Towards Efficient SAT Solving using XOR-OR-AND Normal Forms

work-in-progress

Julian Danner

joint work with B. Andraschko and M. Kreuzer

UNIVERSITY OF PASSAU

XOR-OR-AND Normal Form

XNF

$$\bigwedge \begin{array}{l} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{array}$$

XOR-OR-AND Normal Form

XNF

Lineral

$$\bigwedge \begin{array}{l} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{array}$$

XOR-OR-AND Normal Form

XNF

Lineral

$$\bigwedge \begin{cases} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{cases}$$

XNF clause

XOR-OR-AND Normal Form

XNF

```
p xnf 3 4
-1+3 2 0
1+2+3 -3 0
3 1+2 0
-1+2 1 2 0
```

$$\longleftrightarrow \quad \bigwedge \begin{array}{l} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{array}$$

Lineral: $(\neg X_1 \oplus X_3)$

XNF clause: $X_3 \vee (X_1 \oplus X_2)$

XOR-OR-AND Normal Form

XNF

```
p xnf 3 4
-1+3 2 0
1+2+3 -3 0
3 1+2 0
-1+2 1 2 0
```

$\longleftrightarrow$

Lineral

$$\bigwedge \begin{cases} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{cases}$$

XNF clause

Proposition Every formula is equisatisfiable to a formula in 2-XNF.

$$Y \leftrightarrow (L_1 \vee L_2) \quad \equiv \quad (Y \vee \neg L_2) \wedge ((\neg Y \oplus L_1) \vee L_2).$$

XOR-OR-AND Normal Form

XNF

```
p xnf 3 4
-1+3 2 0
1+2+3 -3 0
3 1+2 0
-1+2 1 2 0
```

$\longleftrightarrow$

$$\bigwedge \begin{cases} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{cases}$$

Lineral: $(\neg X_1 \oplus X_3)$

XNF clause: $X_3 \vee (X_1 \oplus X_2)$

Proposition Every formula is equisatisfiable to a formula in 2-XNF.

$$Y \leftrightarrow (L_1 \vee L_2) \quad \equiv \quad (Y \vee \neg L_2) \wedge ((\neg Y \oplus L_1) \vee L_2).$$

$\longrightarrow$ allows implication graph based solving

XOR-OR-AND Normal Form

XNF

```
p xnf 3 4
-1+3 2 0
1+2+3 -3 0
3 1+2 0
-1+2 1 2 0
```

$\longleftrightarrow$

Lineral

$$\bigwedge \begin{cases} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{cases}$$

XNF clause

Proposition Every formula is equisatisfiable to a formula in 2-XNF.

$$Y \leftrightarrow (L_1 \vee L_2) \quad \equiv \quad (Y \vee \neg L_2) \wedge ((\neg Y \oplus L_1) \vee L_2).$$

$\longrightarrow$ allows implication graph based solving

SCCs, Failed Linerals, ...

XOR-OR-AND Normal Form

XNF

```
p xnf 3 4
-1+3 2 0
1+2+3 -3 0
3 1+2 0
-1+2 1 2 0
```

$\longleftrightarrow$

$$\bigwedge \begin{array}{l} (\neg X_1 \oplus X_3) \vee X_2 \\ (X_1 \oplus X_2 \oplus X_3) \vee \neg X_3 \\ X_3 \vee (X_1 \oplus X_2) \\ (\neg X_1 \oplus X_2) \vee X_1 \vee X_2 \end{array}$$

Lineral: $(\neg X_1 \oplus X_3)$

XNF clause: $X_3 \vee (X_1 \oplus X_2)$

Proposition Every formula is equisatisfiable to a formula in 2-XNF.

$$Y \leftrightarrow (L_1 \vee L_2) \quad \equiv \quad (Y \vee \neg L_2) \wedge ((\neg Y \oplus L_1) \vee L_2).$$

$\longrightarrow$ allows implication graph based solving

implication graph: SCCs, Failed Linerals, ...

Equivalent XNF Clauses

Logic		Algebra
$X_1 \oplus X_2$	$\longleftrightarrow$	$x_1 + x_2 + 1$
$(X_1 \oplus X_2) \vee (\neg X_3 \oplus X_4)$		$(x_1 + x_2 + 1) \cdot (x_3 + x_4)$

Equivalent XNF Clauses

Logic		Algebra
$X_1 \oplus X_2$	$\longleftrightarrow$	$x_1 + x_2 + 1$
$\{ X_1 \oplus X_2, \ \neg X_3 \oplus X_4 \}$		$\{ x_1 + x_2 + 1, \ x_3 + x_4 \}$

Equivalent XNF Clauses

Logic		Algebra
$X_1 \oplus X_2$	$\longleftrightarrow$	$x_1 + x_2 + 1$
$\{X_1 \oplus X_2,\ \neg X_3 \oplus X_4\}$		$\{x_1 + x_2 + 1,\ x_3 + x_4\}$

Definition $C_1 \sim C_2$ iff $\mathcal{S}(C_1) = \mathcal{S}(C_2)$; $V_C = \langle 1 + C \rangle_{\mathbb{F}_2}$

Equivalent XNF Clauses

Logic		Algebra
$X_1 \oplus X_2$	$\longleftrightarrow$	$x_1 + x_2 + 1$
$\{X_1 \oplus X_2, \ \neg X_3 \oplus X_4\}$		$\{x_1 + x_2 + 1, \ x_3 + x_4\}$

Definition $C_1 \sim C_2$ iff $\mathcal{S}(C_1) = \mathcal{S}(C_2)$; $\quad V_C = \langle 1 + C \rangle_{\mathbb{F}_2}$

Proposition

$$C_1 \sim C_2 \quad \Longleftrightarrow \quad V_{C_1} = V_{C_2} \text{ or } 1 \in V_{C_1} \cap V_{C_2}$$

Equivalent XNF Clauses

Logic		Algebra
$X_1 \oplus X_2$	$\longleftrightarrow$	$x_1 + x_2 + 1$
$\{ X_1 \oplus X_2,\ \neg X_3 \oplus X_4 \}$		$\{ x_1 + x_2 + 1,\ x_3 + x_4 \}$

Definition $C_1 \sim C_2$ iff $\mathcal{S}(C_1) = \mathcal{S}(C_2)$; $V_C = \langle 1 + C \rangle_{\mathbb{F}_2}$

Proposition

$$C_1 \sim C_2 \quad \Longleftrightarrow \quad V_{C_1} = V_{C_2} \text{ or } 1 \in V_{C_1} \cap V_{C_2}$$

Corollary For $i \neq j$

$$\{ L_1, \ldots, L_k \} \sim \{ L_1, \ldots, L_i \oplus L_j, \ldots, L_k \}$$

Equivalent XNF Clauses

Logic		Algebra
$X_1 \oplus X_2$	$\longleftrightarrow$	$x_1 + x_2 + 1$
$\{X_1 \oplus X_2,\ \neg X_3 \oplus X_4\}$		$\{x_1 + x_2 + 1,\ x_3 + x_4\}$

Definition $C_1 \sim C_2$ iff $\mathcal{S}(C_1) = \mathcal{S}(C_2)$; $\quad V_C = \langle 1 + C \rangle_{\mathbb{F}_2}$

Proposition

$$C_1 \sim C_2 \quad \Longleftrightarrow \quad V_{C_1} = V_{C_2} \text{ or } 1 \in V_{C_1} \cap V_{C_2}$$

Corollary For $i \neq j$

$$\{L_1, \ldots, L_k\} \sim \{L_1, \ldots, L_i \oplus L_j, \ldots, L_k\}$$

Corollary

$$C \text{ is a tautology} \quad \Longleftrightarrow \quad 1 \in V_C$$

`ANF_to_XNF` converts Algebraic Normal Form (ANF) to XNF.

`ANF_to_XNF` converts Algebraic Normal Form (ANF) to XNF.

ASCON-128	format	#vars	#cls/polys	avg cls len
–	ANF	6080	11 904	–
anf_to_xnf	XNF	12 224	17 920	1.64
SageMath	CNF	26 048	260 416	4.79
ApCoCoA	CNF-XOR	28 545	158 809	3.59
bosphorus	CNF	49 289	1 424 034	5.83

`ANF_to_XNF` converts Algebraic Normal Form (ANF) to XNF.

ASCON-128	format	#vars	#cls/polys	avg cls len
–	ANF	6080	11 904	–
anf_to_xnf	XNF	12 224	17 920	1.64
SageMath	CNF	26 048	260 416	4.79
ApCoCoA	CNF-XOR	28 545	158 809	3.59
bosphorus	CNF	49 289	1 424 034	5.83

$\longrightarrow$ cryptographic instances have *compact* representation

Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.

Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.

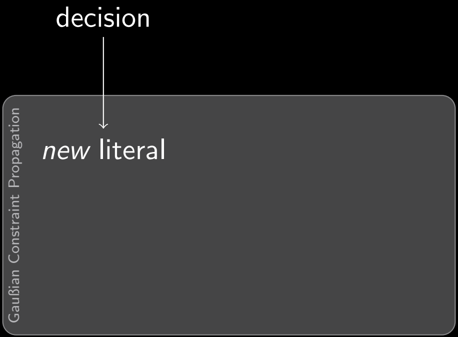
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.

decision

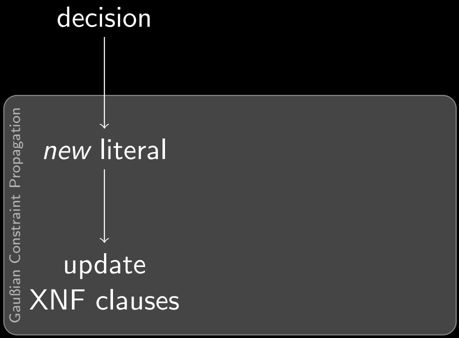
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



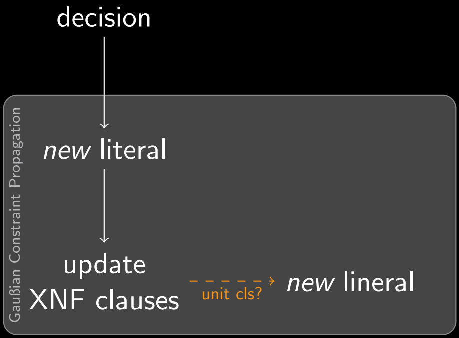
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



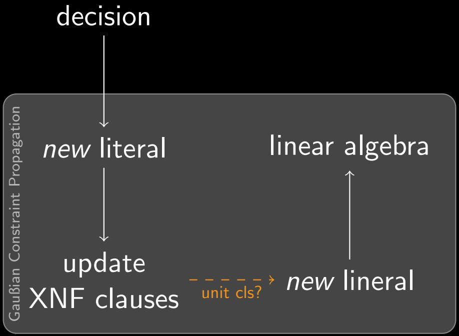
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



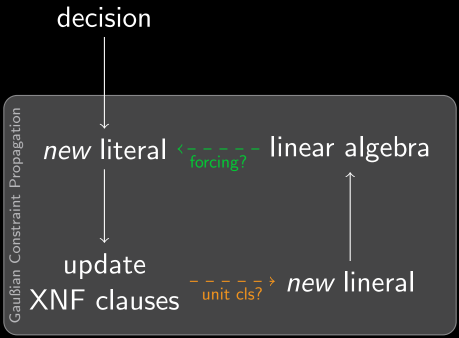
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



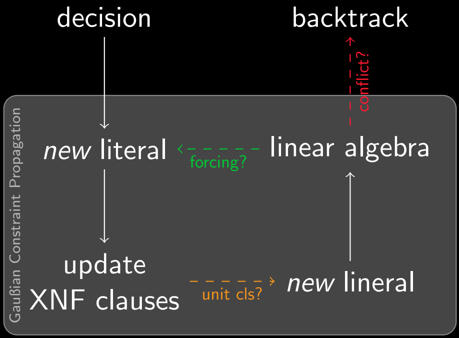
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



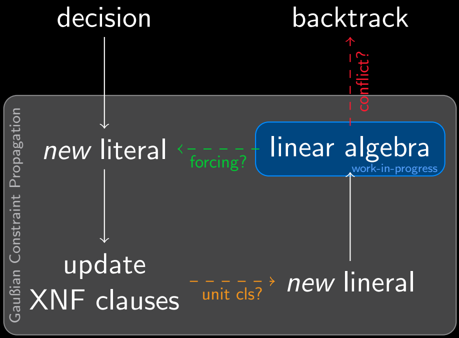
Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



Gaußian Constraint Propagation

Definition A lineral is called **forcing** if it is a literal.



Watched Linerals

Problem watching distinct literals from distinct linerals

$$\{ \quad X_1 \oplus X_2 \oplus X_3 \oplus X_4 \,, \quad X_1 \oplus X_2 \oplus X_5 \quad \}$$

Watched Linerals

Problem watching distinct literals from distinct linerals

$$\{ \quad X_1 \oplus X_2 \oplus X_3 \oplus X_4 , \quad X_1 \oplus X_2 \oplus X_5 \quad \}$$

Watched Linerals

Problem watching distinct literals from distinct linerals

$$\{ \quad X_1 \oplus X_2 \oplus X_3 \oplus X_4 \,, \quad X_1 \oplus X_2 \oplus X_5 \quad \}$$

Watched Linerals

Problem watching distinct literals from distinct linerals

$$\{ \quad X_1 \oplus X_2 \oplus X_3 \oplus X_4 , \quad X_1 \oplus X_2 \oplus X_5 \quad \}$$

Watched Linerals

Problem watching distinct literals from distinct linerals

$$\{ \quad X_1 \oplus X_2 \oplus X_3 \oplus X_4 , \quad X_1 \oplus X_2 \oplus X_5 \quad \}$$

$$\wr$$

$$\{ \quad X_1 \oplus X_2 \quad \}$$

might miss unit clauses!

Watched Linerals

Solution watch unshared literals from two distinct linerals

$$L_1 : \quad X_3 \oplus X_4 \quad \oplus \quad X_1 \oplus X_2$$

$$L_2 : \quad X_1 \oplus X_2 \quad \oplus \quad X_5$$

Watched Linerals

Solution watch unshared literals from two distinct linerals

$$L_1 : \quad X_3 \oplus X_4 \quad \oplus \quad X_1 \oplus X_2$$

$$L_2 : \quad X_1 \oplus X_2 \quad \oplus \quad X_5$$

Watched Linerals

Solution watch unshared literals from two distinct linerals

$$L_1 : \quad x_3 \oplus x_4 \quad \oplus \quad x_1 \oplus x_2$$

$$L_2 : \quad x_1 \oplus x_2 \quad \oplus \quad x_5$$

Watched Linerals

Solution watch unshared literals from two distinct linerals

$$L_1 : \quad X_3 \oplus X_4 \quad \oplus \quad X_1 \oplus X_2$$

$$L_2 : \quad X_1 \oplus X_2 \quad \oplus \quad X_5$$

Watched Linerals

Solution watch unshared literals from two distinct linerals, change representation if necessary

$$L_1: \quad X_3 \oplus X_4 \quad \oplus \quad X_1 \oplus X_2$$

$$L_1 \oplus L_2: \quad X_3 \oplus X_4 \quad \oplus \quad X_5$$

Watched Linerals

Solution watch unshared literals from two distinct linerals, change representation if necessary

$$L_1 : \quad X_3 \oplus X_4 \quad \oplus \quad X_1 \oplus X_2$$

$$L_1 \oplus L_2 : \quad X_3 \oplus X_4 \quad \oplus \quad X_5$$

$\longrightarrow$ swap *shared/unshared* parts

Watched Linerals

Solution watch unshared literals from two distinct linerals, change representation if necessary

$$L_1: \quad X_3 \oplus X_4 \quad \oplus \quad X_1 \oplus X_2$$

$$L_1 \oplus L_2: \quad X_3 \oplus X_4 \quad \oplus \quad X_5$$

$\longrightarrow$ swap *shared/unshared* parts

$\longrightarrow$ XNF clauses can be efficiently managed by watch-lists

Resolution

Towards CDCL

$$\frac{\{X_1, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_2, \neg X_3\}}$$

Resolution

Towards CDCL

$$\frac{\{X_1, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_2, \neg X_3\}}$$

$$\frac{\{X_1, \neg X_2, \neg X_3\} \qquad \{\neg X_1, X_2\}}{}$$

Resolution

Towards CDCL

$$\frac{\{X_1, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_2, \neg X_3\}} \qquad \frac{\{X_1, \neg X_2, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_1 \oplus X_2, \neg X_3\}}$$

Resolution

Towards CDCL

$$\frac{\{X_1, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_2, \neg X_3\}} \qquad \frac{\{X_1, \neg X_2, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_1 \oplus X_2, \neg X_3\}}$$

s-resolution [Horacek]

$$\frac{\bigcup_{i=1}^{s}\{L_i\} \cup F \qquad \bigcup_{i=1}^{s}\{\neg L_i\} \cup G}{\bigcup_{i=1}^{s-1}\{L_i \oplus L_{i+1}\} \cup F \cup G}$$

Resolution

Towards CDCL

$$\frac{\{X_1, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_2, \neg X_3\}} \qquad \frac{\{X_1, \neg X_2, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_1 \oplus X_2, \neg X_3\}}$$

s-resolution [Horacek]

$$\frac{\bigcup_{i=1}^{s}\{L_i\} \cup F \qquad \bigcup_{i=1}^{s}\{\neg L_i\} \cup G}{\bigcup_{i=1}^{s-1}\{L_i \oplus L_{i+1}\} \cup F \cup G}$$

$\rightarrow$ CDCL *in principle* possible

Resolution

Towards CDCL

$$\frac{\{X_1, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_2, \neg X_3\}} \qquad\qquad \frac{\{X_1, \neg X_2, \neg X_3\} \qquad \{\neg X_1, X_2\}}{\{X_1 \oplus X_2, \neg X_3\}}$$

s-resolution [Horacek]

$$\frac{\bigcup_{i=1}^{s}\{L_i\} \cup F \qquad \bigcup_{i=1}^{s}\{\neg L_i\} \cup G}{\bigcup_{i=1}^{s-1}\{L_i \oplus L_{i+1}\} \cup F \cup G}$$

$\rightarrow$ CDCL *in principle* possible

weaken clauses & change representation before resolution

$\rightsquigarrow$ expensive linear algebra?

Current State

`xnf_solver`

- Gaußian Constraint Propagation
  - watched linerals ✓
  - linear algebra ~

Current State

`xnf_solver`

- Gaußian Constraint Propagation
  - watched linerals ✓
  - linear algebra ~
    - ⟶ Gauß-Jordan with backtracking?
    - ⟶ how to treat equivalent literals?

Current State

`xnf_solver`

- Gaußian Constraint Propagation
  - watched linerals ✓
  - linear algebra ~
    - ⟶ Gauß-Jordan with backtracking?
    - ⟶ how to treat equivalent literals?
- conflict learning
  - theory ✓
  - implementation ~

Current State

`xnf_solver`

- Gaußian Constraint Propagation
  - watched linerals ✓
  - linear algebra ~
    - → Gauß-Jordan with backtracking?
    - → how to treat equivalent literals?
- conflict learning
  - theory ✓
  - implementation ~
    - → clause minimization?

Current State

`xnf_solver`

- Gaußian Constraint Propagation
  - watched linerals ✓
  - linear algebra ~
    - → Gauß-Jordan with backtracking?
    - → how to treat equivalent literals?
- conflict learning
  - theory ✓
  - implementation ~
    - → clause minimization?
- modern decision heuristics ×
- proofs for UNSAT instances ×

Current State

`xnf_solver`

- Gaußian Constraint Propagation
  - watched linerals ✓
  - linear algebra ~
    - → Gauß-Jordan with backtracking?
    - → how to treat equivalent literals?
- conflict learning
  - theory ✓
  - implementation ~
    - → clause minimization?
- modern decision heuristics ×
- proofs for UNSAT instances ×

→ DPLL solver in C++ ✓

Experiments

`XNF_to_ANF`

$$L_1 \vee \cdots \vee L_k \quad \longleftrightarrow \quad \ell_1 \cdots \ell_k$$

Experiments

`XNF_to_ANF`

$$L_1 \vee \cdots \vee L_k \quad \longleftrightarrow \quad \ell_1 \cdots \ell_k$$

`XNF_to_CNF-XOR`

$$L_1 \vee \cdots \vee L_k$$

$$\updownarrow$$

$$(Y_1 \oplus \neg L_1) \wedge \cdots \wedge (Y_k \oplus \neg L_k) \wedge (Y_1 \vee \cdots \vee Y_k)$$

Experiments

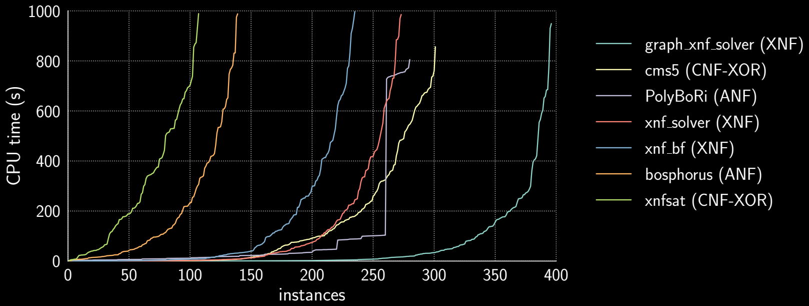


Figure: Cactus plots for 400 random *satisfiable* 2-XNF in n variables and $3n$ clauses where $n \in \{21, \dots, 40\}$.

Experiments

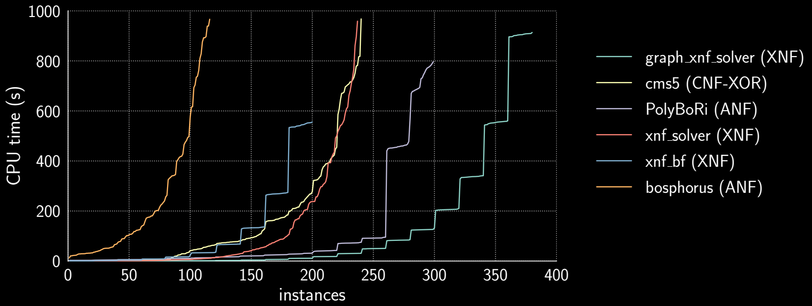


Figure: Cactus plots for 400 random 2-XNF in n variables and $3n$ clauses where $n \in \{21, \ldots, 40\}$.

Experiments

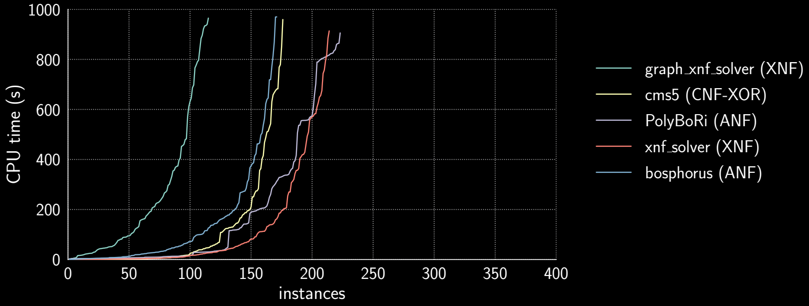


Figure: Cactus plots for 400 random *satisfiable* ANFs in n indeterminates and $2n$ quadratic polynomials where $n \in \{21, \dots, 40\}$.

Experiments

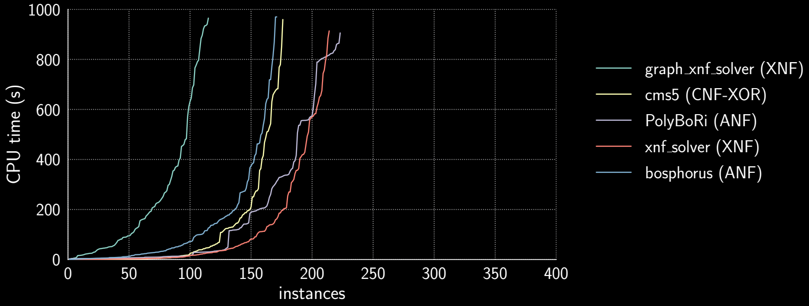


Figure: Cactus plots for 400 random *satisfiable* ANFs in n indeterminates and $2n$ quadratic polynomials where $n \in \{21, \ldots, 40\}$.

Thank you for your attention!