# Sage Reference Manual: Sat

Release 8.5

**The Sage Development Team** 

## **CONTENTS**

1	Solvers	3
2	Converters	19
3	Highlevel Interfaces	27
4	Indices and Tables	31
Bibliography		33
Python Module Index		35
In	dex	37

Sage supports solving clauses in Conjunctive Normal Form (see Wikipedia article Conjunctive\_normal\_form), i.e., SAT solving, via an interface inspired by the usual DIMACS format used in SAT solving [SG09]. For example, to express that:

x1 OR x2 OR (NOT x3)

should be true, we write:

(1, 2, -3)

Warning: Variable indices must start at one.

CONTENTS 1

2 CONTENTS

**CHAPTER** 

ONE

## **SOLVERS**

By default, Sage solves SAT instances as an Integer Linear Program (see sage.numerical.mip), but any SAT solver supporting the DIMACS input format is easily interfaced using the sage.sat.solvers.dimacs. DIMACS blueprint. Sage ships with pre-written interfaces for RSat [RS] and Glucose [GL]. Furthermore, Sage provides an interface to the CryptoMiniSat [CMS] SAT solver which can be used interchangably with DIMACS-based solvers. For this last solver, the optional CryptoMiniSat package must be installed, this can be accomplished by typing the following in the shell:

```
sage -i cryptominisat sagelib
```

We now show how to solve a simple SAT problem.

```
(x1 OR x2 OR x3) AND (x1 OR x2 OR (NOT x3))
```

In Sage's notation:

```
sage: solver = SAT()
sage: solver.add_clause( ( 1, 2, 3) )
sage: solver.add_clause( ( 1, 2, -3) )
sage: solver()  # random
(None, True, True, False)
```

**Note:** add\_clause() creates new variables when necessary. When using CryptoMiniSat, it creates *all* variables up to the given index. Hence, adding a literal involving the variable 1000 creates up to 1000 internal variables.

DIMACS-base solvers can also be used to write DIMACS files:

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: solver.add_clause( ( 1, 2, 3) )
sage: solver.add_clause( ( 1, 2, -3) )
sage: _ = solver.write()
sage: for line in open(fn).readlines():
....: print(line)
p cnf 3 2
1 2 3 0
1 2 -3 0
```

Alternatively, there is sage.sat.solvers.dimacs.DIMACS.clauses():

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS()
sage: solver.add_clause( ( 1, 2, 3) )
sage: solver.add_clause( ( 1, 2, -3) )
sage: solver.clauses(fn)
sage: for line in open(fn).readlines():
....:    print(line)
p cnf 3 2
1 2 3 0
1 2 -3 0
```

These files can then be passed external SAT solvers.

## 1.1 Details on Specific Solvers

#### 1.1.1 Abstract SAT Solver

All SAT solvers must inherit from this class.

**Note:** Our SAT solver interfaces are 1-based, i.e., literals start at 1. This is consistent with the popular DIMACS format for SAT solving but not with Pythion's 0-based convention. However, this also allows to construct clauses using simple integers.

#### **AUTHORS:**

• Martin Albrecht (2012): first version

```
sage.sat.solvers.satsolver.SAT (solver=None, *args, **kwds)
Return a SatSolver instance.
```

Through this class, one can define and solve SAT problems.

#### INPUT:

- solver (string) select a solver. Admissible values are:
  - "cryptominisat" note that the cryptominisat package must be installed.
  - "picosat" note that the pycosat package must be installed.
  - "LP" use SatLP to solve the SAT instance.
  - None (default) use CryptoMiniSat if available, else PicoSAT if available, and a LP solver otherwise.

#### **EXAMPLES:**

```
sage: SAT(solver="LP")
an ILP-based SAT Solver
```

```
class sage.sat.solvers.satsolver.SatSolver
    Bases: object
    add_clause (lits)
        Add a new clause to set of clauses.
    INPUT:
```

4 Chapter 1. Solvers

• lits - a tuple of integers != 0

**Note:** If any element e in lits has abs (e) greater than the number of variables generated so far, then new variables are created automatically.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.add_clause( (1, -2 , 3) )
Traceback (most recent call last):
...
NotImplementedError
```

#### clauses (filename=None)

Return original clauses.

#### INPUT:

• filename'' - if not ``None clauses are written to filename in DIMACS format (default: None)

#### **OUTPUT:**

If filename is None then a list of lits, is\_xor, rhs tuples is returned, where lits is a tuple of literals, is\_xor is always False and rhs is always None.

If filename points to a writable file, then the list of original clauses is written to that file in DIMACS format.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.clauses()
Traceback (most recent call last):
...
NotImplementedError
```

## conflict\_clause()

Return conflict clause if this instance is UNSAT and the last call used assumptions.

### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.conflict_clause()
Traceback (most recent call last):
...
NotImplementedError
```

#### learnt\_clauses (unitary\_only=False)

Return learnt clauses.

#### INPUT:

• unitary\_only - return only unitary learnt clauses (default: False)

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.learnt_clauses()
Traceback (most recent call last):
...
NotImplementedError

sage: solver.learnt_clauses(unitary_only=True)
Traceback (most recent call last):
...
NotImplementedError
```

#### nvars()

Return the number of variables.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.nvars()
Traceback (most recent call last):
...
NotImplementedError
```

#### read (filename)

Reads DIMAC files.

Reads in DIMAC formatted lines (lazily) from a file or file object and adds the corresponding clauses into this solver instance. Note that the DIMACS format is not well specified, see http://people.sc.fsu.edu/~jburkardt/data/cnf/cnf.html, http://www.satcompetition.org/2009/format-benchmarks2009.html, and http://elis.dvo.ru/~lab\_11/glpk-doc/cnfsat.pdf.

The differences were summarized in the discussion on the ticket trac ticket #16924. This method assumes the following DIMACS format:

- Any line starting with "c" is a comment
- Any line starting with "p" is a header
- Any variable 1-n can be used
- Every line containing a clause must end with a "0"

The format is extended to allow lines starting with "x" defining xor clauses, with the notation introduced in cryptominisat, see https://www.msoos.org/xor-clauses/

#### INPUT:

6

• filename - The name of a file as a string or a file object

#### **EXAMPLES:**

With xor clauses:

```
sage: from six import StringIO # for python 2/3 support
sage: file_object = StringIO("c A sample .cnf file with xor clauses.\np cnf 3_
\rightarrow3\n1 2 0\n3 0\nx1 2 3 0")
sage: from sage.sat.solvers.cryptominisat import CryptoMiniSat
                                                                          #__
→optional - cryptominisat
sage: solver = CryptoMiniSat()
→optional - cryptominisat
sage: solver.read(file_object)
→optional - cryptominisat
sage: solver.clauses()
→optional - cryptominisat
[((1, 2), False, None), ((3,), False, None), ((1, 2, 3), True, True)]
sage: solver()
→optional - cryptominisat
(None, True, True, True)
```

#### trait names()

Allow alias to appear in tab completion.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.trait_names()
['gens']
```

#### var (decision=None)

Return a new variable.

### INPUT:

• decision - is this variable a decision variable?

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.satsolver import SatSolver
sage: solver = SatSolver()
sage: solver.var()
Traceback (most recent call last):
...
NotImplementedError
```

#### 1.1.2 SAT-Solvers via DIMACS Files

Sage supports calling SAT solvers using the popular DIMACS format. This module implements infrastructure to make it easy to add new such interfaces and some example interfaces.

Currently, interfaces to **RSat** and **Glucose** are included by default.

**Note:** Our SAT solver interfaces are 1-based, i.e., literals start at 1. This is consistent with the popular DIMACS format for SAT solving but not with Pythion's 0-based convention. However, this also allows to construct clauses using simple integers.

**AUTHORS:** 

• Martin Albrecht (2012): first version

#### **Classes and Methods**

Note: Usually, users won't have to use this class directly but some class which inherits from this class.

```
__init__ (command=None, filename=None, verbosity=0, **kwds)
Construct a new generic DIMACS solver.
```

#### INPUT:

- command a named format string with the command to run. The string must contain {input} and may contain {output} if the solvers writes the solution to an output file. For example "sat-solver {input}" is a valid command. If None then the class variable command is used. (default: None)
- filename a filename to write clauses to in DIMACS format, must be writable. If None a temporary filename is chosen automatically. (default: None)
- verbosity a verbosity level, where zero means silent and anything else means verbose output.
   (default: 0)
- \*\*kwds accepted for compatibility with other solves, ignored.

```
__call__(assumptions=None)
```

Run 'command' and collect output.

#### INPUT:

assumptions - ignored, accepted for compatibility with other solvers (default: None)

#### add\_clause (lits)

Add a new clause to set of clauses.

#### INPUT:

• lits - a tuple of integers != 0

**Note:** If any element e in lits has abs (e) greater than the number of variables generated so far, then new variables are created automatically.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: solver = DIMACS()
sage: solver.var()
1
sage: solver.var(decision=True)
2
sage: solver.add_clause( (1, -2 , 3) )
sage: solver
DIMACS Solver: ''
```

#### clauses (filename=None)

Return original clauses.

#### INPUT:

• filename - if not None clauses are written to filename in DIMACS format (default: None)

#### **OUTPUT**:

If filename is None then a list of lits, is\_xor, rhs tuples is returned, where lits is a tuple of literals, is\_xor is always False and rhs is always None.

If filename points to a writable file, then the list of original clauses is written to that file in DIMACS format.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS()
sage: solver.add_clause( (1, 2, 3) )
sage: solver.clauses()
[((1, 2, 3), False, None)]

sage: solver.add_clause( (1, 2, -3) )
sage: solver.clauses(fn)
sage: print(open(fn).read())
p cnf 3 2
1 2 3 0
1 2 -3 0
```

#### nvars()

Return the number of variables.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: solver = DIMACS()
sage: solver.var()
1
sage: solver.var(decision=True)
2
sage: solver.nvars()
2
```

#### static render\_dimacs (clauses, filename, nlits)

Produce DIMACS file filename from clauses.

#### INPUT:

- clauses a list of clauses, either in simple format as a list of literals or in extended format for CryptoMiniSat: a tuple of literals, is\_xor and rhs.
- filename the file to write to
- nlits -- the number of literals appearing in ``clauses

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS()
```

(continues on next page)

(continued from previous page)

```
sage: solver.add_clause( (1, 2, -3) )
sage: DIMACS.render_dimacs(solver.clauses(), fn, solver.nvars())
sage: print(open(fn).read())
p cnf 3 1
1 2 -3 0
```

This is equivalent to:

```
sage: solver.clauses(fn)
sage: print(open(fn).read())
p cnf 3 1
1 2 -3 0
```

This function also accepts a "simple" format:

```
sage: DIMACS.render_dimacs([ (1,2), (1,2,-3) ], fn, 3)
sage: print(open(fn).read())
p cnf 3 2
1 2 0
1 2 -3 0
```

var (decision=None)

Return a new variable.

INPUT:

• decision - accepted for compatibility with other solvers, ignored.

**EXAMPLES**:

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: solver = DIMACS()
sage: solver.var()
1
```

write (filename=None)

Write DIMACS file.

INPUT:

• filename - if None default filename specified at initialization is used for writing to (default: None)

**EXAMPLES:** 

```
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: solver.add_clause( (1, -2 , 3) )
sage: _ = solver.write()
sage: for line in open(fn).readlines():
....:     print(line)
p cnf 3 1
1 -2 3 0

sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS()
sage: solver.add_clause( (1, -2 , 3) )
```

(continues on next page)

(continued from previous page)

```
sage: _ = solver.write(fn)
sage: for line in open(fn).readlines():
....:     print(line)
p cnf 3 1
1 -2 3 0
```

Bases: sage.sat.solvers.dimacs.DIMACS

An instance of the Glucose solver.

For information on Glucose see: http://www.lri.fr/~simon/?page=glucose

class sage.sat.solvers.dimacs.RSat (command=None, filename=None, verbosity=0, \*\*kwds)
Bases: sage.sat.solvers.dimacs.DIMACS

An instance of the RSat solver.

For information on RSat see: http://reasoning.cs.ucla.edu/rsat/

#### 1.1.3 PicoSAT Solver

This solver relies on the pycosat Python bindings to PicoSAT.

The pycosat package should be installed on your Sage installation.

#### **AUTHORS:**

• Thierry Monteil (2018): initial version.

```
class sage.sat.solvers.picosat.PicoSAT(verbosity=0, prop_limit=0)
    Bases: sage.sat.solvers.satsolver.SatSolver
```

PicoSAT Solver.

#### INPUT:

- verbosity an integer between 0 and 2 (default: 0); verbosity
- prop\_limit an integer (default: 0); the propagation limit

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.picosat import PicoSAT
sage: solver = PicoSAT() # optional - pycosat
```

#### add clause (lits)

Add a new clause to set of clauses.

### INPUT:

• lits – a tuple of nonzero integers

**Note:** If any element e in lits has abs (e) greater than the number of variables generated so far, then new variables are created automatically.

**EXAMPLES:** 

```
sage: from sage.sat.solvers.picosat import PicoSAT
sage: solver = PicoSAT() # optional - pycosat
sage: solver.add_clause((1, -2 , 3)) # optional - pycosat
```

#### clauses (filename=None)

Return original clauses.

#### INPUT:

• filename – (optional) if given, clauses are written to filename in DIMACS format

#### **OUTPUT:**

If filename is None then a list of lits is returned, where lits is a list of literals.

If filename points to a writable file, then the list of original clauses is written to that file in DIMACS format.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.picosat import PicoSAT
sage: solver = PicoSAT()  # optional - pycosat
sage: solver.add_clause((1,2,3,4,5,6,7,8,-9))  # optional - pycosat
sage: solver.clauses()  # optional - pycosat
[[1, 2, 3, 4, 5, 6, 7, 8, -9]]
```

#### DIMACS format output:

```
sage: from sage.sat.solvers.picosat import PicoSAT
sage: solver = PicoSAT()  # optional - pycosat
sage: solver.add_clause((1, 2, 4))  # optional - pycosat
sage: solver.add_clause((1, 2, -4))  # optional - pycosat
sage: fn = tmp_filename()  # optional - pycosat
sage: solver.clauses(fn)  # optional - pycosat
sage: print(open(fn).read())  # optional - pycosat
p cnf 4 2
1 2 4 0
1 2 -4 0
```

## nvars()

Return the number of variables. Note that for compatibility with DIMACS convention, the number of variables corresponds to the maximal index of the variables used.

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.picosat import PicoSAT
sage: solver = PicoSAT()  # optional - pycosat
sage: solver.nvars()  # optional - pycosat
0
```

If a variable with intermediate index is not used, it is still considered as a variable:

```
sage: solver.add_clause((1,-2,4)) # optional - pycosat
sage: solver.nvars() # optional - pycosat
4
```

#### var (decision=None)

Return a new variable.

INPUT:

decision – ignored; accepted for compatibility with other solvers

#### **EXAMPLES:**

```
sage: from sage.sat.solvers.picosat import PicoSAT
sage: solver = PicoSAT()  # optional - pycosat
sage: solver.var()  # optional - pycosat

sage: solver.add_clause((-1,2,-4))  # optional - pycosat
sage: solver.var()  # optional - pycosat
```

## 1.1.4 Solve SAT problems Integer Linear Programming

The class defined here is a *SatSolver* that solves its instance using MixedIntegerLinearProgram. Its performance can be expected to be slower than when using CryptoMiniSat.

```
class sage.sat.solvers.sat_lp.SatLP (solver=None, verbose=0)
    Bases: sage.sat.solvers.satsolver.SatSolver
```

Initializes the instance

#### INPUT:

- solver (default: None) Specify a Linear Program (LP) solver to be used. If set to None, the default one is used. For more information on LP solvers and which default solver is used, see the method solve() of the class MixedIntegerLinearProgram.
- verbose integer (default: 0). Sets the level of verbosity of the LP solver. Set to 0 by default, which means quiet.

#### **EXAMPLES:**

```
sage: S=SAT(solver="LP"); S
an ILP-based SAT Solver
```

#### add clause (lits)

Add a new clause to set of clauses.

#### INPUT:

• lits - a tuple of integers != 0

**Note:** If any element e in lits has abs (e) greater than the number of variables generated so far, then new variables are created automatically.

#### **EXAMPLES:**

#### nvars()

Return the number of variables.

#### **EXAMPLES:**

```
sage: S=SAT(solver="LP"); S
an ILP-based SAT Solver
sage: S.var()
1
sage: S.var()
2
sage: S.nvars()
2
```

#### var()

Return a new variable.

#### **EXAMPLES:**

```
sage: S=SAT(solver="LP"); S
an ILP-based SAT Solver
sage: S.var()
1
```

## 1.1.5 CryptoMiniSat Solver

This solver relies on Python bindings provided by upstream cryptominisat.

The cryptominisat package should be installed on your Sage installation.

#### **AUTHORS:**

- Thierry Monteil (2017): complete rewrite, using upstream Python bindings, works with crypominisat 5.
- Martin Albrecht (2012): first version, as a cython interface, works with crypominisat 2.

CryptoMiniSat Solver.

#### INPUT:

- verbosity an integer between 0 and 15 (default: 0). Verbosity.
- confl\_limit an integer (default: None). Abort after this many conflicts. If set to None, never aborts.
- threads an integer (default: None). The number of thread to use. If set to None, the number of threads used corresponds to the number of cpus.

## **EXAMPLES:**

#### add clause (lits)

Add a new clause to set of clauses.

#### INPUT:

• lits – a tuple of nonzero integers.

**Note:** If any element e in lits has abs (e) greater than the number of variables generated so far, then new variables are created automatically.

#### **EXAMPLES:**

#### add\_xor\_clause (lits, rhs=True)

Add a new XOR clause to set of clauses.

#### INPUT:

- lits a tuple of positive integers.
- rhs boolean (default: True). Whether this XOR clause should be evaluated to True or False.

#### **EXAMPLES:**

#### clauses (filename=None)

Return original clauses.

#### INPUT:

• filename – if not None clauses are written to filename in DIMACS format (default: None)

#### **OUTPUT**:

If filename is None then a list of lits, is\_xor, rhs tuples is returned, where lits is a tuple of literals, is\_xor is always False and rhs is always None.

If filename points to a writable file, then the list of original clauses is written to that file in DIMACS format.

#### **EXAMPLES:**

## DIMACS format output:

```
sage: from sage.sat.solvers import CryptoMiniSat
sage: solver = CryptoMiniSat()
                                                     # optional - cryptominisat
sage: solver.add_clause((1, 2, 4))
                                                     # optional - cryptominisat
sage: solver.add_clause((1, 2, -4))
                                                     # optional - cryptominisat
                                                     # optional - cryptominisat
sage: fn = tmp_filename()
                                                     # optional - cryptominisat
sage: solver.clauses(fn)
sage: print(open(fn).read())
                                                     # optional - cryptominisat
p cnf 4 2
1 2 4 0
1 \ 2 \ -4 \ 0
```

Note that in cryptominisat, the DIMACS standard format is augmented with the following extension: having an x in front of a line makes that line an XOR clause:

```
sage: solver.add_xor_clause((1,2,3), rhs=True) # optional - cryptominisat
sage: solver.clauses(fn) # optional - cryptominisat
sage: print(open(fn).read()) # optional - cryptominisat
p cnf 4 3
1 2 4 0
1 2 -4 0
x1 2 3 0
```

Note that inverting an xor-clause is equivalent to inverting one of the variables:

```
sage: solver.add_xor_clause((1,2,5),rhs=False) # optional - cryptominisat
sage: solver.clauses(fn) # optional - cryptominisat
sage: print(open(fn).read()) # optional - cryptominisat
p cnf 5 4
1 2 4 0
1 2 -4 0
x1 2 3 0
x1 2 -5 0
```

#### nvars()

Return the number of variables. Note that for compatibility with DIMACS convention, the number of variables corresponds to the maximal index of the variables used.

#### **EXAMPLES:**

If a variable with intermediate index is not used, it is still considered as a variable:

## var (decision=None)

Return a new variable.

### INPUT:

• decision – accepted for compatibility with other solvers, ignored.

### **EXAMPLES:**

18 Chapter 1. Solvers

**CHAPTER** 

**TWO** 

## **CONVERTERS**

Sage supports conversion from Boolean polynomials (also known as Algebraic Normal Form) to Conjunctive Normal Form:

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B)
sage: e.clauses_sparse(a*b + a + 1)
sage: _ = solver.write()
sage: print(open(fn).read())
p cnf 3 2
-2 0
1 0
```

## 2.1 Details on Specific Converterts

## 2.1.1 An ANF to CNF Converter using a Dense/Sparse Strategy

This converter is based on two converters. The first one, by Martin Albrecht, was based on [CB2007], this is the basis of the "dense" part of the converter. It was later improved by Mate Soos. The second one, by Michael Brickenstein, uses a reduced truth table based approach and forms the "sparse" part of the converter.

#### **AUTHORS:**

- Martin Albrecht (2008-09) initial version of 'anf2cnf.py'
- Michael Brickenstein (2009) 'cnf.py' for PolyBoRi
- Mate Soos (2010) improved version of 'anf2cnf.py'
- Martin Albrecht (2012) unified and added to Sage

#### **Classes and Methods**

```
 \begin{array}{c} \textbf{class} \text{ sage.sat.converters.polybori.CNFEncoder} (solver, & ring, & max\_vars\_sparse=6, \\ & use\_xor\_clauses=None, & cutting\_number=6, random\_seed=16) \\ & \text{Bases: sage.sat.converters.anf2cnf.ANF2CNFConverter} \end{array}
```

ANF to CNF Converter using a Dense/Sparse Strategy. This converter distinguishes two classes of polynomials.

- 1. Sparse polynomials are those with at most max\_vars\_sparse variables. Those are converted using reduced truth-tables based on PolyBoRi's internal representation.
- 2. Polynomials with more variables are converted by introducing new variables for monomials and by converting these linearised polynomials.

Linearised polynomials are converted either by splitting XOR chains — into chunks of length cutting\_number — or by constructing XOR clauses if the underlying solver supports it. This behaviour is disabled by passing use\_xor\_clauses=False.

```
__init__(solver, ring, max_vars_sparse=6, use_xor_clauses=None, cutting_number=6, ran-dom_seed=16)
```

Construct ANF to CNF converter over ring passing clauses to solver.

#### INPUT:

- solver a SAT-solver instance
- ring a sage.rings.polynomial.pbori.BooleanPolynomialRing
- max\_vars\_sparse maximum number of variables for direct conversion
- use\_xor\_clauses use XOR clauses; if None use if solver supports it. (default: None)
- cutting\_number maximum length of XOR chains after splitting if XOR clauses are not supported (default: 6)
- random\_seed the direct conversion method uses randomness, this sets the seed (default: 16)

#### **EXAMPLES:**

We compare the sparse and the dense strategies, sparse first:

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B)
sage: e.clauses_sparse(a*b + a + 1)
sage: _ = solver.write()
sage: print(open(fn).read())
p cnf 3 2
-2 0
1 0
sage: e.phi
[None, a, b, c]
```

Now, we convert using the dense strategy:

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B)
sage: e.clauses_dense(a*b + a + 1)
sage: _ = solver.write()
sage: print(open(fn).read())
p cnf 4 5
1 -4 0
2 -4 0
```

(continues on next page)

(continued from previous page)

```
4 -1 -2 0

-4 -1 0

4 1 0

sage: e.phi

[None, a, b, c, a*b]
```

**Note:** This constructor generates SAT variables for each Boolean polynomial variable.

#### $\underline{\phantom{a}}$ call $\underline{\phantom{a}}$ (F)

Encode the boolean polynomials in  $\mathbb{F}$ .

#### INPUT:

• F - an iterable of sage.rings.polynomial.pbori.BooleanPolynomial

OUTPUT: An inverse map int -> variable

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B, max_vars_sparse=2)
sage: e([a*b + a + 1, a*b+ a + c])
[None, a, b, c, a*b]
sage: _ = solver.write()
sage: print(open(fn).read())
p cnf 4 9
-2 0
1 0
1 -4 0
2 - 4 0
4 - 1 - 2 0
-4 -1 -3 0
4 1 -3 0
4 - 1 \ 3 \ 0
-4 1 3 0
sage: e.phi
[None, a, b, c, a*b]
```

## clauses(f)

Convert f using the sparse strategy if f.nvariables () is at most max\_vars\_sparse and the dense strategy otherwise.

#### INPUT:

• f-a sage.rings.polynomial.pbori.BooleanPolynomial

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
```

(continues on next page)

(continued from previous page)

```
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B, max_vars_sparse=2)
sage: e.clauses(a*b + a + 1)
sage: _ = solver.write()
sage: print (open (fn) . read())
p cnf 3 2
-2 0
1 0
sage: e.phi
[None, a, b, c]
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B, max_vars_sparse=2)
sage: e.clauses(a*b + a + c)
sage: _ = solver.write()
sage: print (open(fn).read())
p cnf 4 7
1 - 4 0
2 - 4 0
4 - 1 - 2 0
-4 -1 -3 0
4 \ 1 \ -3 \ 0
4 - 1 \ 3 \ 0
-4 1 3 0
sage: e.phi
[None, a, b, c, a*b]
```

#### $clauses\_dense(f)$

Convert f using the dense strategy.

#### INPUT:

• f-a sage.rings.polynomial.pbori.BooleanPolynomial

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B)
sage: e.clauses_dense(a*b + a + 1)
sage: _ = solver.write()
sage: print (open(fn).read())
p cnf 4 5
1 - 4 0
2 - 4 0
4 -1 -2 0
-4 -1 0
4 1 0
sage: e.phi
[None, a, b, c, a*b]
```

#### $clauses\_sparse(f)$

Convert f using the sparse strategy.

#### INPUT:

• f-a sage.rings.polynomial.pbori.BooleanPolynomial

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B)
sage: e.clauses_sparse(a*b + a + 1)
sage: _ = solver.write()
sage: print(open(fn).read())
p cnf 3 2
-2 0
1 0
sage: e.phi
[None, a, b, c]
```

#### monomial(m)

Return SAT variable for m

#### INPUT:

• m - a monomial.

OUTPUT: An index for a SAT variable corresponding to m.

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B)
sage: e.clauses_dense(a*b + a + 1)
sage: e.phi
[None, a, b, c, a*b]
```

If monomial is called on a new monomial, a new variable is created:

```
sage: e.monomial(a*b*c)
5
sage: e.phi
[None, a, b, c, a*b, a*b*c]
```

If monomial is called on a monomial that was queried before, the index of the old variable is returned and no new variable is created:

```
sage: e.monomial(a*b)
4
sage: e.phi
[None, a, b, c, a*b, a*b*c]
```

(continues on next page)

(continued from previous page)

```
.. note::

For correctness, this function is cached.
```

#### permutations (length, equal\_zero)

Return permutations of length length which are equal to zero if equal\_zero and equal to one otherwise.

A variable is false if the integer in its position is smaller than zero and true otherwise.

#### INPUT:

- length the number of variables
- equal\_zero should the sum be equal to zero?

### **EXAMPLES**:

```
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: ce = CNFEncoder(DIMACS(), B)
sage: ce.permutations(3, True)
[[-1, -1, -1], [1, 1, -1], [1, -1, 1], [-1, 1, 1]]
sage: ce.permutations(3, False)
[[1, -1, -1], [-1, 1, -1], [-1, -1, 1], [1, 1, 1]]
```

#### phi

Map SAT variables to polynomial variables.

### **EXAMPLES:**

```
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: ce = CNFEncoder(DIMACS(), B)
sage: ce.var()
4
sage: ce.phi
[None, a, b, c, None]
```

### split\_xor (monomial\_list, equal\_zero)

Split XOR chains into subchains.

#### INPUT:

- monomial\_list a list of monomials
- equal\_zero is the constant coefficient zero?

#### EXAMPLES:

(continues on next page)

(continued from previous page)

```
sage: ce = CNFEncoder(DIMACS(), B, cutting_number=4)
sage: ce.split_xor([1,2,3,4,5,6], False)
[[[1, 2, 7], False], [[7, 3, 4, 8], True], [[8, 5, 6], True]]
sage: ce = CNFEncoder(DIMACS(), B, cutting_number=5)
sage: ce.split_xor([1,2,3,4,5,6], False)
[[[1, 2, 3, 7], False], [[7, 4, 5, 6], True]]
```

#### to\_polynomial(c)

Convert clause to sage.rings.polynomial.pbori.BooleanPolynomial

#### INPUT:

• c - a clause

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: fn = tmp_filename()
sage: solver = DIMACS(filename=fn)
sage: e = CNFEncoder(solver, B, max_vars_sparse=2)
sage: _ = e([a*b + a + 1, a*b+ a + c])
sage: e.to_polynomial( (1,-2,3) )
a*b*c + a*b + b*c + b
```

#### var (m=None, decision=None)

Return a new variable.

This is a thin wrapper around the SAT-solvers function where we keep track of which SAT variable corresponds to which monomial.

#### INPUT:

- m something the new variables maps to, usually a monomial
- decision is this variable a decision variable?

#### **EXAMPLES:**

```
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: ce = CNFEncoder(DIMACS(), B)
sage: ce.var()
4
```

#### zero blocks(f)

Divide the zero set of f into blocks.

#### **EXAMPLES:**

```
sage: B.<a,b,c> = BooleanPolynomialRing()
sage: from sage.sat.converters.polybori import CNFEncoder
sage: from sage.sat.solvers.dimacs import DIMACS
sage: e = CNFEncoder(DIMACS(), B)
sage: sorted(sorted(d.items()) for d in e.zero_blocks(a*b*c))
[[(c, 0)], [(b, 0)], [(a, 0)]]
```

**Note:** This function is randomised.

**CHAPTER** 

THREE

## HIGHLEVEL INTERFACES

Sage provides various highlevel functions which make working with Boolean polynomials easier. We construct a very small-scale AES system of equations and pass it to a SAT solver:

## 3.1 Details on Specific Highlevel Interfaces

## 3.1.1 SAT Functions for Boolean Polynomials

These highlevel functions support solving and learning from Boolean polynomial systems. In this context, "learning" means the construction of new polynomials in the ideal spanned by the original polynomials.

#### **AUTHOR:**

• Martin Albrecht (2012): initial version

## **Functions**

#### NI 0 I.

- F a sequence of Boolean polynomials
- converter an ANF to CNF converter class or object. If converter is None then sage.sat. converters.polybori.CNFEncoder is used to construct a new converter. (default: None)
- solver a SAT-solver class or object. If solver is None then sage.sat.solvers. cryptominisat.CryptoMiniSat is used to construct a new converter. (default: None)
- max\_learnt\_length only clauses of length <= max\_length\_learnt are considered and converted to polynomials. (default: 3)

• interreduction - inter-reduce the resulting polynomials (default: False)

**Note:** More parameters can be passed to the converter and the solver by prefixing them with  $c_a$  and  $s_b$  respectively. For example, to increase CryptoMiniSat's verbosity level, pass  $s_b$  verbosity=1.

#### **OUTPUT:**

A sequence of Boolean polynomials.

#### **EXAMPLES:**

We construct a simple system and solve it:

```
sage: set_random_seed(2300)  # optional - cryptominisat
sage: sr = mq.SR(1,2,2,4,gf2=True,polybori=True) # optional - cryptominisat
sage: F,s = sr.polynomial_system()  # optional - cryptominisat
sage: H = learn_sat(F)  # optional - cryptominisat
sage: H[-1]  # optional - cryptominisat
k033 + 1
```

```
sage.sat.boolean\_polynomials. \textbf{solve}(\textit{F}, converter=None, solver=None, n=1, tar-get\_variables=None, **kwds) \\ \\ tar-get\_variables=None, **kwds)
```

Solve system of Boolean polynomials F by solving the SAT-problem - produced by converter - using solver.

#### INPUT:

- F a sequence of Boolean polynomials
- n number of solutions to return. If n is +infinity then all solutions are returned. If n <infinity then n solutions are returned if F has at least n solutions. Otherwise, all solutions of F are returned. (default: 1)
- converter an ANF to CNF converter class or object. If converter is None then sage.sat. converters.polybori.CNFEncoder is used to construct a new converter. (default: None)
- solver a SAT-solver class or object. If solver is None then sage.sat.solvers. cryptominisat.CryptoMiniSat is used to construct a new converter. (default: None)
- target\_variables a list of variables. The elements of the list are used to exclude a particular combination of variable assignments of a solution from any further solution. Furthermore target\_variables denotes which variable-value pairs appear in the solutions. If target\_variables is None all variables appearing in the polynomials of F are used to construct exclusion clauses. (default: None)
- \*\*kwds parameters can be passed to the converter and the solver by prefixing them with c\_ and s\_ respectively. For example, to increase CryptoMiniSat's verbosity level, pass s\_verbosity=1.

#### **OUTPUT:**

A list of dictionaries, each of which contains a variable assignment solving F.

#### **EXAMPLES:**

We construct a very small-scale AES system of equations:

```
sage: sr = mq.SR(1,1,1,4,gf2=True,polybori=True)
sage: F,s = sr.polynomial_system()
```

and pass it to a SAT solver:

This time we pass a few options through to the converter and the solver:

We construct a very simple system with three solutions and ask for a specific number of solutions:

```
sage: B.<a,b> = BooleanPolynomialRing() # optional - cryptominisat
sage: f = a*b
                                        # optional - cryptominisat
                                        # optional - cryptominisat
sage: l = solve_sat([f], n=1)
sage: len(1) == 1, f.subs(1[0])
                                       # optional - cryptominisat
(True, 0)
sage: 1 = \text{sorted(solve\_sat([a*b], n=2))} # optional - cryptominisat
sage: len(1) == 2, f.subs(1[0]), f.subs(1[1]) # optional - cryptominisat
(True, 0, 0)
sage: sorted(solve_sat([a*b],n=3))
                                           # optional - cryptominisat
[{b: 0, a: 0}, {b: 0, a: 1}, {b: 1, a: 0}]
sage: sorted(solve_sat([a*b],n=4))
                                           # optional - cryptominisat
[{b: 0, a: 0}, {b: 0, a: 1}, {b: 1, a: 0}]
sage: sorted(solve_sat([a*b],n=infinity)) # optional - cryptominisat
[{b: 0, a: 0}, {b: 0, a: 1}, {b: 1, a: 0}]
```

In the next example we see how the target\_variables parameter works:

First the normal use case:

Now we are only interested in the solutions of the variables a and b:

**Note:** Although supported, passing converter and solver objects instead of classes is discouraged because these objects are stateful.

REFERENCES:

## **CHAPTER**

## **FOUR**

## **INDICES AND TABLES**

- Index
- Module Index
- Search Page

## **BIBLIOGRAPHY**

[RS] http://reasoning.cs.ucla.edu/rsat/

[GL] http://www.lri.fr/~simon/?page=glucose

[CMS] http://www.msoos.org

 $\textbf{[SG09]}\ http://www.satcompetition.org/2009/format-benchmarks 2009.html$ 

34 Bibliography

## **PYTHON MODULE INDEX**

## S

```
sage.sat.boolean_polynomials, 27
sage.sat.converters.polybori, 19
sage.sat.solvers.cryptominisat, 14
sage.sat.solvers.dimacs, 7
sage.sat.solvers.picosat, 11
sage.sat.solvers.sat_lp, 13
sage.sat.solvers.satsolver, 4
```

36 Python Module Index

## **INDEX**

## call () (sage.sat.converters.polybori.CNFEncoder method), 21 \_\_call\_\_() (sage.sat.solvers.dimacs.DIMACS method), 8 \_\_init\_\_() (sage.sat.converters.polybori.CNFEncoder method), 20 \_\_init\_\_() (sage.sat.solvers.dimacs.DIMACS method), 8 Α add\_clause() (sage.sat.solvers.cryptominisat.CryptoMiniSat method), 14 add\_clause() (sage.sat.solvers.dimacs.DIMACS method), 8 add\_clause() (sage.sat.solvers.picosat.PicoSAT method), 11 add\_clause() (sage.sat.solvers.sat\_lp.SatLP method), 13 add\_clause() (sage.sat.solvers.satsolver.SatSolver method), 4 add\_xor\_clause() (sage.sat.solvers.cryptominisat.CryptoMiniSat method), 15 C clauses() (sage.sat.converters.polybori.CNFEncoder method), 21 clauses() (sage.sat.solvers.cryptominisat.CryptoMiniSat method), 15 clauses() (sage.sat.solvers.dimacs.DIMACS method), 8 clauses() (sage.sat.solvers.picosat.PicoSAT method), 12 clauses() (sage.sat.solvers.satsolver.SatSolver method), 5 clauses\_dense() (sage.sat.converters.polybori.CNFEncoder method), 22 clauses\_sparse() (sage.sat.converters.polybori.CNFEncoder method), 22 CNFEncoder (class in sage.sat.converters.polybori), 19 CNFEncoder.permutations() (in module sage.sat.converters.polybori), 24 conflict\_clause() (sage.sat.solvers.satsolver.SatSolver method), 5 CryptoMiniSat (class in sage.sat.solvers.cryptominisat), 14 D DIMACS (class in sage.sat.solvers.dimacs), 8 G Glucose (class in sage.sat.solvers.dimacs), 11 learn() (in module sage.sat.boolean\_polynomials), 27 learnt\_clauses() (sage.sat.solvers.satsolver.SatSolver method), 5

**Symbols** 

```
M
monomial() (sage.sat.converters.polybori.CNFEncoder method), 23
Ν
nvars() (sage.sat.solvers.cryptominisat.CryptoMiniSat method), 16
nvars() (sage.sat.solvers.dimacs.DIMACS method), 9
nvars() (sage.sat.solvers.picosat.PicoSAT method), 12
nvars() (sage.sat.solvers.sat_lp.SatLP method), 13
nvars() (sage.sat.solvers.satsolver.SatSolver method), 6
phi (sage.sat.converters.polybori.CNFEncoder attribute), 24
PicoSAT (class in sage.sat.solvers.picosat), 11
R
read() (sage.sat.solvers.satsolver.SatSolver method), 6
render_dimacs() (sage.sat.solvers.dimacs.DIMACS static method), 9
RSat (class in sage.sat.solvers.dimacs), 11
S
sage.sat.boolean_polynomials (module), 27
sage.sat.converters.polybori (module), 19
sage.sat.solvers.cryptominisat (module), 14
sage.sat.solvers.dimacs (module), 7
sage.sat.solvers.picosat (module), 11
sage.sat.solvers.sat_lp (module), 13
sage.sat.solvers.satsolver (module), 4
SAT() (in module sage.sat.solvers.satsolver), 4
SatLP (class in sage.sat.solvers.sat_lp), 13
SatSolver (class in sage.sat.solvers.satsolver), 4
solve() (in module sage.sat.boolean_polynomials), 28
split_xor() (sage.sat.converters.polybori.CNFEncoder method), 24
Т
to_polynomial() (sage.sat.converters.polybori.CNFEncoder method), 25
trait names() (sage.sat.solvers.satsolver.SatSolver method), 7
V
var() (sage.sat.converters.polybori.CNFEncoder method), 25
var() (sage.sat.solvers.cryptominisat.CryptoMiniSat method), 16
var() (sage.sat.solvers.dimacs.DIMACS method), 10
var() (sage.sat.solvers.picosat.PicoSAT method), 12
var() (sage.sat.solvers.sat_lp.SatLP method), 14
var() (sage.sat.solvers.satsolver.SatSolver method), 7
W
write() (sage.sat.solvers.dimacs.DIMACS method), 10
Ζ
zero blocks() (sage.sat.converters.polybori.CNFEncoder method), 25
```

38 Index