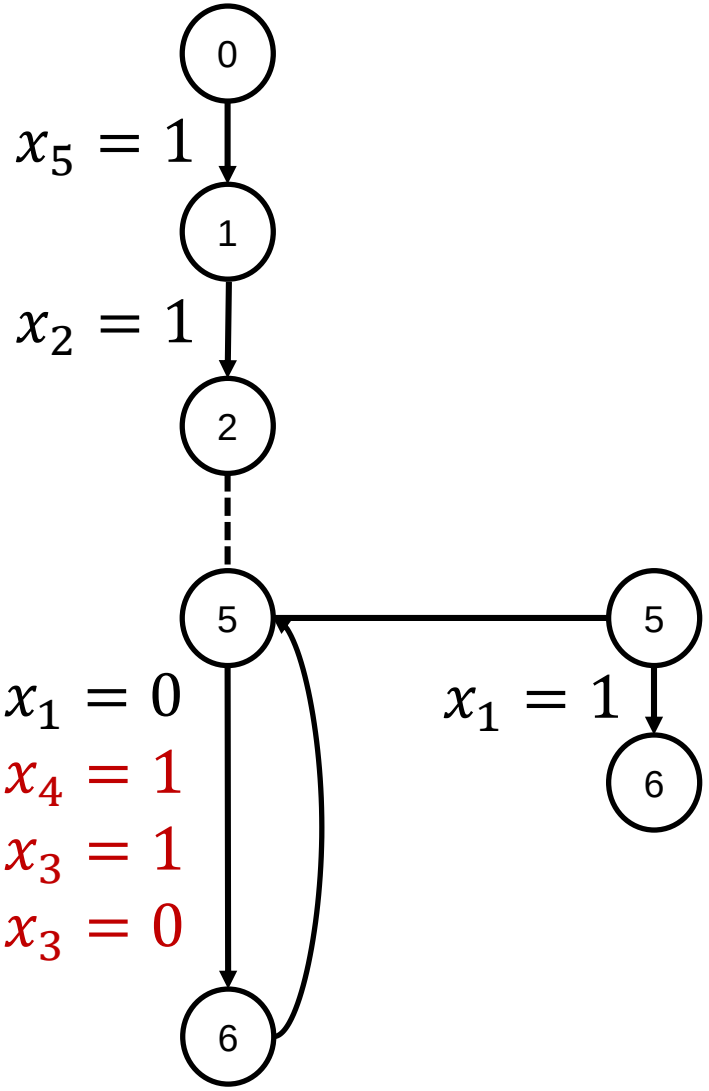
Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

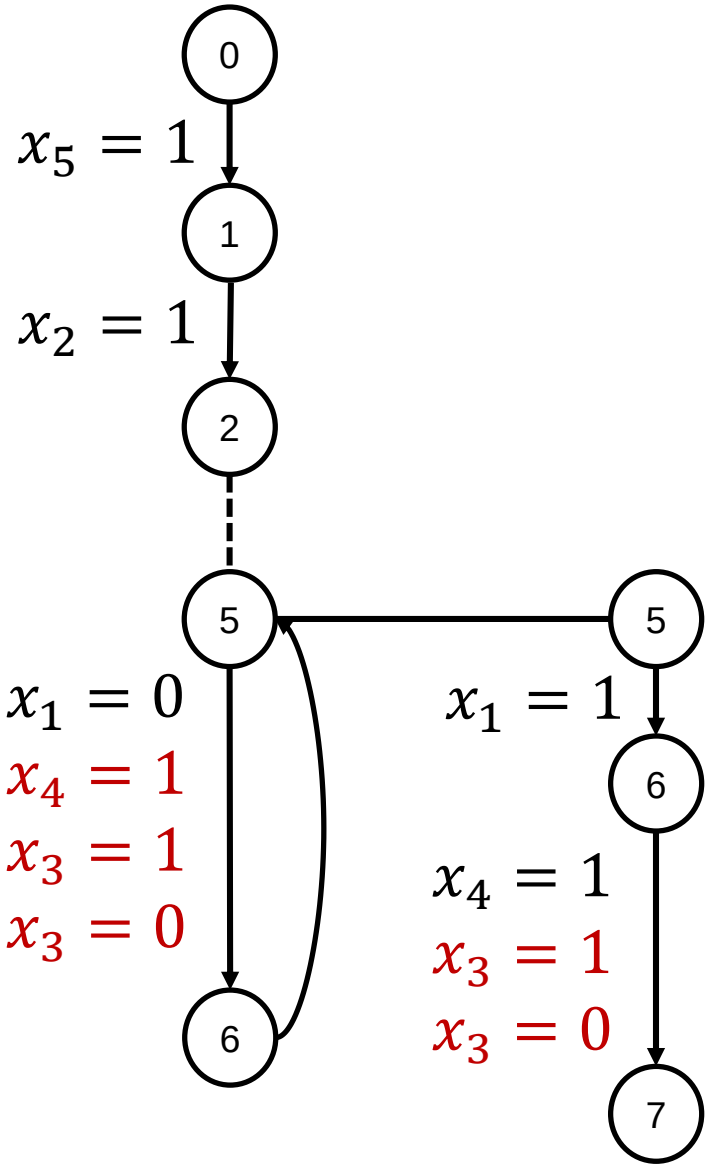
$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

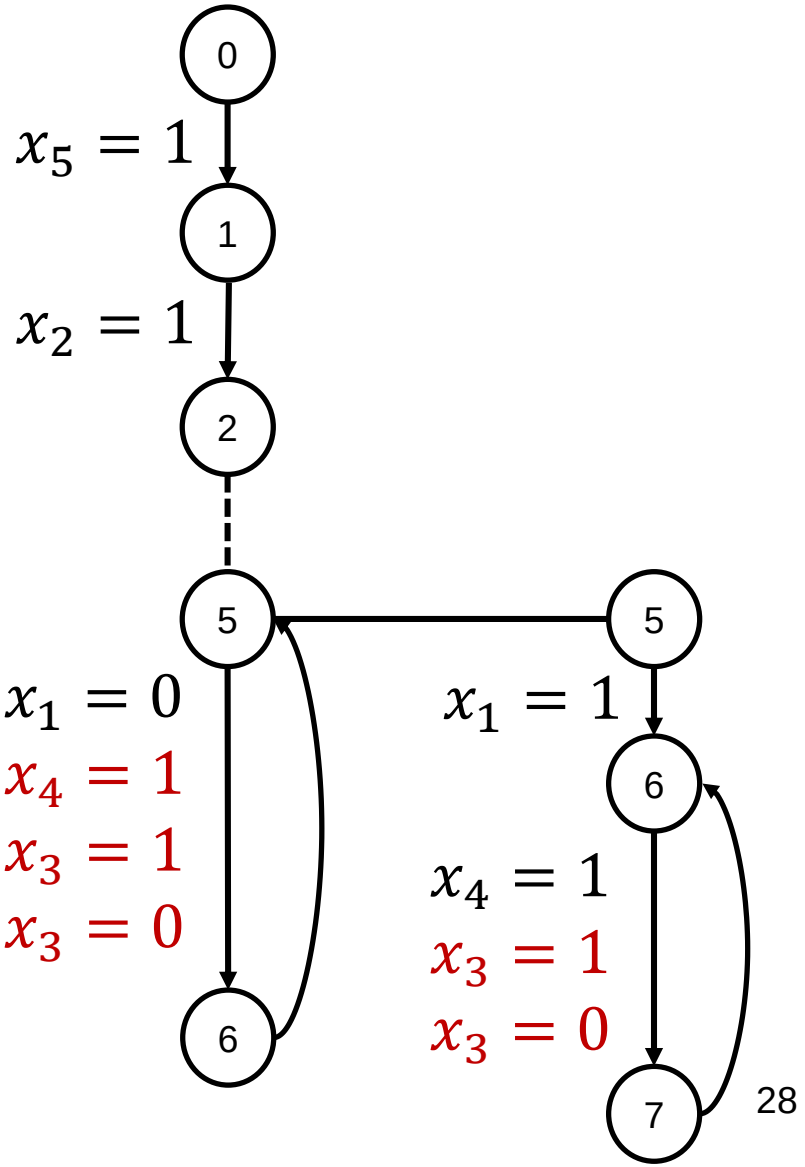
$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

Опять конфликт!



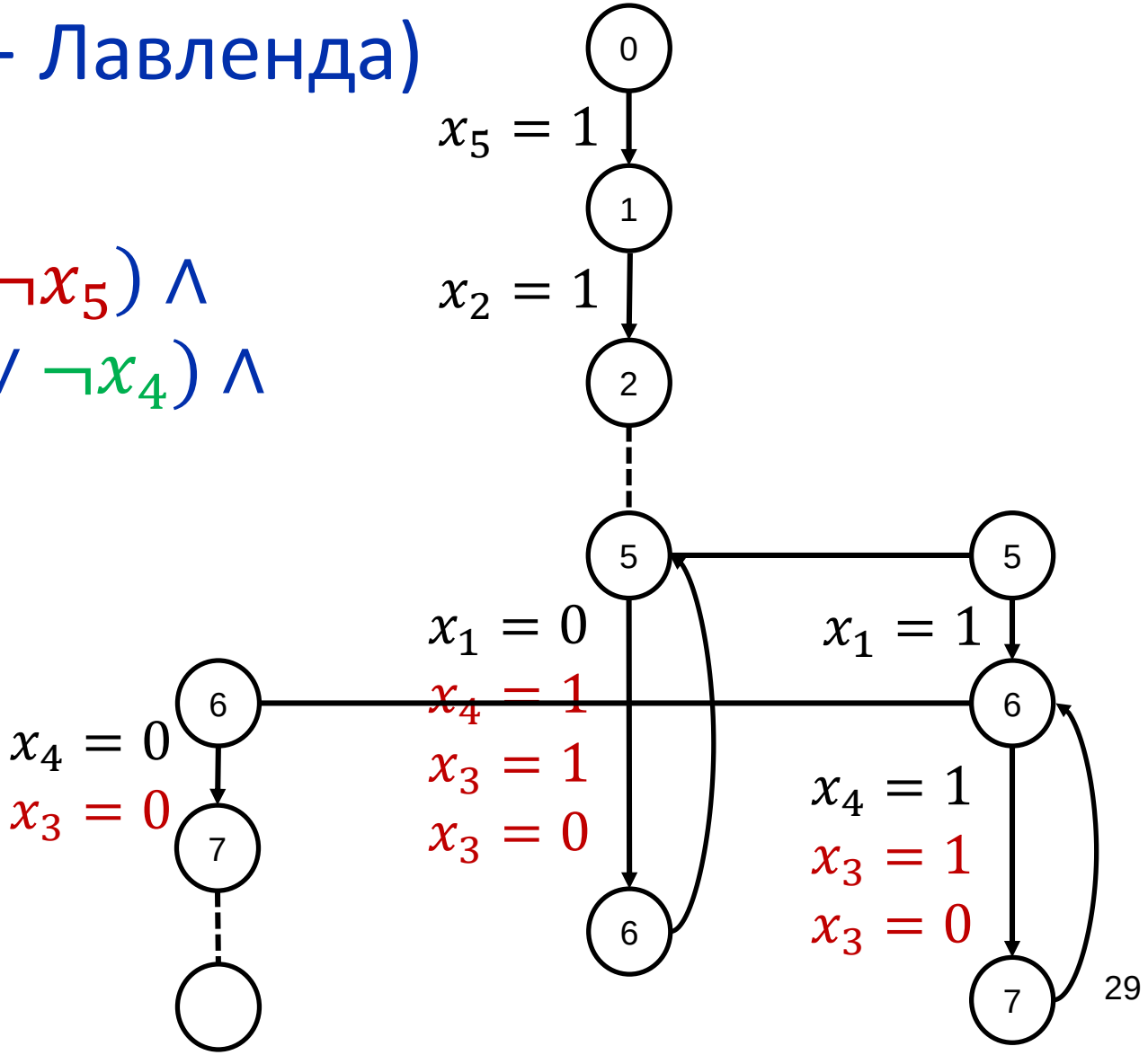
Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

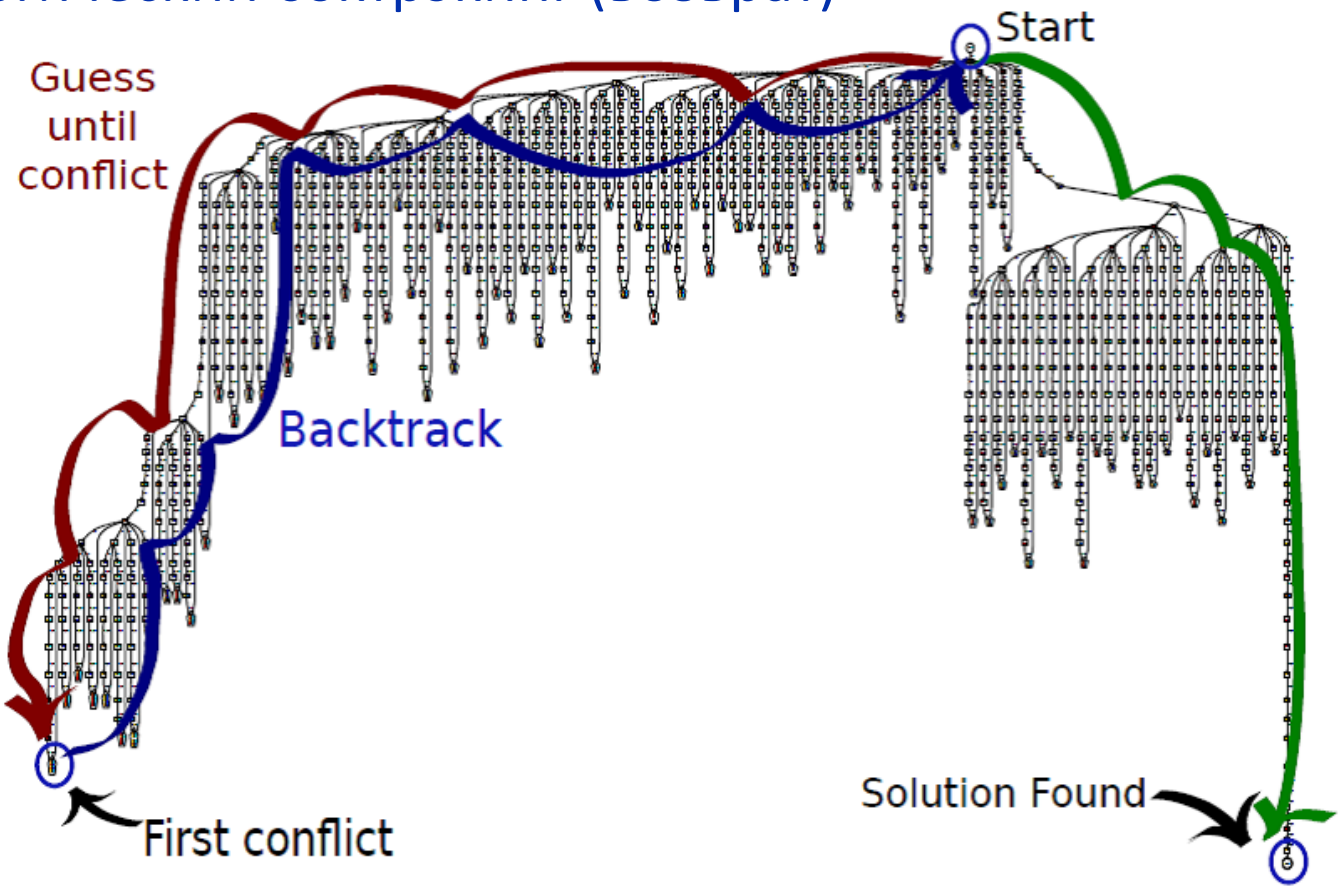
$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



SAT!

Алгоритм DPLL (Дэвиса — Патнема — Логемана — Лавленда)

Хронологический бэктрэкинг (возврат)



https://srlabs.de/bites/minisat-intro/

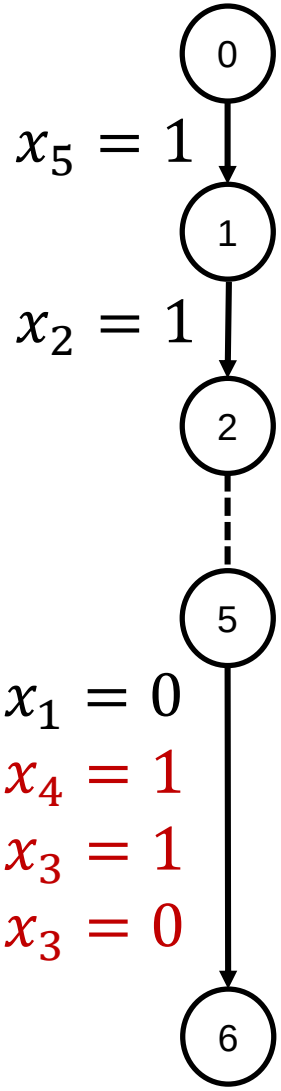
Алгоритм CDCL (Conflict Driven Clause Learning)

- «Управляемое конфликтами обучение дизъюнктам»
- Marques-Silva J., Sakallah K. GRASP – a new search algorithm for satisfiability // Proceedings of ICCAD, 1996
- Основная идея: использовать знание о конфликтах
- Основа всех современных полных SAT-решателей

Алгоритм CDCL

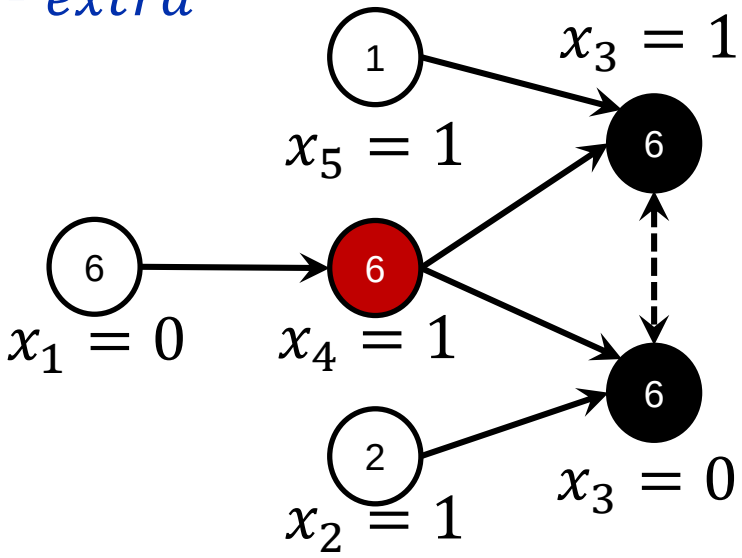
$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

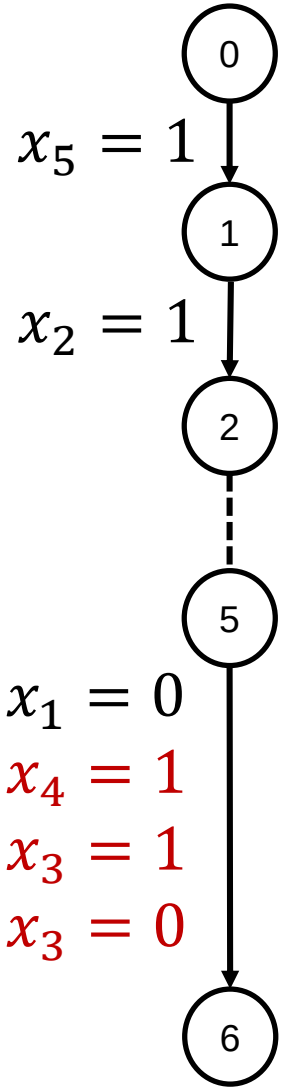
Конфликт!



Алгоритм CDCL

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

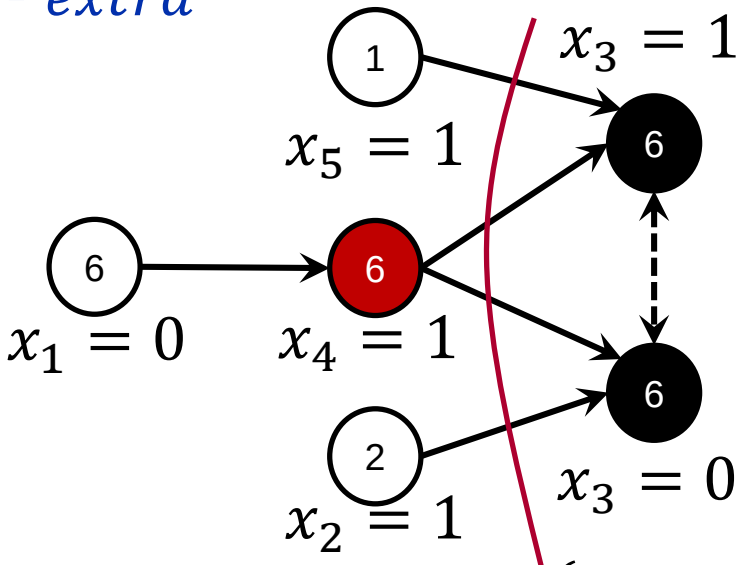


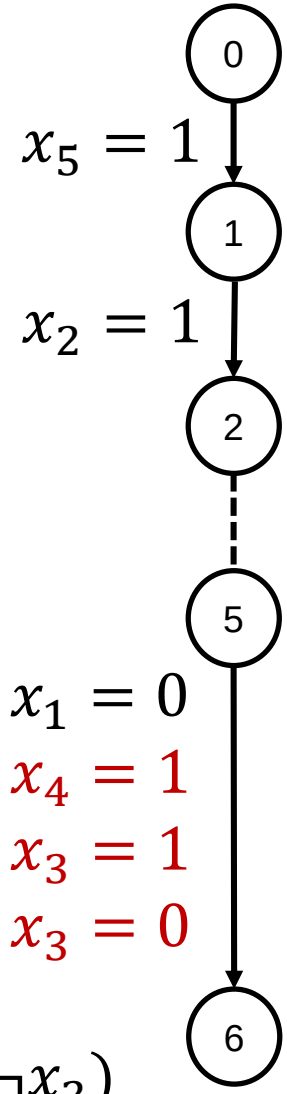


Импликационный граф

Алгоритм CDCL

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}



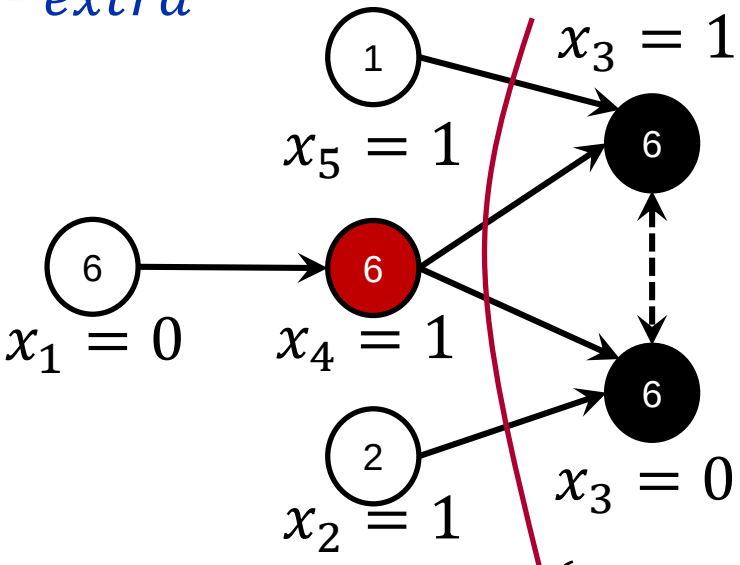


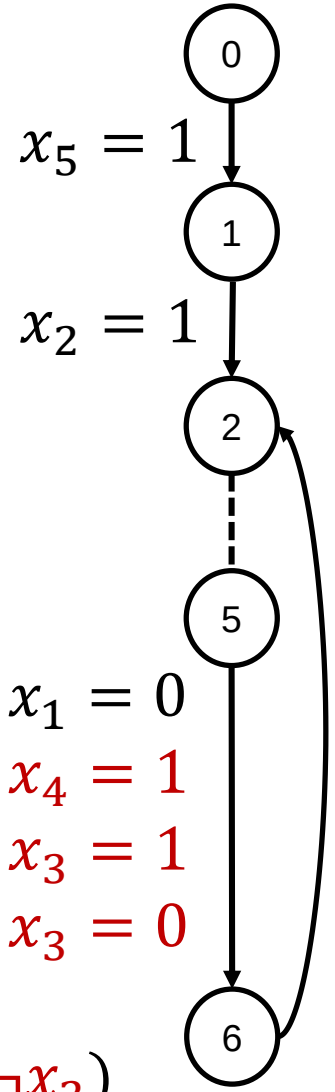
$(\neg x_5 \vee \neg x_4 \vee \neg x_2)$

Конфликтный дизъюнкт

Алгоритм CDCL

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}

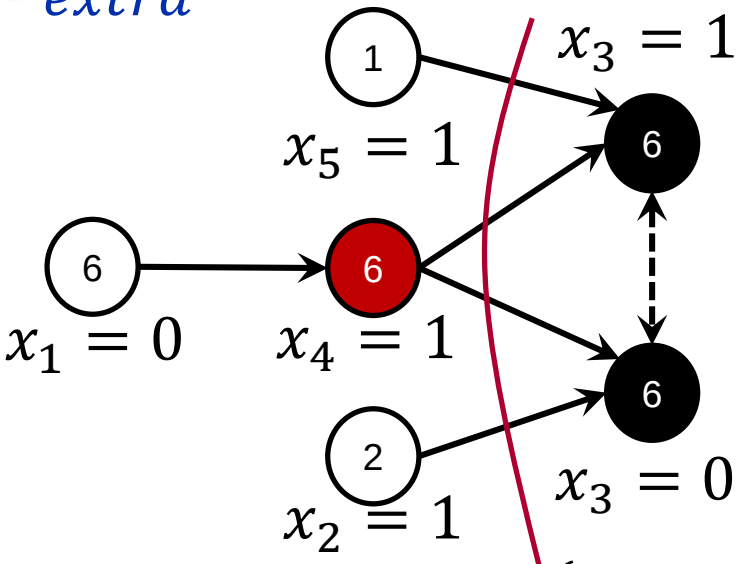


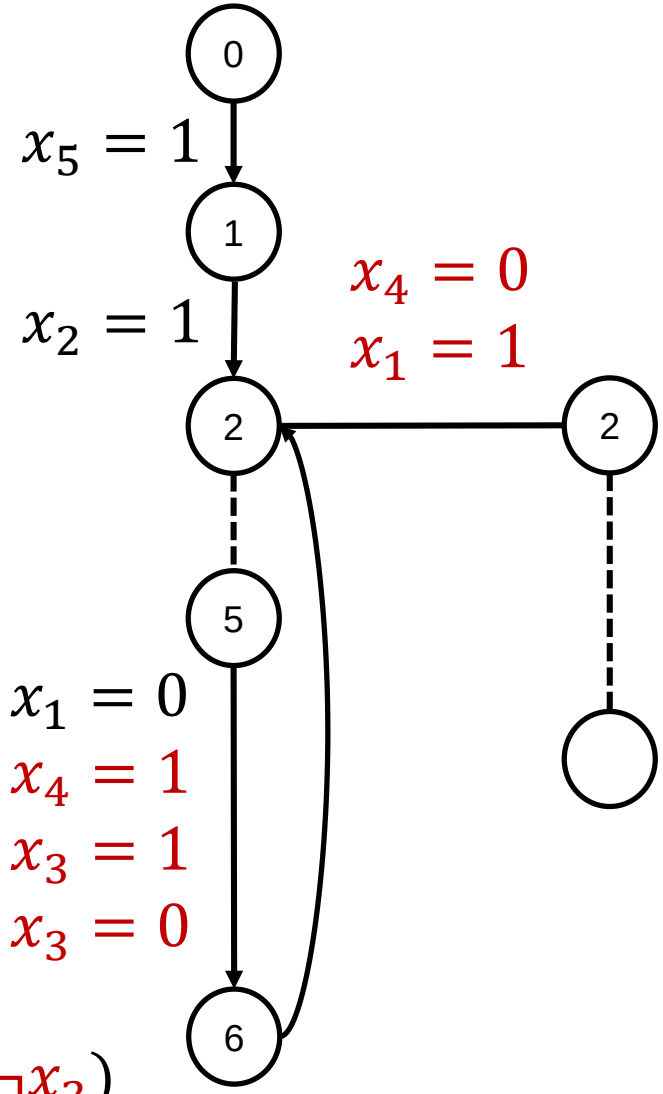


Нехронологический бэктрекинг

Алгоритм CDCL

$(x_1 \vee x_4) \wedge$
$(x_3 \vee \neg x_4 \vee \neg x_5) \wedge$
$(\neg x_3 \vee \neg x_2 \vee \neg x_4) \wedge$
F_{extra}





Алгоритм CDCL: псевдокод

```
1:  while TRUE do
2:      l_decision := GetDecisionLiteral( )
3:      If no l_decision then return satisfiable
4:      F := Simplify( F(l_decision ← 1) )
5:      while F contains C_falsified do
6:          C_conflict := AnalyzeConflict( C_falsified )
7:          If C_conflict = ∅ then return unsatisfiable
8:          BackTrack( C_conflict )
9:          F := Simplify( F ∪ {C_conflict} )
10:     end while
11: end while
```

Эвристики

Выбор переменной

Какую переменную угадываем?

Выбор значения переменной

Какое значение выбрать?

Стратегии перезапуска

Выбор переменной

На основе представленности в формуле

- Наибольшая представленность в дизъюнктах наименьшей длины

Variable State Independent Decaying Sum (VSIDS)
[MoskewiczMZZM’01]

- Рейтинг переменных
- Для каждого конфликта увеличиваем на 1
- Делим пополам раз в 256 конфликтов

Выбор значения переменной

На основе активности, например «Сохранение фазы» [PipatsrisawatDarwiche’07]

- Запоминаем последнее выбранное значение для каждой переменной
- В первую очередь выбираем запомненное значение

Перезапуски в CDCL решателях

Цель: избежать «зарывания» алгоритма в неперспективную ветку дерева поиска [GomesSelmanCrato'97]

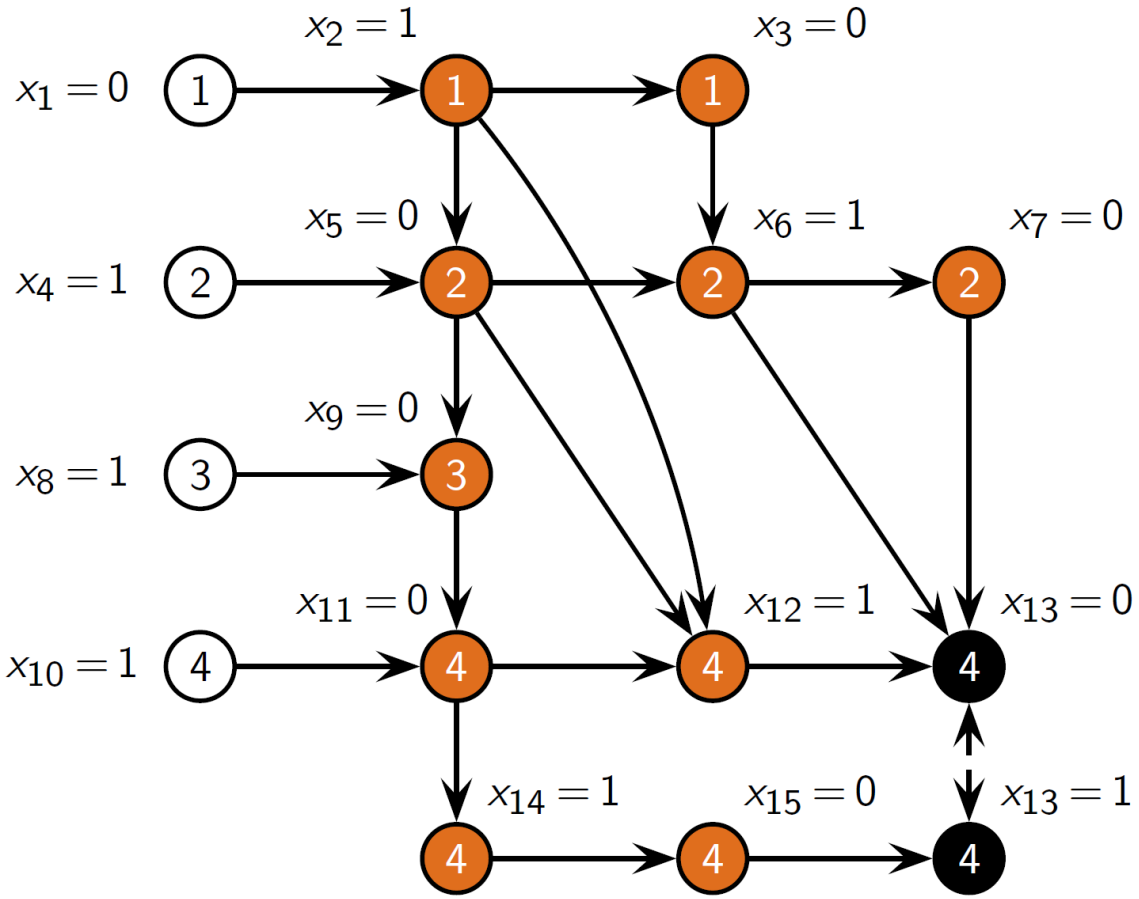
Отменяем назначения всех переменных

- Конфликтные дизъюнкты не удаляются!

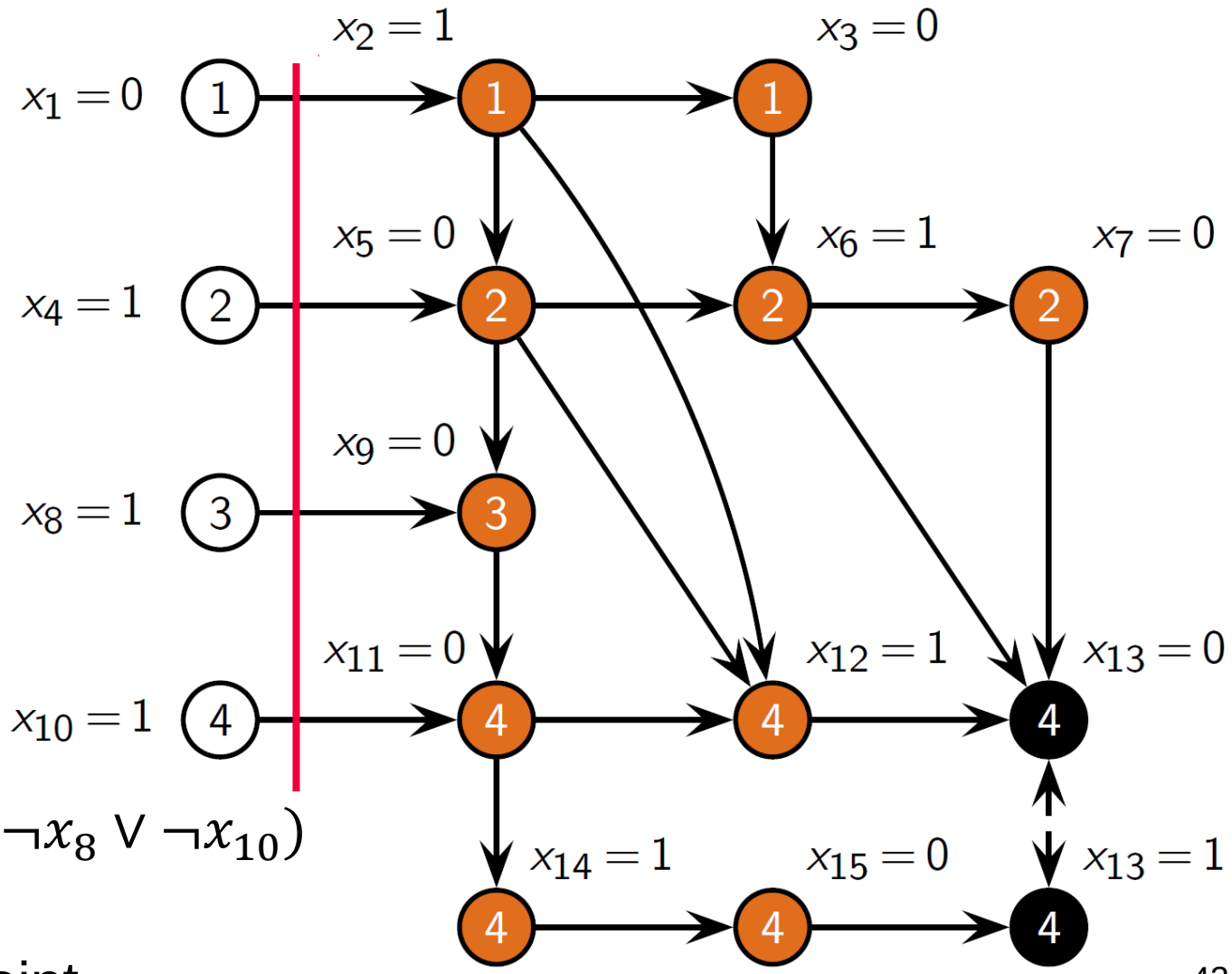
Геометрические: 100, 150, 225, 333, 500, 750,
Luby sequence: 100, 100, 200, 100, 100, 200, 400,

Минимизация конфликтных дизъюнктов

Как получить «оптимальный» конфликтный дизъюнкт?



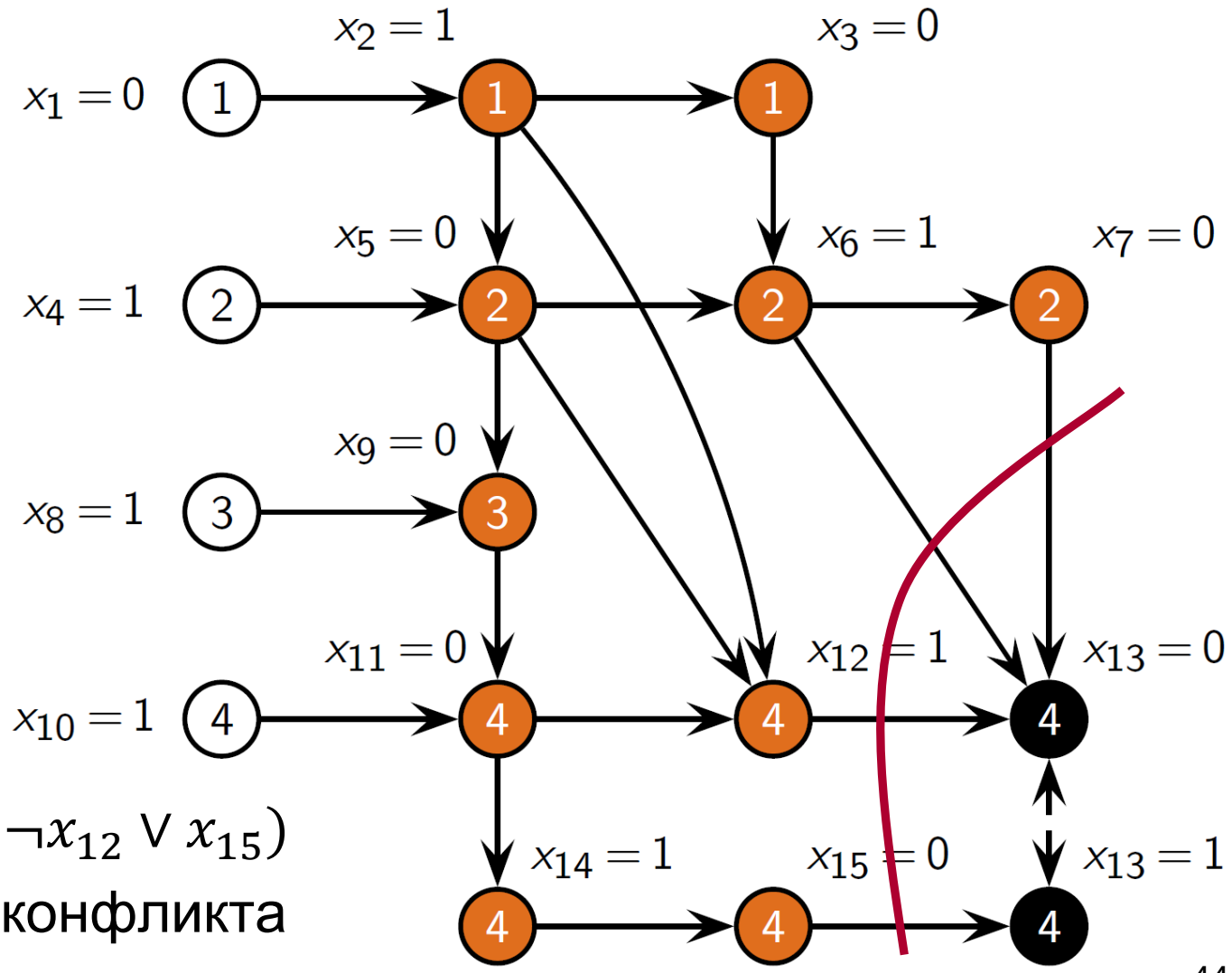
Минимизация конфликтных дизъюнктов



$(x_1 \vee \neg x_4 \vee \neg x_8 \vee \neg x_{10})$

Last unique implication point

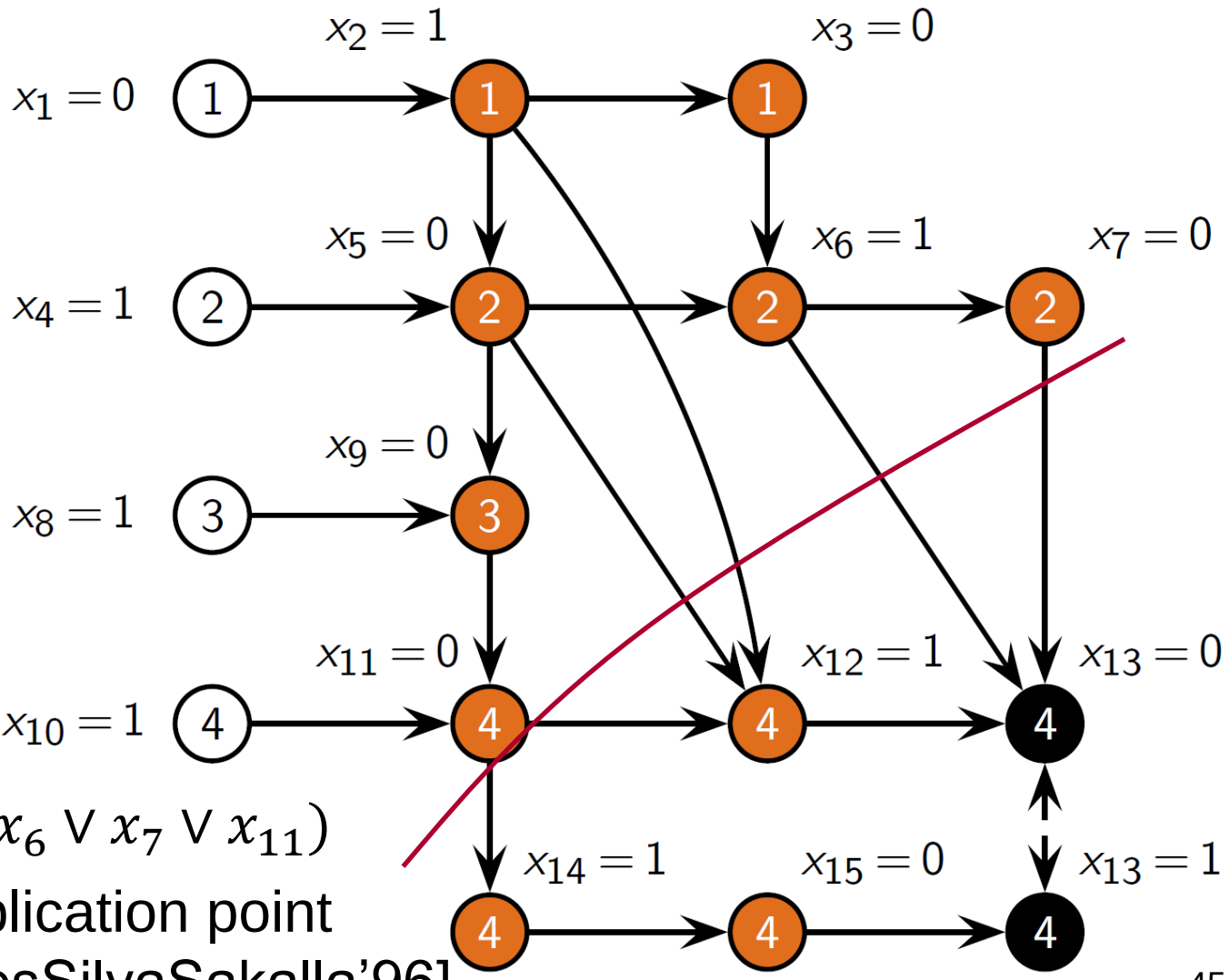
Минимизация конфликтных дизъюнктов



$(x_7 \vee \neg x_6 \vee \neg x_{12} \vee x_{15})$

Антецедент конфликта

Минимизация конфликтных дизъюнктов

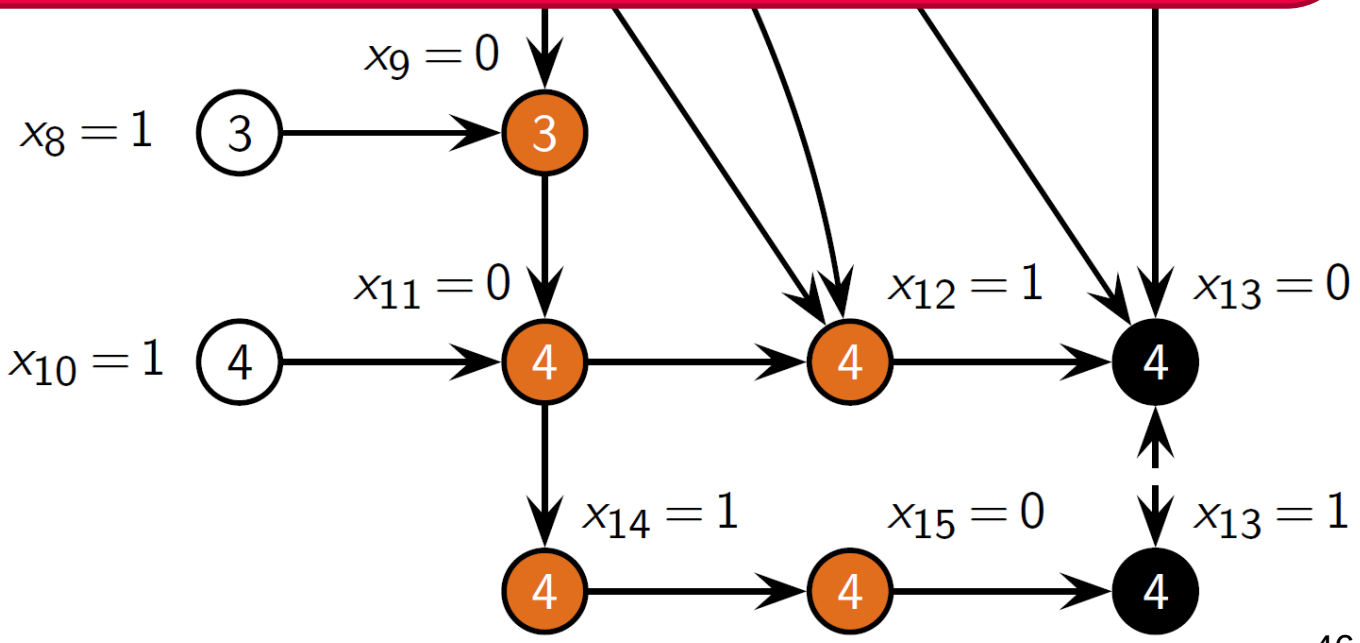


$(\neg x_2 \vee x_5 \vee \neg x_6 \vee x_7 \vee x_{11})$

First unique implication point (1-UIP) [MarquesSilvaSakalla'96]

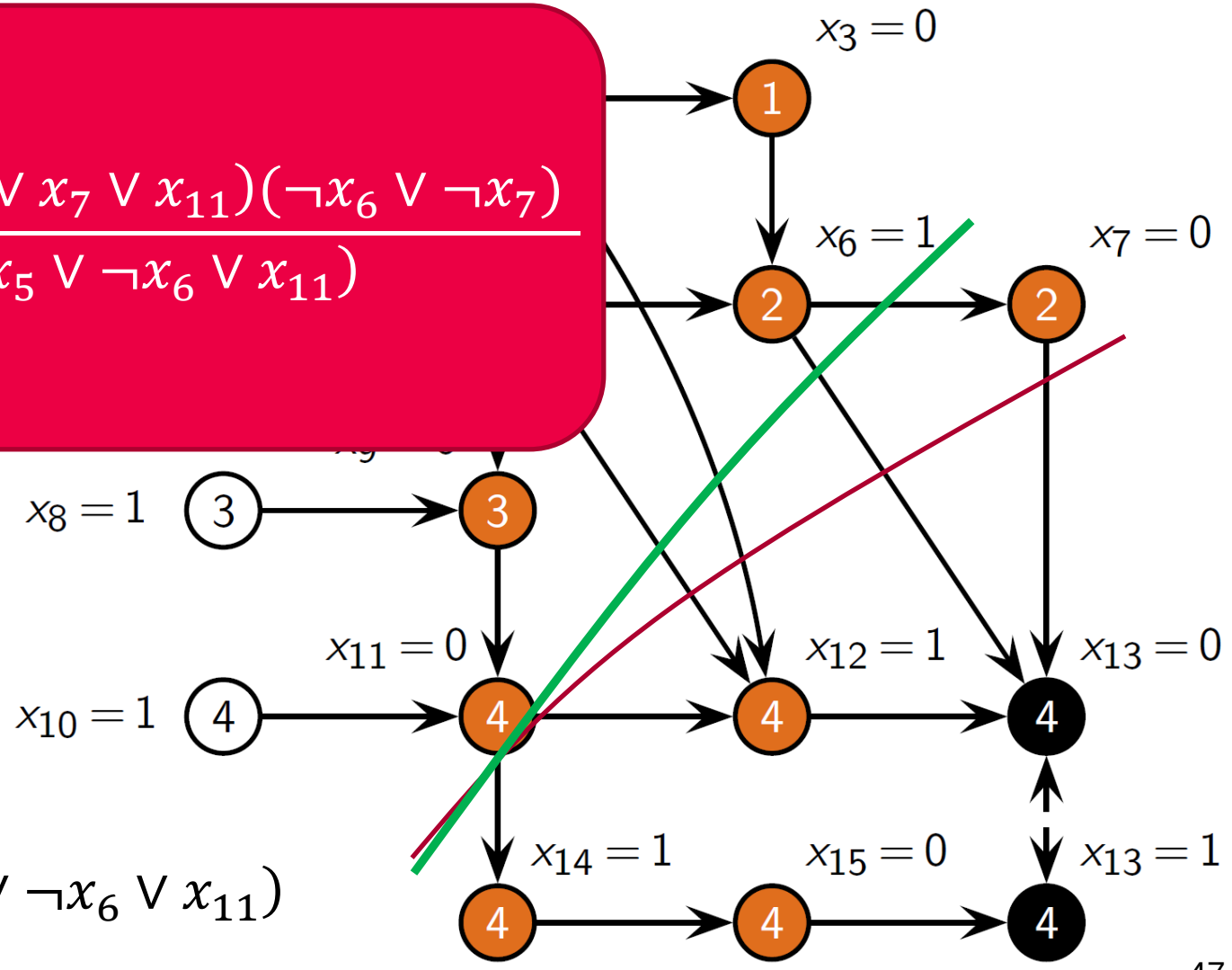
Минимизация конфликтных дизъюнктов

Локальная минимизация : если в дизъюнкте есть литерал и его причина, причину можно удалить [SorenssonBiere'09]



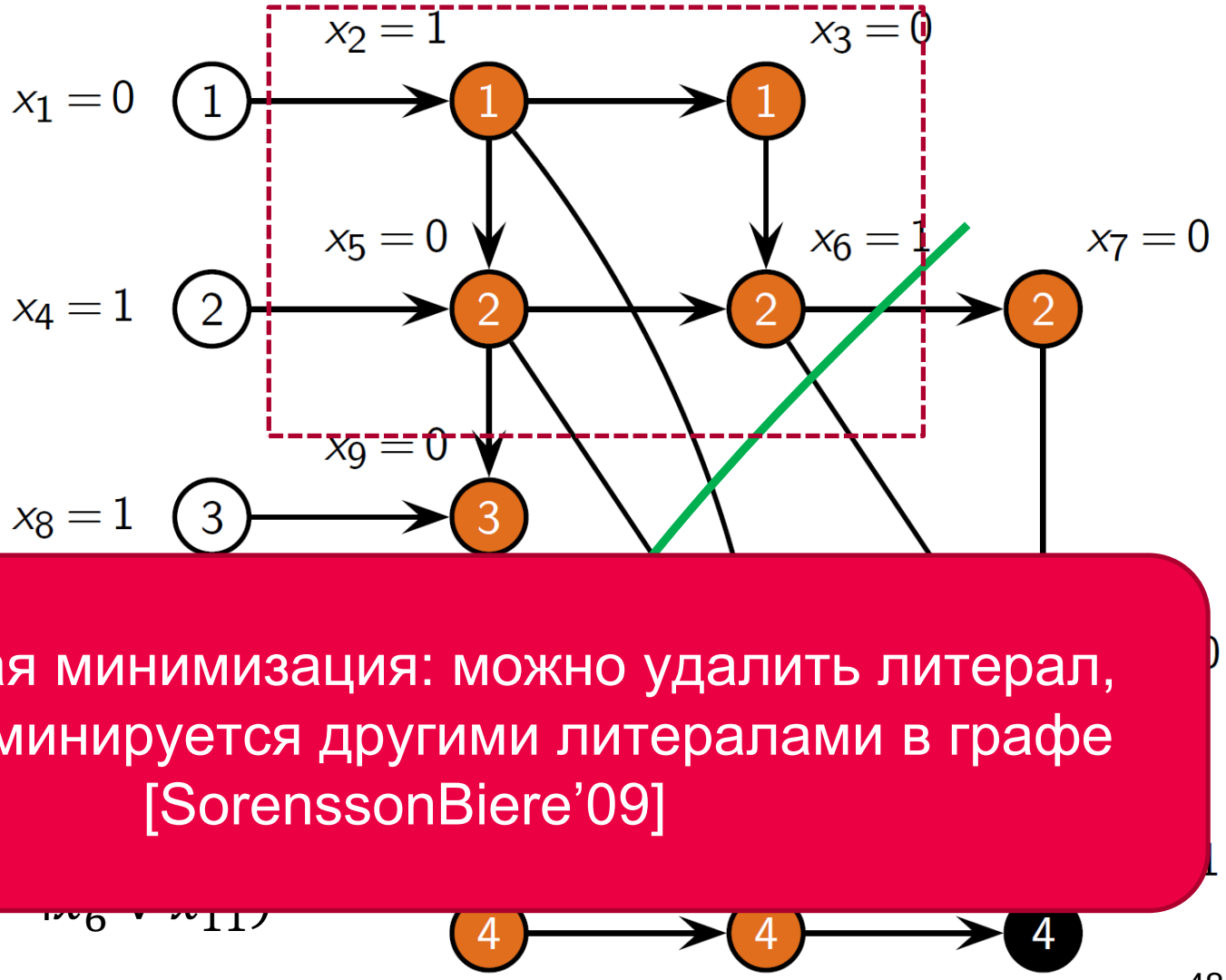
Минимизация конфликтных дизъюнктов

$$\frac{(\neg x_2 \vee x_5 \vee \neg x_6 \vee x_7 \vee x_{11})(\neg x_6 \vee \neg x_7)}{(\neg x_2 \vee x_5 \vee \neg x_6 \vee x_{11})}$$



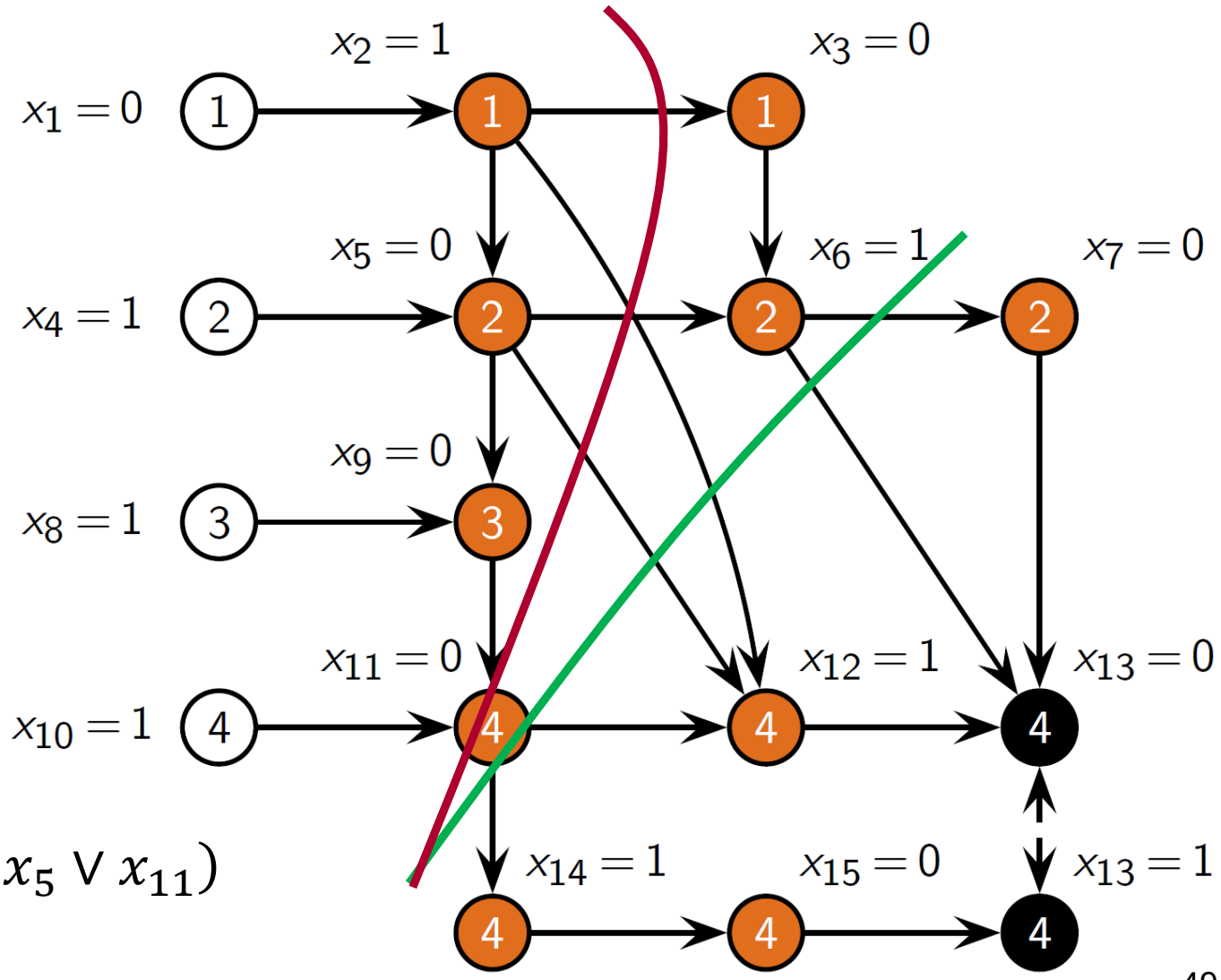
$$(\neg x_2 \vee x_5 \vee \neg x_6 \vee x_{11})$$

Минимизация конфликтных дизъюнктов



Рекурсивная минимизация: можно удалить литерал, если он доминируется другими литералами в графе [SorenssonBiere'09]

Минимизация конфликтных дизъюнктов



$(\neg x_2 \vee x_5 \vee x_{11})$

За кадром

- Добавление/удаление дополнительных дизъюнктов
- Добавление/удаление дополнительных переменных
- Implementation-related эвристики

Об одном типичном улучшении SAT-решателя [Kochemazov'19]

- Решатель MapleLCMDistChronoBT
- Повторное порождение конфликтных дизъюнктов
- Предложен механизм отслеживания, запрещающий удалять некоторые конфликтные дизъюнкты

Современные SAT-решатели

- lingeling, plingeling, treengeling
- CaDiCal
- Glucose
- Cryptominisat
- Семейство Maple*
- Microsoft Z3 (больше, чем SAT-решатель)

PySAT – Python-интерфейс для SAT-решателей
https://github.com/pysathq/pysat

Современные SAT-решатели

- Инкрементальное решение
- Сохранение доказательств неразрешимости (UNSAT proofs)
- Ядра невыполнимости (UNSAT cores)
- …

Сообщество, соревнования

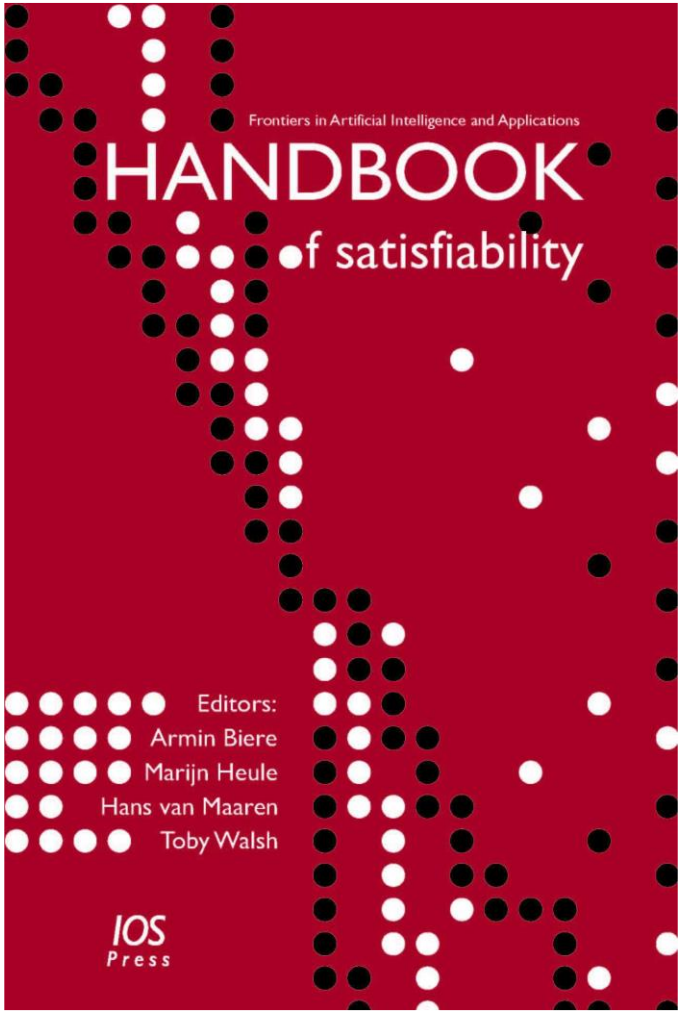
- Сообщество:

http://satassociation.org/

- Соревнования:

http://www.satcompetition.org/

- SAT/SMT Summer School
- SAT conference (1996 –)
- Handbook of satisfiability



Итоги

SAT-решатели: мощная технология для решения сложных задач.

Активные исследования и разработки как в области решения SAT, так и в области применения SAT-решателей.

Далее

16:30 – 18:00. Константин Чухарев. «Решение задач путем сведения к SAT. Практические аспекты использования SAT-решателей»

18:00 – начало контеста на Codeforces по решению задач путем сведения к SAT

ITMO UNIVERSITY

Спасибо за внимание!

chivdan@itmo.ru
Telegram: @chivdan