A SAT-based approach for index calculus on binary elliptic curves

Monika Trimoska Sorina Ionica Gilles Dequen

Laboratoire MIS, Université de Picardie Jules Verne

GT BAC
16 May 2019

Discrete logarithm

Given a finite cyclic group $(G, +)$ and two elements g, $h \in G$, find $x \in \mathbb{Z}$ such that

$$h = x \cdot g.$$

- Generic attacks - Pollard rho, Baby-step Giant-step, Kangaroo
- Index calculus attack : subexponential in $(\mathbb{Z}/p\mathbb{Z})*$.

Index calculus

1. Finding an appropriate *factor base* $\mathcal{B} = \{g_1, ..., g_k\}$, such that $\mathcal{B} \subseteq G$
2. Relation search phase : find relations of the form

$$[a_i]g \ + \ [b_i]h \ = \ \sum_{j=1}^{n}[c_{ij}]g_j$$

   for random integers a_i, b_i.
3. Linear algebra phase : having matrices $A = (a_i b_i)$ and $M = (c_{ij})$, find a kernel vector $v = (v_1 ... v_k)$ of the matrix M. Compute solution :

$$x = -(\sum_i a_i v_i)/(\sum_i b_i v_i)$$

Index calculus on elliptic curve groups

Let $\mathbb{F}_{2^n}$ be a finite field and E be an elliptic curve defined by

$$E : y^2 + xy = x^3 + ax^2 + b$$

with $a, b \in \mathbb{F}_{2^n}$.

- Semaev's summation polynomials (2004)

  $$S_2(X_1, X_2) = X_1 + X_2,$$
  $$S_3(X_1, X_2, X_3) = X_1^2X_2^2 + X_1^2X_3^2 + X_1X_2X_3 + X_2^2X_3^2 + b,$$

  For $m \geq 4$

  $$S_m(X_1, \ldots, X_m) =$$
  $$Res_X(S_{m-k}(X_1, \ldots, X_{m-k-1}, X), S_{k+2}(X_{m-k}, \ldots, X_m, X))$$

Index calculus on elliptic curve groups

Let $\mathbb{F}_{2^n}$ be a finite field and E be an elliptic curve defined by

$$E : y^2 + xy = x^3 + ax^2 + b$$

with $a, b \in \mathbb{F}_{2^n}$.

- Semaev's summation polynomials (2004)

$$S_2(X_1, X_2) = X_1 + X_2,$$
$$S_3(X_1, X_2, X_3) = X_1^2X_2^2 + X_1^2X_3^2 + X_1X_2X_3 + X_2^2X_3^2 + b,$$

For $m \geq 4$

$$S_m(X_1, \ldots, X_m) =$$
$$Res_X(S_{m-k}(X_1, \ldots, X_{m-k-1}, X), S_{k+2}(X_{m-k}, \ldots, X_m, X))$$

For $P_1, \ldots, P_m \in E(\mathbb{F}_{2^n})$

$$P_1 + \ldots + P_m = \mathcal{O} \iff S_m(\mathbf{x}_{P_1}, \ldots, \mathbf{x}_{P_m}) = 0$$

Index calculus on elliptic curve groups

- Gaudry and Diem (2008 and 2009)
  Solving the point decomposition problem (PDP) for elliptic curves over extension fields, using Semaev's summation polynomials.
- Symmetrization
  Rewrite S_m in terms of the elementary symmetric polynomials

$$\begin{aligned} e_1 &= \sum_{1 \le i_1 \le m} X_{i_1}, \\ e_2 &= \sum_{1 \le i_1, i_2 \le m} X_{i_1} X_{i_2}, \\ &\dots \\ e_m &= \prod_{1 \le i \le m} X_i. \end{aligned}$$

PDP algebraic model

Our focus : $E(\mathbb{F}_{2^n})$, where n is prime.

PDP algebraic model

Our focus : $E(\mathbb{F}_{2^n})$, where n is prime.

Choice of a factor base : an l-dimensional vector subspace V of $\mathbb{F}_{2^n}/\mathbb{F}_2$. When $l \sim \frac{n}{m}$ the system has a reasonable chance to have a solution.

PDP algebraic model

Our focus : $E(\mathbb{F}_{2^n})$, where n is prime.

Choice of a factor base : an l-dimensional vector subspace V of $\mathbb{F}_{2^n}/\mathbb{F}_2$. When $l \sim \frac{n}{m}$ the system has a reasonable chance to have a solution.

Defining the PDP for this case:
Given an l-dimensional vector subspace V of $\mathbb{F}_{2^n}/\mathbb{F}_2$ find $(\mathbf{x}_1, \ldots, \mathbf{x}_m) \in V^m$ such that $S_m(\mathbf{x}_1, \ldots, \mathbf{x}_m) = 0$.

PDP algebraic model

Our focus : $E(\mathbb{F}_{2^n})$, where n is prime.

Choice of a factor base : an l-dimensional vector subspace V of $\mathbb{F}_{2^n}/\mathbb{F}_2$. When $l \sim \frac{n}{m}$ the system has a reasonable chance to have a solution.

Defining the PDP for this case:
Given an l-dimensional vector subspace V of $\mathbb{F}_{2^n}/\mathbb{F}_2$ find $(\mathbf{x}_1, \ldots, \mathbf{x}_m) \in V^m$ such that $S_m(\mathbf{x}_1, \ldots, \mathbf{x}_m) = 0$.

Weil descent : rewrite the equation $S_m(\mathbf{x}_1, \ldots, \mathbf{x}_m) = 0$ as a system of n equations over $\mathbb{F}_2$.

PDP algebraic model

Let t be a root of a defining polynomial of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

X_i-variables

$$X_1 = c_{1,0} + \ldots + c_{1,l-1}t^{l-1}$$
$$X_2 = c_{2,0} + \ldots + c_{2,l-1}t^{l-1}$$
$$\ldots$$
$$X_m = c_{m,0} + \ldots + c_{m,l-1}t^{l-1}$$

e_i-variables

$$e_1 = d_{1,0} + \ldots + d_{1,l-1}t^{l-1}$$
$$e_2 = d_{2,0} + \ldots + d_{2,2l-2}t^{2l-2}$$
$$\ldots$$
$$e_m = d_{m,0} + \ldots + d_{m,m(l-1)}t^{m(l-1)}$$

PDP algebraic model

Two sets of equations

- Equations defining symmetric polynomials

$$d_{1,0} = c_{1,0} + \ldots + c_{m,0}$$
$$d_{1,1} = c_{1,1} + \ldots + c_{m,1}$$
$$\ldots$$
$$d_{m,m(l-1)} = c_{1,l} \cdot \ldots \cdot c_{m,l}.$$

- Equations derived from the Weil descent

PDP algebraic model

Two sets of equations

- Equations defining symmetric polynomials

$$d_{1,0} = c_{1,0} + \ldots + c_{m,0}$$
$$d_{1,1} = c_{1,1} + \ldots + c_{m,1}$$
$$\ldots$$
$$d_{m,m(l-1)} = c_{1,l} \cdot \ldots \cdot c_{m,l}.$$

- Equations derived from the Weil descent

The system is commonly solved using Gröbner basis methods.

Algebraic model to SAT-reasoning model

Variables in $\mathbb{F}_2$:

$\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6$.

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_4 + \mathbf{x}_5 \cdot \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_4 + \mathbf{x}_5 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_2 \cdot \mathbf{x}_4 + 1 = 0$$
$$\mathbf{x}_2 + \mathbf{x}_5 + \mathbf{x}_2 \cdot \mathbf{x}_4 + \mathbf{x}_5 \cdot \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_6 + 1 = 0$$

$$(x_1 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge$$
$$(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus (x_2 \wedge x_4)) \wedge$$
$$(x_2 \oplus x_5 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$

Algebraic model to SAT-reasoning model

Add new variable x_7 to substitute the conjunction $x_2 \wedge x_4$. We have that

$$x_7 \Leftrightarrow (x_2 \wedge x_4)$$

$$(x_7 \Rightarrow (x_2 \wedge x_4)) \wedge ((x_2 \wedge x_4) \Rightarrow x_7)$$

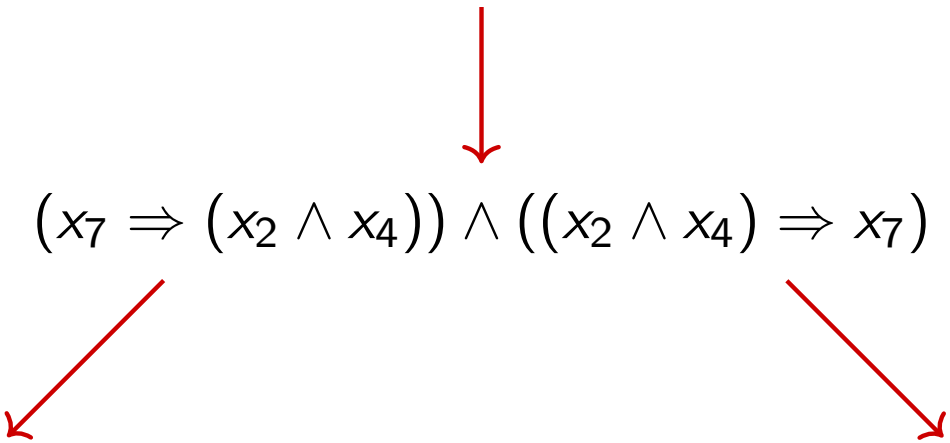
$$\neg x_7 \vee (x_2 \wedge x_4) \qquad \neg(x_2 \wedge x_4) \vee x_7$$

$$(\neg x_7 \vee x_2) \wedge (\neg x_7 \vee x_4) \qquad \neg x_2 \vee \neg x_4 \vee x_7$$

Algebraic model to SAT-reasoning model

Add new variable x_7 to substitute the conjunction $x_2 \wedge x_4$. We have that

$$x_7 \Leftrightarrow (x_2 \wedge x_4)$$



$$(x_7 \Rightarrow (x_2 \wedge x_4)) \wedge ((x_2 \wedge x_4) \Rightarrow x_7)$$

$$\neg x_7 \vee (x_2 \wedge x_4) \qquad \neg(x_2 \wedge x_4) \vee x_7$$

$$(\neg x_7 \vee x_2) \wedge (\neg x_7 \vee x_4) \qquad \neg x_2 \vee \neg x_4 \vee x_7$$

Algebraic model to SAT-reasoning model

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(x_1 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge$$
$$(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus (x_2 \wedge x_4)) \wedge$$
$$(x_2 \oplus x_5 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$

$$(\neg x_7 \vee x_2) \wedge$$
$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_1 \oplus x_7 \oplus x_8) \wedge$$
$$(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$

Algebraic model to SAT-reasoning model

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

- Literal

Algebraic model to SAT-reasoning model

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

- Literal
- OR-clause

Algebraic model to SAT-reasoning model

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

- Literal
- OR-clause
- XOR-clause

Algebraic model to SAT-reasoning model

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

- Literal
- OR-clause
- XOR-clause
- CNF formula

Algebraic model to SAT-reasoning model

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

- Literal
- OR-clause
- XOR-clause
- CNF formula
- Propositional satisfiability problem (SAT)

Unit propagation

Assigning literal l to TRUE will lead to :

1. Every clause containing l is removed (since the clause is satisfied).
2. In every clause that contains $\neg l$ this literal is deleted (since it can not contribute to the clause being satisfied).

- Propagation - obtaining a *unit clause* (clause containing a single literal) $\rightarrow$ the remaining literal is set to TRUE.
- Conflict - it exists at least one clause with all literals assigned to FALSE.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

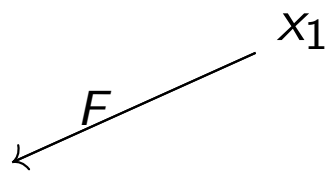
$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_2) \wedge$$
$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_1 \oplus x_7 \oplus x_8) \wedge$$
$$(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



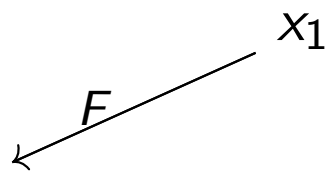
Assigned: $x_1 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_2) \wedge$$
$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(\cancel{x_1} \oplus x_7 \oplus x_8) \wedge$$
$$(\cancel{x_1} \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



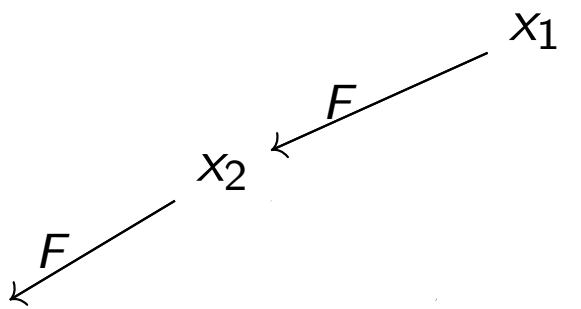
Assigned: $x_1 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee \cancel{x_2}) \wedge$$
$$(\neg x_7 \vee x_4) \wedge$$
$$\cancel{(\neg x_2 \vee \neg x_4 \vee x_7) \wedge}$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow F$;

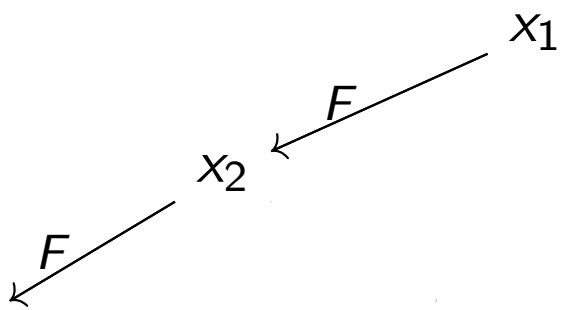
Propagation: $x_7 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$\cancel{(\neg x_7 \vee x_2)} \wedge$$
$$\cancel{(\neg x_7 \vee x_4)} \wedge$$
$$\cancel{(\neg x_2 \vee \neg x_4 \vee x_7)} \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(\cancel{x_7} \oplus x_8) \wedge$$
$$(\cancel{x_2} \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus \cancel{x_7}) \wedge$$
$$(\cancel{x_2} \oplus x_5 \oplus \cancel{x_7} \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F; x_2 \leftarrow F; x_7 \leftarrow F;$

Propagation: $x_8 \leftarrow T;$

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\cancel{\neg x_8} \vee x_5) \wedge$

$(\cancel{\neg x_8} \vee x_6) \wedge$

$\cancel{(\neg x_5 \vee \neg x_6 \vee x_8) \wedge}$

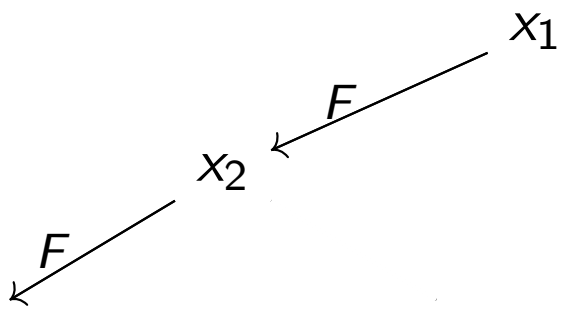
$(x_8) \wedge$

$(x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4) \wedge$

$(x_5 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow F; x_2 \leftarrow F; x_7 \leftarrow F;$
$x_8 \leftarrow T;$

Propagation: $x_5 \leftarrow T; x_6 \leftarrow T;$

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$\cancel{(\neg x_8 \vee x_5) \wedge}$

$\cancel{(\neg x_8 \vee x_6) \wedge}$

$\cancel{(\neg x_5 \vee \neg x_6 \vee x_8) \wedge}$

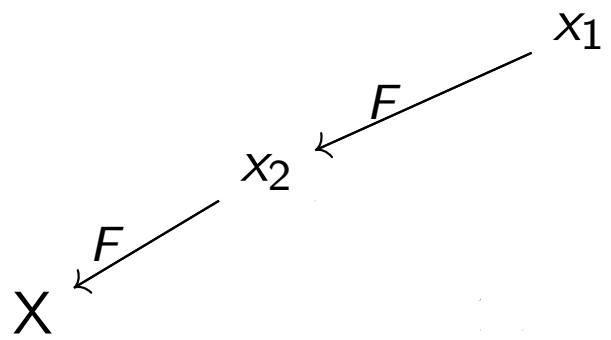
$(\cancel{x_8}\, T) \wedge$

$(x_4 \oplus \cancel{x_5}\, T) \wedge$

$(x_3 \oplus x_4) \wedge$

$(\cancel{x_5}\, T \oplus \cancel{x_8}\, T) \wedge$

$(x_3 \oplus x_4 \oplus \cancel{x_6}\, T)$



Assigned: $x_1 \leftarrow F; x_2 \leftarrow F; x_7 \leftarrow F;$
$x_8 \leftarrow T; x_5 \leftarrow T; x_6 \leftarrow T;$

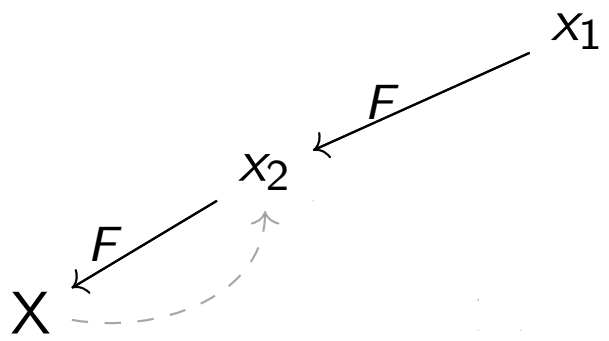
Conflict on fourth XOR-clause.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_2) \wedge$$
$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F$;

Backtrack.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_7 \vee x_2) \wedge$~~

$(\neg x_7 \vee x_4) \wedge$

$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

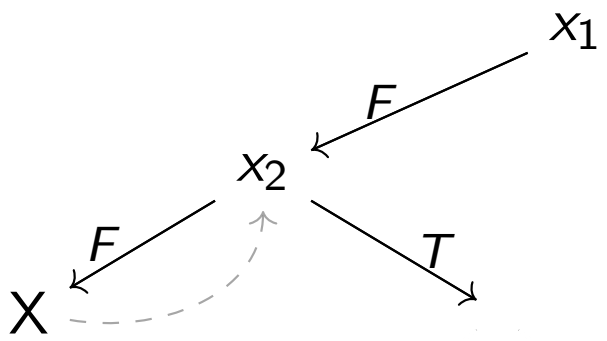
$(x_7 \oplus x_8) \wedge$

$(x_2 \, T \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4 \oplus x_7) \wedge$

$(x_2 \, T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



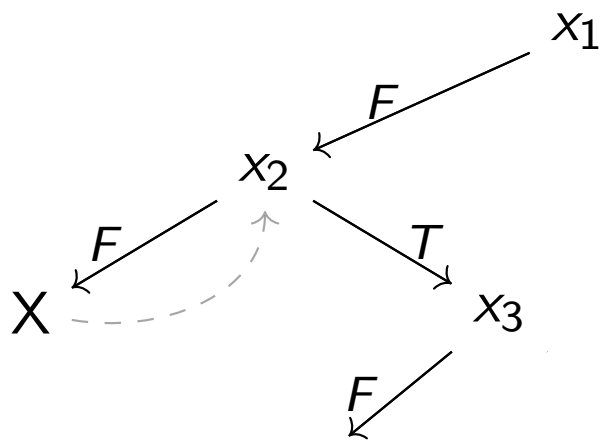
Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(T \oplus x_4 \oplus x_5) \wedge$$
$$(\cancel{x_3} \oplus x_4 \oplus x_7) \wedge$$
$$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(\cancel{x_3} \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee \cancel{x_4}) \wedge$

$\cancel{(\neg x_4 \vee x_7) \wedge}$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

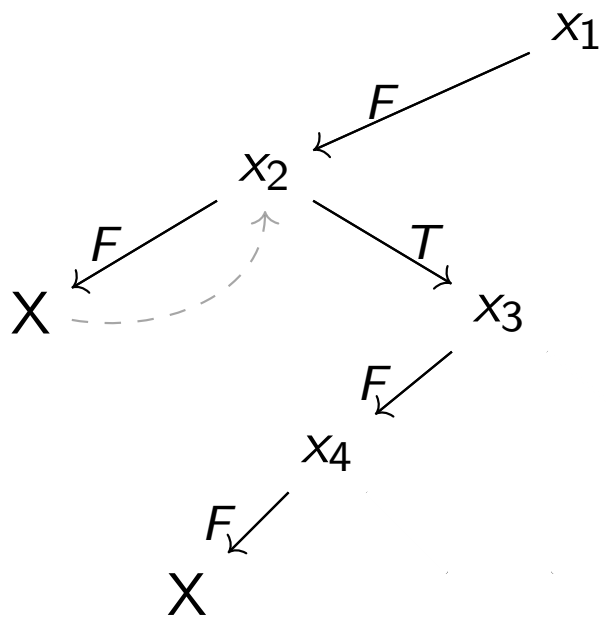
$(x_7 \oplus x_8) \wedge$

$(T \oplus \cancel{x_4} \oplus x_5) \wedge$

$(\cancel{x_4} \oplus x_7) \wedge$

$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(\cancel{x_4} \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow F$; $x_4 \leftarrow F$;

Propagation: $x_7 \leftarrow F$; $x_7 \leftarrow T$;

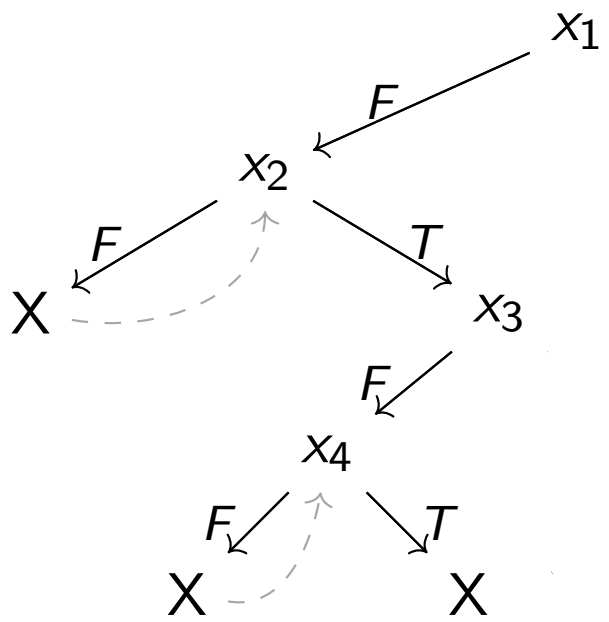
Conflict.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$\cancel{(\neg x_7 \vee x_4) \wedge}$$
$$(\cancel{\neg x_4} \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(T \oplus \cancel{x_4}\, T \oplus x_5) \wedge$$
$$(\cancel{x_4}\, T \oplus x_7) \wedge$$
$$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(\cancel{x_4}\, T \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow F$; $x_4 \leftarrow F$;

Propagation: $x_7 \leftarrow T$; $x_7 \leftarrow F$; ...

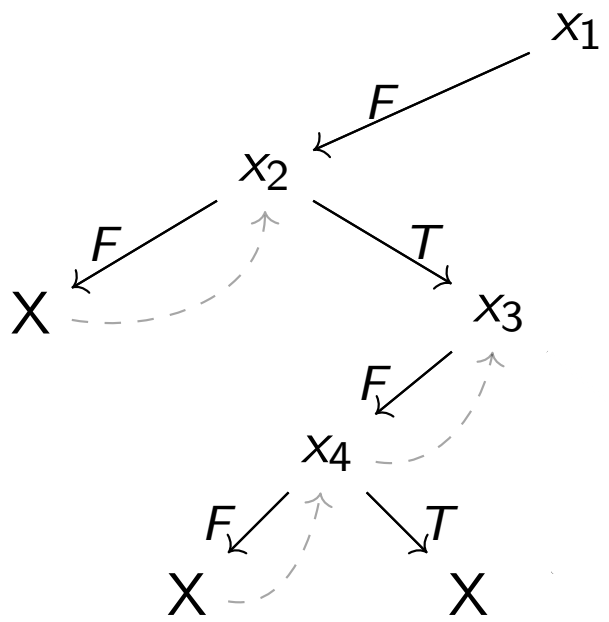
Conflict.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(T \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$;

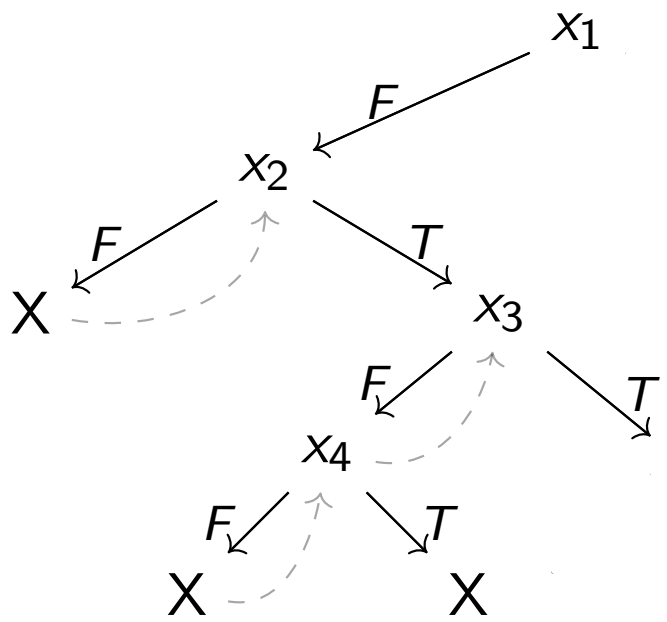
Backtrack

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(T \oplus x_4 \oplus x_5) \wedge$$
$$(\cancel{x_3}\, T \oplus x_4 \oplus x_7) \wedge$$
$$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(\cancel{x_3}\, T \oplus x_4 \oplus x_6)$$



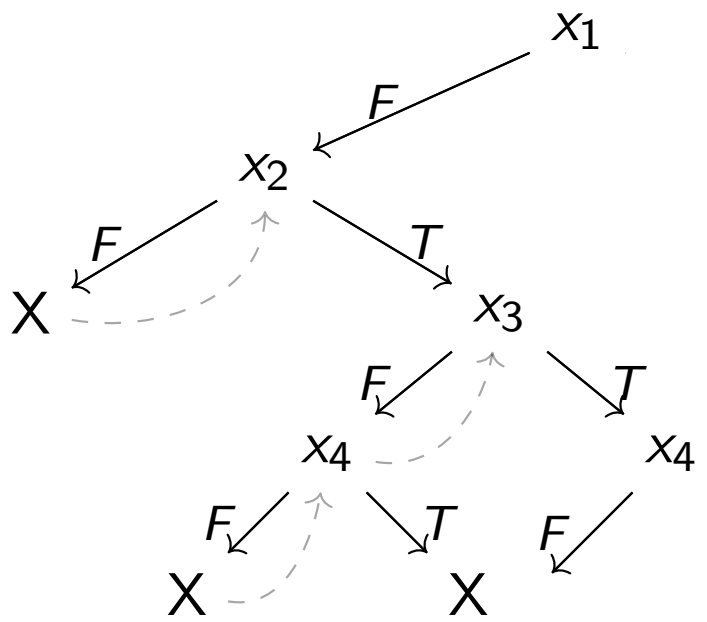
Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(T \oplus x_4 \oplus x_5) \wedge$$
$$(T \oplus x_4 \oplus x_7) \wedge$$
$$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(T \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$;

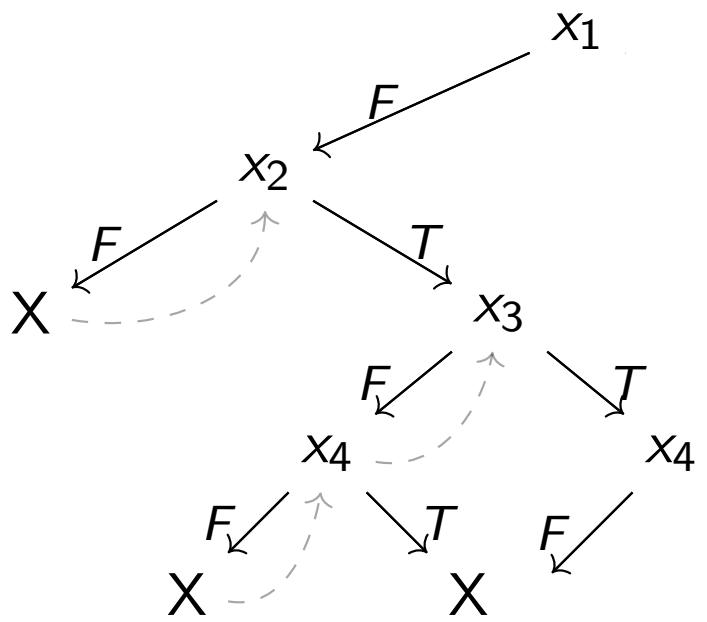
Propagated: $x_7 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(\cancel{x_7} \oplus x_8) \wedge$$
$$(T \oplus \cancel{x_4} \oplus x_5) \wedge$$
$$(T \oplus \cancel{x_4} \oplus \cancel{x_7}) \wedge$$
$$(T \oplus x_5 \oplus \cancel{x_7} \oplus x_8) \wedge$$
$$(T \oplus \cancel{x_4} \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow F$; $x_7 \leftarrow F$;

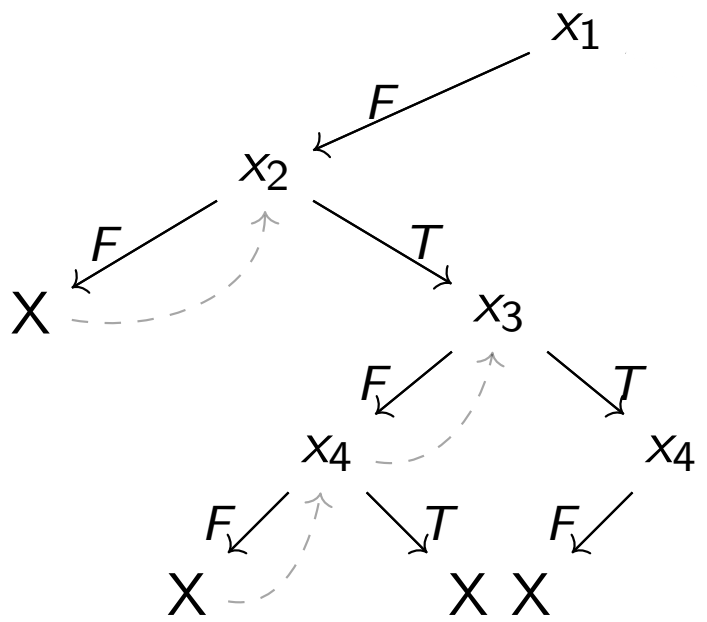
Propagated: $x_8 \leftarrow T$; $x_5 \leftarrow F$; $x_6 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\cancel{\neg x_8} \vee \cancel{x_5}) \wedge$$
$$(\cancel{\neg x_8} \vee \cancel{x_6}) \wedge$$
$$\cancel{(\neg x_5 \vee \neg x_6 \vee x_8) \wedge}$$
$$(\cancel{x_8}\, T) \wedge$$
$$(T \oplus \cancel{x_5}) \wedge$$
$$(T) \wedge$$
$$(T \oplus \cancel{x_5} \oplus \cancel{x_8}\, T) \wedge$$
$$(T \oplus \cancel{x_6})$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow F$; $x_7 \leftarrow F$; $x_8 \leftarrow T$; $x_5 \leftarrow F$; $x_6 \leftarrow F$;

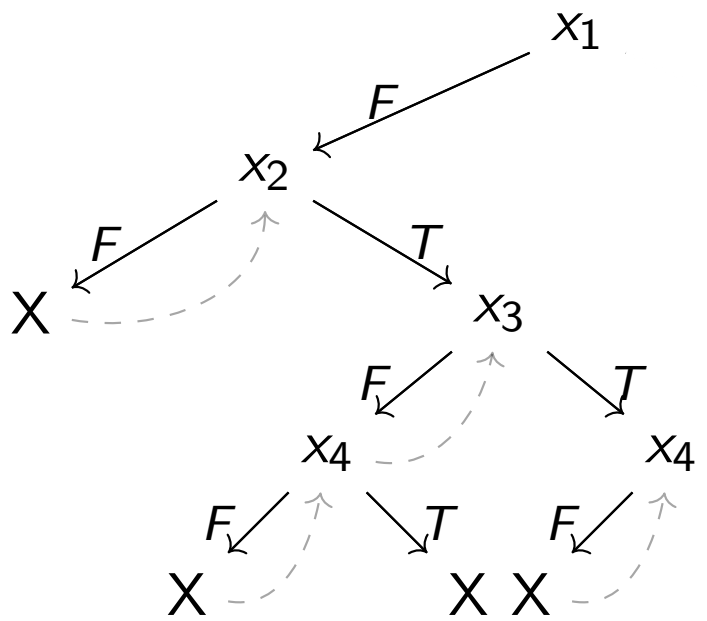
Conflict.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_7 \oplus x_8) \wedge \\
&(T \oplus x_4 \oplus x_5) \wedge \\
&(T \oplus x_4 \oplus x_7) \wedge \\
&(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(T \oplus x_4 \oplus x_6)
\end{aligned}
$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$;

Backtrack.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_7 \vee x_4) \wedge$~~

~~$(\neg x_4$~~ $\vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

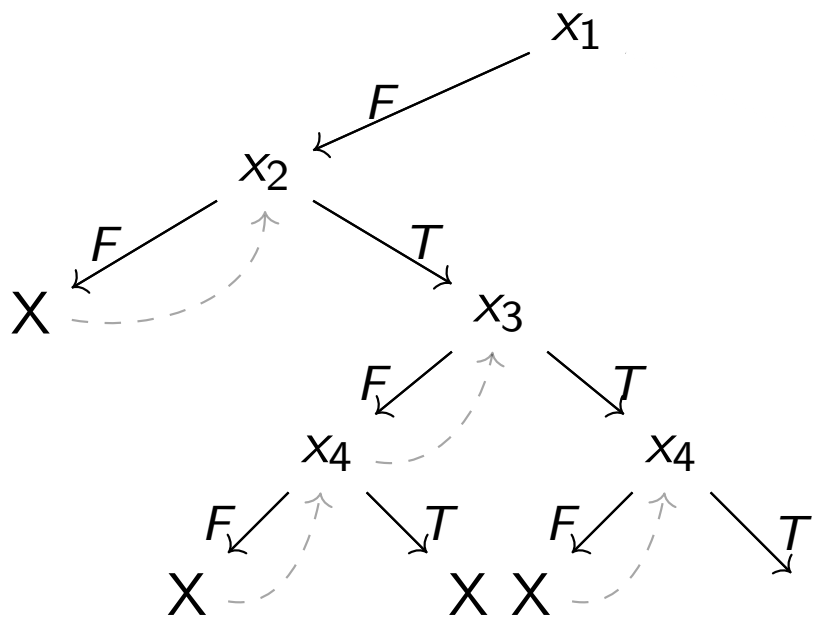
$(\cancel{x_7} T \oplus x_8) \wedge$

$(T \oplus \cancel{x_4} T \oplus x_5) \wedge$

$(T \oplus \cancel{x_4} T \oplus \cancel{x_7} T) \wedge$

$(T \oplus x_5 \oplus \cancel{x_7} T \oplus x_8) \wedge$

$(T \oplus \cancel{x_4} T \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow T$;

Propagation: $x_7 \leftarrow T$; $x_5 \leftarrow T$; $x_6 \leftarrow T$; $x_8 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_8 \vee x_5) \wedge$~~

~~$(\neg x_8 \vee x_6) \wedge$~~

~~$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$~~

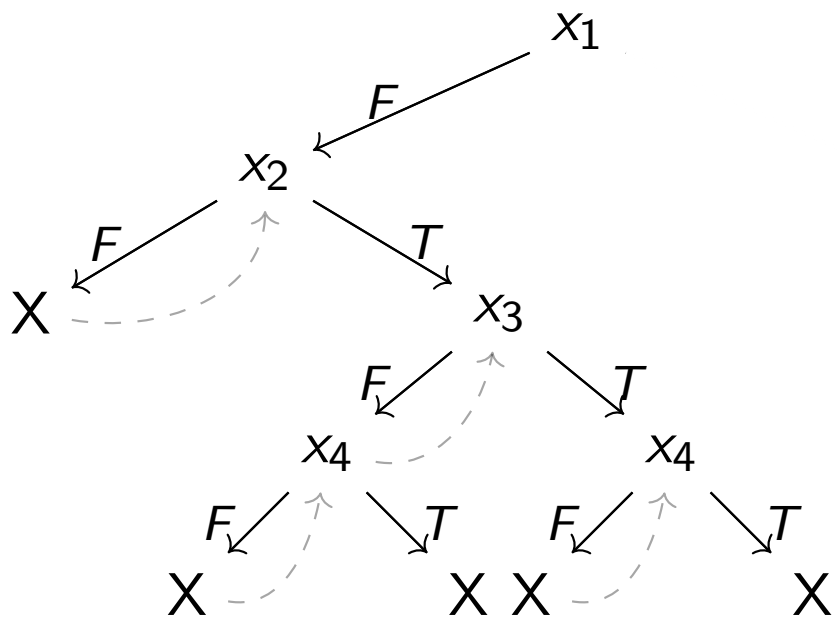
$(T) \wedge$

$(T) \wedge$

$(T) \wedge$

$(T) \wedge$

$(T) \wedge$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow T$; $x_7 \leftarrow T$; $x_5 \leftarrow T$; $x_6 \leftarrow T$; $x_8 \leftarrow F$;

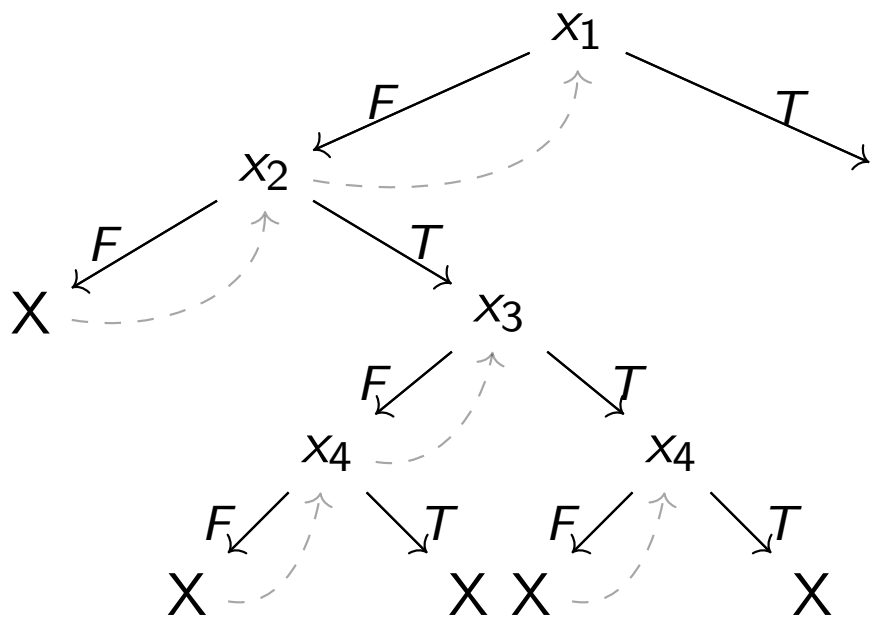
Conflict.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(\cancel{x_1}\, T \oplus x_7 \oplus x_8) \wedge \\
&(\cancel{x_1}\, T \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$



Assigned: $x_1 \leftarrow T$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee \cancel{x_2}) \wedge$

$(\neg x_7 \vee x_4) \wedge$

$\cancel{(\neg x_2 \vee \neg x_4 \vee x_7) \wedge}$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

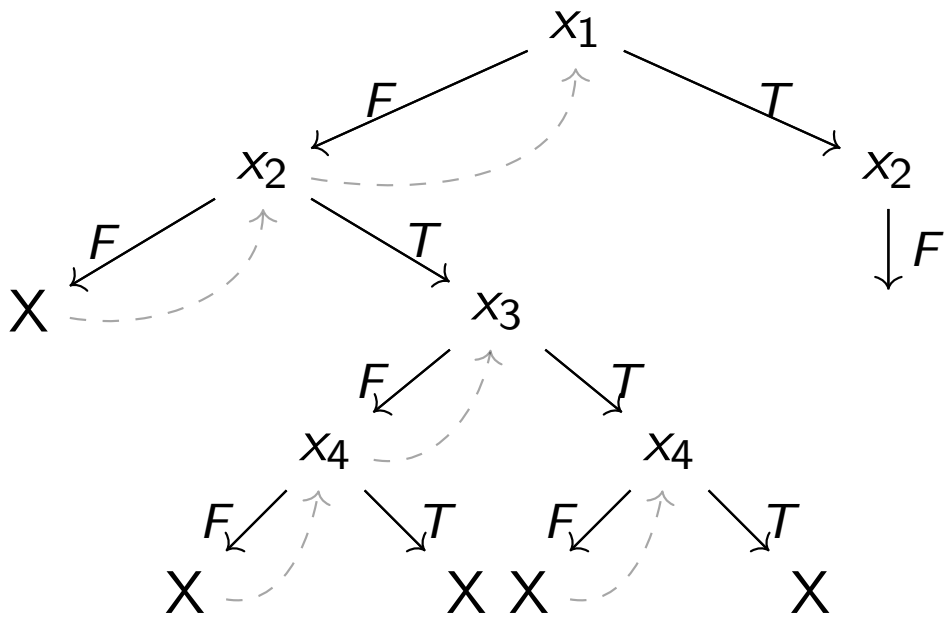
$(T \oplus x_7 \oplus x_8) \wedge$

$(T \oplus x_2 \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4 \oplus x_7) \wedge$

$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow T$; $x_2 \leftarrow F$;

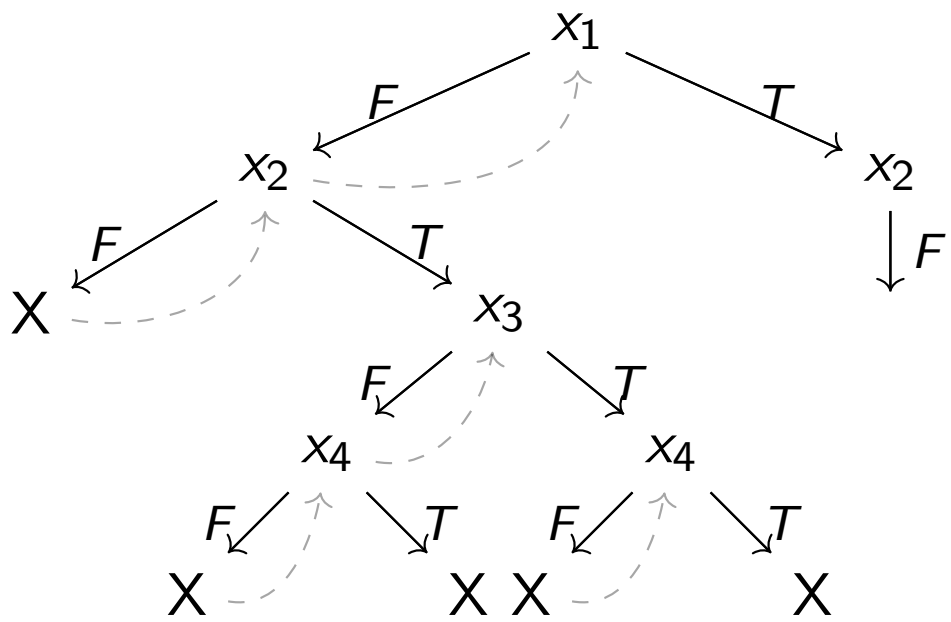
Propagation: $x_7 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(T \oplus \cancel{x_7} \oplus x_8) \wedge$$
$$(T \oplus \cancel{x_2} \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus \cancel{x_7}) \wedge$$
$$(\cancel{x_2} \oplus x_5 \oplus \cancel{x_7} \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow T$; $x_2 \leftarrow F$; $x_7 \leftarrow F$;

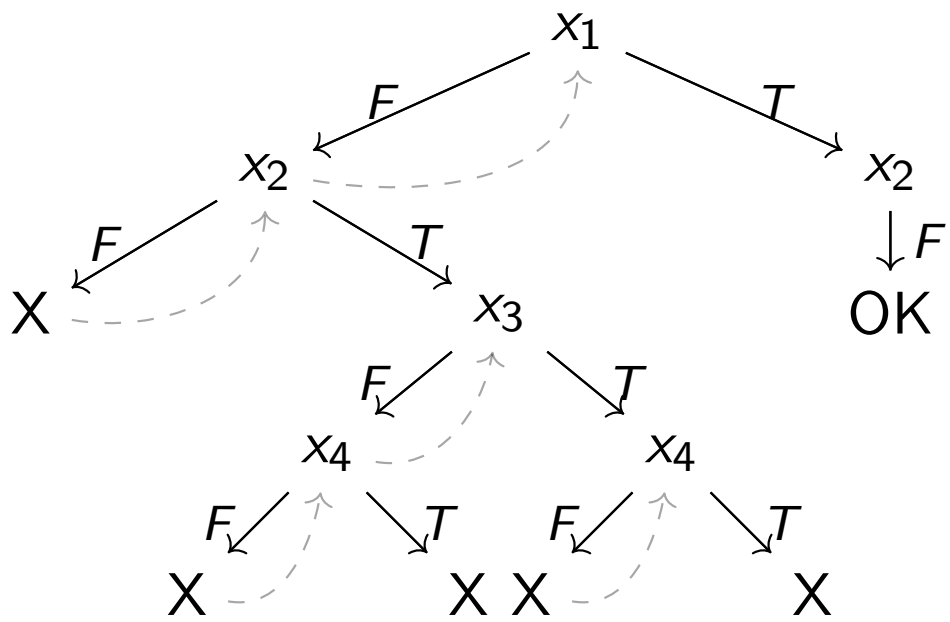
Propagation: $x_8 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$\cancel{(\neg x_8 \vee x_5) \wedge}$$
$$\cancel{(\neg x_8 \vee x_6) \wedge}$$
$$(\neg x_5 \vee \neg x_6 \vee \cancel{x_8}) \wedge$$
$$(T \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4) \wedge$$
$$(x_5 \oplus \cancel{x_8}) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow T$; $x_2 \leftarrow F$; $x_7 \leftarrow F$; $x_8 \leftarrow F$;

Propagation: $x_5 \leftarrow T$; ... $x_4 \leftarrow T$; ... $x_3 \leftarrow F$; ... $x_6 \leftarrow F$;

WDSat algorithm

- Based on the Davis-Putnam-Logemann-Loveland (DPLL) algorithm.
- Recursively building a binary search-tree of height equivalent (at worst) to the number of *elementary* variables.
- Adapted for XOR-reasoning.

		Gröbner model		CNF model		XOR model		
l	n	#Vars	#Equations	#Vars	#CNF-clauses	#Vars	#CNF-clauses	#XOR-clauses
6	17	51	50	4686	18237	767	2364	50
	19	51	52	5019	19577	767	2364	52
7	19	60	58	6981	27216	1101	3466	58
	23	60	62	8223	32201	1101	3466	62
8	23	69	68	11036	43210	1510	4835	68
	26	69	71	12074	47374	1510	4835	71
9	37	78	88	20969	82721	2000	6495	88
	47	78	98	25456	100709	2000	6495	98
	59	78	110	31942	126702	2000	6495	110
	67	78	118	35917	142632	2000	6495	118

Table: Number of variables and equations/clauses for three different models.

WDSat

Three reasoning modules

1. CNF module
   Performs fast unit propagation on CNF-clauses.
2. XORSET module
   Performs unit propagation on the parity constraints. When all except one literal in a XOR clause is assigned, we infer the truth value of the last literal according to parity reasoning.
3. XORGAUSS module
   Performs Gaussian elimination on the XOR system.

The three modules are combined when a truth value is assigned to a literal.

WDSat - breaking symmetry

- Exploiting the symmetry of Semaev's summation polynomials: when $\mathbf{x}_1, ..., \mathbf{x}_m$ is a solution, all permutations of this set are a solution as well.
- Establish the following constraint $\mathbf{x}_1 \leq \mathbf{x}_2 \leq \ldots \leq \mathbf{x}_m$.
- Implement constraint in the solver using a tree-pruning-like technique.
- Optimizes the complexity by a factor of $m!$.

Experimental results

			SATisfiable			UNSATisfiable		
Approach	l	n	Runtime	#Conflicts	Memory	Runtime	#Conflicts	Memory
Gröbner basis	6	17	207.220	NA	3601	142.119	NA	3291
		19	215.187	NA	3940	155.765	NA	4091
	7	19	3854.708	NA	38763	2650.696	NA	38408
		23	3128.844	NA	35203	2286.136	NA	35162
WDSat	6	17	.601	49117	1.4	3.851	254686	1.4
		19	.470	38137	1.4	3.913	255491	1.4
	7	19	9.643	534867	16.7	44.107	2073089	16.7
		23	9.303	477632	16.7	47.347	2067168	16.7
WDSat breaking-sym	6	17	.220	17792	1.4	.605	43875	1.4
		19	.243	19166	1.4	.639	44034	1.4
	7	19	2.205	130062	1.4	6.859	351353	1.4
		23	3.555	189940	1.4	7.478	350257	1.4

Table: Comparing the WDSat approach with the Gröbner basis approach for solving the PDP. Running times are in seconds and memory is in MB.

Experimental results

		SATisfiable			UNSATisfiable		
l	n	Runtime	#Conflicts	Memory	Runtime	#Conflicts	Memory
8	23	29.584	1145966	17.0	81.767	2800335	17.0
9	37	447	10557129	17.1	1048	22396994	17.1
	47	609	12675174	17.2	1167	22381494	17.2
	59	611	11297325	17.3	1327	22390211	17.3
	67	677	11608420	17.4	1430	22388053	17.4
10	47	5847	95131900	17.3	11963	179019409	17.3
	59	6849	97254458	17.4	13649	179067171	17.4
	67	6530	88292215	17.4	14555	179052277	17.4
	79	7221	86174432	17.5	16294	179043408	17.5
11	59	64162	727241718	19.2	135801	1432191354	19.2
	67	70075	741222864	19.3	145357	1432183842	19.3
	79	61370	599263451	19.4	161388	1432120827	19.4
	89	85834	736610196	19.5	175718	1432099666	19.5

Table: Experimental results using the WDSAT solver with breaking symmetry. Running times are in seconds and memory is in MB.

Conclusion

- When solving the PDP for prime degree extension fields $\mathbb{F}_2$, Gröbner basis methods can be replaced with a SAT-based approach.
- The dedicated SAT-solver, WDSAT, yields significantly faster running times.
- The memory is no longer a constraint for the PDP.
- Preprint at `https://eprint.iacr.org/2019/313`